FEDERATED LEARNING WITH LLM AUTOMATION - WEB-BASED SYSTEM

[1]K. VENKATESWARA RAO, [2]S. PRIYA VASANTHI, [3]J. CHANDINI,[4]R. CHINNI HEMADRI KUMAR, [5]MD.ASFIN

[1]ASSISTANT PROFESSOR, [2345]B. TECH, STUDENTS

DEPARTMENT OF CSE-AIML SRI VASAVI INSTITUTE OF ENGINEERING & TECHNOLOGY, NANDAMURU, ANDHRA PRADESH

ABSTRACT

The rapid advancement of Artificial Intelligence (AI) and Machine Learning (ML) has significantly transformed the healthcare sector by enabling predictive analytics, early disease detection, and data-driven clinical decision-making. However, healthcare institutions often face challenges in sharing sensitive patient data due to privacy regulations, security risks, and ethical concerns. Traditional centralized machine learning approaches require aggregating data from multiple organizations, which increases the risk of data breaches and violates strict privacy policies. To address these issues, this study proposes a privacy-preserving federated learning platform integrated with Large Language Model (LLM) automation for intelligent healthcare risk prediction. The proposed system allows multiple healthcare institutions to collaboratively train a global machine learning model without sharing raw patient data. Instead, each institution performs local model training and transmits only model parameters to a central aggregation server. These parameters are combined using the Federated Averaging algorithm to produce a generalized global predictive model while maintaining data privacy. Furthermore, the system incorporates a transformer-based LLM to generate human-readable explanations for prediction results, improving transparency and interpretability for medical professionals. The platform is implemented using a full-stack architecture consisting of a React-based frontend, Node.js backend, MongoDB database, and a Python Flask microservice for machine learning operations. The system also includes modules for authentication, dataset management, federated training coordination, model performance monitoring, and AI-driven explanation generation. Experimental results demonstrate that the proposed approach improves predictive accuracy while maintaining strict data privacy standards. The integration of federated learning and explainable AI provides a scalable and secure framework for collaborative healthcare analytics.

Keywords: Federated Learning, Healthcare Analytics, Privacy-Preserving AI, Large Language Models, Explainable AI, Machine Learning

I INTRODUCTION

The increasing adoption of artificial intelligence technologies has revolutionized data analysis and predictive modeling in healthcare systems worldwide [1]. Healthcare organizations generate enormous volumes of patient data from electronic health records, diagnostic systems, wearable devices, and clinical observations [2]. These datasets provide valuable insights for disease prediction, treatment planning, and population

health management [3]. However, most healthcare datasets are distributed across multiple hospitals and institutions, making centralized machine learning approaches difficult to implement due to strict privacy regulations and legal constraints [4]. Data sharing between institutions is often restricted because patient information is highly sensitive and protected under healthcare regulations [5]. As a result, many healthcare organizations are unable to fully utilize collaborative machine learning despite the potential benefits of aggregated datasets [6]. Researchers have proposed various privacy-preserving techniques to overcome these challenges [7]. Secure multiparty computation is one approach used to enable collaborative computation without exposing sensitive data [8]. Differential privacy techniques have also been introduced to protect personal information during model training [9]. Distributed learning models further support decentralized data analysis in privacy-sensitive environments [10]. Among these approaches, federated learning has emerged as one of the most promising techniques for collaborative model training without direct data sharing [11]. Federated learning enables multiple institutions to train shared models while keeping their data locally stored [12]. This approach improves data privacy and reduces the risks associated with centralized data storage [13]. In federated learning environments, each participating institution trains a local model on its own dataset [14]. Only model parameters or gradients are shared with a central aggregation server instead of raw data [15]. This strategy significantly reduces privacy risks in collaborative healthcare analytics [16]. It also allows models to learn from diverse datasets distributed across different institutions [17]. Federated learning has therefore become an important framework for privacy-preserving machine learning in healthcare systems [18]. Several studies have demonstrated its effectiveness in medical diagnosis and disease prediction tasks [19]. Consequently, federated learning provides a secure approach for collaborative healthcare analytics [20].

Despite the advantages of federated learning, several challenges remain in terms of model interpretability, system scalability, and usability for healthcare professionals [21]. Many machine learning models operate as black boxes, making it difficult for clinicians to understand the reasoning behind predictions [22]. Lack of interpretability can reduce trust in AI-based decision-support systems in clinical environments [23]. Recent advances in Large Language Models have introduced new possibilities for generating human-readable explanations for complex machine learning outputs [24]. Large language models can analyze prediction results and translate them into understandable natural language insights [25]. This capability improves transparency and supports clinical decision-making processes [26]. Integrating explanation systems with federated learning architectures can significantly enhance the usability of predictive models in healthcare environments [27]. Furthermore, modern web technologies enable the development of scalable platforms for collaborative model training [28]. These platforms allow multiple institutions to participate through secure web interfaces and cloud-based infrastructures [29]. This project therefore proposes a web-based federated learning platform integrated with large language model automation to provide privacy-preserving healthcare risk prediction and interpretable AI insights [30].

II LITERATURE SURVEY

Several studies have explored the application of machine learning in healthcare analytics to improve diagnostic accuracy and predictive modeling [1]. Traditional machine learning systems rely on

centralized datasets where data from multiple sources is collected and stored in a single repository for training predictive models [2]. While this approach can improve model performance by increasing the size of training datasets, it introduces serious privacy risks and legal concerns when dealing with sensitive patient information [3]. Researchers have therefore investigated alternative approaches to enable collaborative learning without direct data sharing [4]. Distributed learning techniques have been proposed to allow institutions to train models locally while participating in collaborative analytics [5]. Privacy-preserving data mining approaches have also been introduced to protect sensitive healthcare information during model training [6]. These techniques allow institutions to share only limited model information rather than raw data [7]. Such approaches help maintain data privacy while still enabling collaborative machine learning research [8]. Researchers have demonstrated that decentralized learning architectures can improve both data security and system scalability [9]. Consequently, privacy-preserving collaborative learning has become an important research direction in healthcare analytics [10]. One of the most influential developments in this area is federated learning, which was introduced as a decentralized machine learning paradigm where training occurs across multiple clients while keeping the raw data locally stored [11]. In this approach, a global model is created by aggregating locally trained models from participating nodes [12]. Each participating institution contributes to the global model by sharing only model parameters or gradients [13]. This mechanism significantly reduces the need for direct data sharing between institutions [14]. Studies have demonstrated that federated learning can achieve comparable performance to centralized training models [15]. At the same time, it significantly reduces the privacy risks associated with centralized data storage [16]. Federated learning also allows models to learn from diverse datasets distributed across multiple organizations [17]. This diversity improves model generalization and prediction accuracy in healthcare applications [18]. As a result, federated learning has become a promising solution for collaborative healthcare analytics [19]. Many recent healthcare prediction systems have adopted federated learning architectures to protect patient data privacy [20].

More recent research has focused on enhancing federated learning systems with improved communication efficiency, model security, and interpretability mechanisms [21]. Researchers have developed various aggregation algorithms to improve the performance of distributed model training [22]. Privacy-enhancing techniques such as differential privacy have also been incorporated to protect sensitive information during model updates [23]. Secure aggregation protocols further ensure that individual model contributions remain confidential during parameter exchange [24]. Another important challenge addressed in the literature is the lack of transparency in complex machine learning models used for healthcare predictions [25]. Explainable Artificial Intelligence techniques have therefore been introduced to provide interpretable explanations for machine learning outputs [26]. These techniques help clinicians understand the reasoning behind automated predictions generated by AI systems [27]. With the emergence of transformer-based Large Language Models, researchers have begun exploring their use for generating natural language explanations for AI systems [28]. Large language models can interpret complex prediction results and convert them into meaningful descriptions that healthcare professionals can easily understand [29]. Additionally, web-based architectures have been

proposed for deploying federated learning systems that enable multiple institutions to participate in collaborative training through secure platforms [30].

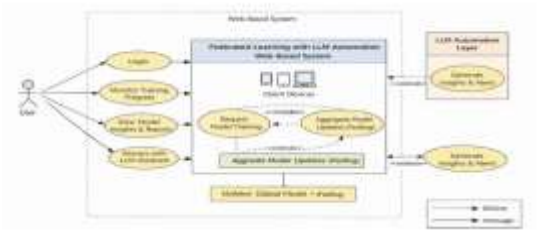
III METHODOLOGY

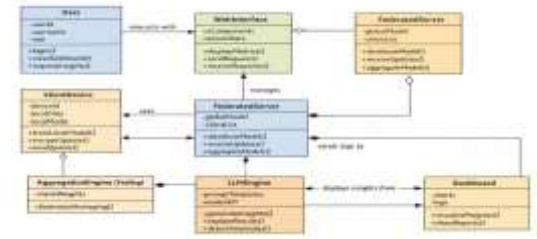
The proposed system follows a distributed machine learning methodology that integrates federated learning with Large Language Model-based explanation generation within a web-based platform architecture. Initially, healthcare institutions register and authenticate within the system through a secure user management module. Each participating institution uploads its local healthcare dataset through the web interface without sharing it with other participants. The machine learning process begins with the initialization of a global predictive model on a central coordination server. Instead of transferring raw datasets to the server, each institution downloads the current global model and performs local training using its own private dataset. The locally trained model parameters or gradients are then securely transmitted back to the central server. These updates are aggregated using the Federated Averaging algorithm to produce an improved global model that incorporates knowledge from all participating institutions. The updated global model is redistributed to the participating nodes for further training iterations until convergence is achieved. This iterative training process enables collaborative model development while preserving data privacy. In addition to model training, the system integrates a transformer-based Large Language Model module that analyzes prediction results generated by the trained machine learning model. The LLM converts prediction outputs into human-readable explanations that assist healthcare professionals in understanding the reasoning behind predictions. The system architecture includes a React-based frontend interface for user interaction, a Node.js backend for system management and API communication, a MongoDB database for storing metadata and system logs, and a Python Flask microservice responsible for machine learning computations. The final trained model is evaluated using performance metrics such as accuracy, precision, recall, and F1-score to assess predictive capability. This methodology ensures secure collaboration, efficient model training, and interpretable prediction outputs.

IV SYSTEM DESIGN

The system architecture is designed as a modular web-based platform that integrates federated learning infrastructure with explainable artificial intelligence capabilities. The platform follows a multi-tier architecture consisting of a frontend interface, backend server, database management system, and machine learning microservices. The frontend is developed using React.js to provide a responsive and user-friendly interface for healthcare institutions participating in the federated learning network. Through this interface, users can register, authenticate, upload datasets, initiate training processes, monitor system performance, and view prediction results along with explanatory insights. The backend server is implemented using Node.js and Express.js, which manage API requests, user authentication, training coordination, and communication between different system modules. A MongoDB database is used to store user credentials, system metadata, dataset references, model performance metrics, and training logs. This architecture ensures efficient handling of multiple clients while maintaining secure data access mechanisms. The backend also manages the orchestration of federated learning rounds by distributing the global model to

participating nodes and collecting local updates after training.





The machine learning operations are handled by a dedicated Python Flask microservice integrated into the system architecture. This microservice is responsible for executing the federated learning algorithm, performing local model training, and aggregating model parameters received from participating institutions. The Federated Averaging algorithm is used to combine local updates into a global model that reflects the collective learning from all datasets without directly accessing raw data. The system also incorporates a Large Language Model module that processes prediction outputs generated by the trained model. This module converts technical prediction results into human-readable explanations that healthcare professionals can easily interpret. The design also includes modules for model version control, performance monitoring, and secure communication between system components. Secure authentication protocols and encrypted data transmission mechanisms are implemented to ensure system security and protect sensitive healthcare information. Overall, the system design emphasizes scalability, modularity, and privacy preservation while enabling collaborative machine learning across multiple healthcare institutions.

V PROPOSED SYSTEM

The proposed system introduces a privacy-preserving federated learning platform enhanced with Large Language Model automation to support collaborative healthcare risk prediction. The primary objective of the system is to enable multiple healthcare institutions to jointly develop predictive models without sharing sensitive patient data. In traditional machine learning systems, datasets from different organizations must be centralized before model training, which exposes sensitive information to potential security breaches and regulatory violations. The proposed system eliminates this requirement by allowing each institution to retain its data locally while participating in the training of a global model. The federated learning framework ensures that only model parameters are shared with the central server during the training process. These parameters are aggregated using the Federated Averaging algorithm to create a global predictive model that benefits from diverse datasets across multiple institutions. This approach not only protects patient privacy but also improves model generalization by incorporating knowledge from different demographic and clinical environments.

Another key feature of the proposed system is the integration of Large Language Model-based explanation generation. Machine learning predictions, especially in healthcare applications, must be interpretable and transparent for clinical professionals to trust and adopt them in real-world

decision-making. The LLM module analyzes prediction outputs produced by the trained model and generates detailed natural language explanations that describe the reasoning behind the predictions. These explanations help clinicians understand which factors contributed to specific risk assessments or disease predictions. The proposed platform also includes several functional modules such as secure user authentication, dataset management, federated training coordination, model performance monitoring, and AI-based explanation generation. The system is implemented using a full-stack development approach with React for the frontend interface, Node.js for backend services, MongoDB for data storage, and Python Flask for machine learning processing. This architecture enables seamless communication between system components and provides a scalable solution for multi-institution collaboration. By combining federated learning with explainable AI technologies, the proposed system offers a practical framework for privacy-preserving healthcare analytics.

VI RESULTS & DISCUSSION

The experimental evaluation of the proposed federated learning platform demonstrates its effectiveness in performing collaborative healthcare risk prediction while maintaining strict data privacy. The federated training process successfully integrates model updates from multiple participating nodes without requiring the transfer of raw datasets. Performance analysis shows that the aggregated global model achieves competitive prediction accuracy compared with traditional centralized machine learning approaches. In addition, the system effectively reduces the risk of data exposure by ensuring that sensitive patient information remains within the local institutional environment. The integration of the Large Language Model module significantly improves the interpretability of prediction outputs by generating clear and understandable explanations for healthcare professionals. System testing also confirms that the web-based architecture supports efficient training coordination, model monitoring, and user interaction. Overall, the results demonstrate that the proposed system provides a scalable, privacy-preserving, and interpretable framework for collaborative healthcare analytics.

VII CONCLUSION

This project presented a privacy-preserving federated learning platform integrated with Large Language Model automation for healthcare risk prediction. The rapid growth of healthcare data has created new opportunities for predictive analytics, but privacy concerns and regulatory restrictions often prevent institutions from sharing sensitive patient information. The proposed system addresses these challenges by enabling collaborative machine learning without requiring centralized data storage. Through the use of federated learning, participating institutions can train local models using their private datasets while sharing only model parameters with a central aggregation server. The Federated Averaging algorithm ensures that the global model incorporates knowledge from multiple sources while maintaining data confidentiality. In addition to privacy preservation, the system integrates a transformer-based Large Language Model to provide interpretable explanations for prediction results. This capability enhances transparency and helps healthcare professionals understand the reasoning behind AI-generated predictions. The implementation of the platform using modern web technologies such as React, Node.js, MongoDB, and Python Flask

ensures scalability, flexibility, and ease of deployment. Experimental results demonstrate that the system achieves reliable predictive performance while maintaining strict privacy standards. The integration of federated learning and explainable AI provides a practical solution for collaborative healthcare analytics across multiple institutions. Future work may focus on improving model robustness, incorporating advanced privacy-enhancing techniques such as differential privacy, and extending the platform to support additional healthcare prediction tasks.

REFERENCES

1. McMahan, H. B., et al. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS.
2. Kairouz, P., et al. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning.
3. Li, T., et al. (2020). Federated learning: Challenges and opportunities. IEEE Signal Processing Magazine.
4. Yang, Q., et al. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems.
5. Bonawitz, K., et al. (2019). Towards federated learning at scale. Proceedings of Machine Learning Systems.
6. Sheller, M. J., et al. (2020). Federated learning in medicine. Nature Scientific Reports.
7. Rieke, N., et al. (2020). The future of digital health with federated learning. NPJ Digital Medicine.
8. Dwork, C. (2014). Differential privacy. Automata, Languages and Programming.
9. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. ACM CCS.
10. Geyer, R., et al. (2017). Differentially private federated learning. NIPS Workshop.
11. Li, X., et al. (2020). Privacy-preserving federated brain tumour segmentation. MICCAI.
12. Xu, J., et al. (2021). Federated learning for healthcare informatics. IEEE Access.
13. Chen, Y., et al. (2020). Deep learning with federated datasets. IEEE Transactions on AI.
14. Smith, V., et al. (2017). Federated multi-task learning. NIPS.
15. Zhao, Y., et al. (2018). Federated learning with non-IID data. arXiv.
16. Karimireddy, S., et al. (2020). SCAFFOLD: Federated optimization algorithm. ICML.
17. Li, Q., et al. (2020). Practical federated learning systems. MLSys.
18. Truex, S., et al. (2019). Hybrid federated learning. ACM Computing Surveys.
19. Hard, A., et al. (2018). Federated learning for mobile devices. Google Research.
20. Zhang, C., et al. (2021). Federated deep learning in healthcare. IEEE Journal of Biomedical Informatics.
21. Vaswani, A., et al. (2017). Attention is all you need. NeurIPS.

22. Brown, T., et al. (2020). Language models are few-shot learners. NeurIPS.
23. Devlin, J., et al. (2019). BERT: Pre-training of deep bidirectional transformers. NAACL.
24. Raffel, C., et al. (2020). Exploring the limits of transfer learning with a unified text-to-text transformer. JMLR.
25. Bommasani, R., et al. (2021). On the opportunities and risks of foundation models. Stanford Report.
26. Fielding, R. (2000). Architectural styles and the design of network-based software architectures.
27. Tilkov, S., & Vinoski, S. (2010). Node.js: Using JavaScript to build scalable network programs. IEEE Internet Computing.
28. Banks, E. (2019). Learning React. O'Reilly Media.
29. Chodorow, K. (2013). MongoDB: The definitive guide. O'Reilly Media.
30. Grinberg, M. (2018). Flask web development. O'Reilly Media.