Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(6):95-100

Research Article ISSN: 2394 - 658X

Collaborative Artificial Intelligence for Multi-Hospital Disease Risk Assessment Ensuring Patient Data Confidentiality

Abhishek Murikipudi

DEVAPPSIT LLC, USA

ABSTRACT

This report explores the integration of collaborative Artificial Intelligence (AI) in multi-hospital disease risk assessment preserving patient's data confidentiality, this report examines this integration. Hospitals can train collaborative AI models while keeping privacy-sensitive patient data at hospitals and complying with laws like HIPAA and GDPR applying the FL framework. The study discusses how privacy-preserving AI technologies can support compliance when working with collaborative model training. It also discusses the effects of including multiple healthcare center datasets from diverse patients on the accuracy and applicability of disease risk models. Finally, the report suggests best practices for secure federated learning frameworks in use in different hospital settings to strengthen disease risk assessment capabilities.

Keywords: artificial intelligence (AI), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), data privacy, Federated learning (FL), collaborative model, security, privacy

INTRODUCTION

The integration of collaborative "artificial intelligence (AI)" is a fundamental solution to the healthcare analytics problem in various hospital disease risk evaluations. Centralized data is applied by traditional AI-integrated models, and those are challenging regarding patient data security and regulations like "Health Insurance Portability and Accountability Act (HIPAA)" and "General Data Protection Regulation (GDPR)". Collaborative Learning particularly accelerates numerous healthcare organizations to collaboratively train AI models without access to the sensitive data of a patient and support data security measures while modifying the accuracy of AI models. This prototype shift is also determining the security issue, by pooling the wide-ranging dataset to provide more robust and generalized risk forecasts for disease based on that. Collaborative AI ensures that patient privacy is maintained while applying decentralized information processing to offer the most efficient and equitable healthcare solutions.

Aim

The aim of the research is to investigate how the workflow of collaborative AI technologies and federated learning can increase disease risk forecasting across various hospitals while maintaining patient-sensitive data security and agreement with rules and regulations like ‘GDPR’, 'And HIPAA'.

Objectives

- To examine the function of federated learning in facilitating multi-specialty hospital cooperation for disease risk assessment while enabling limited use of patient data
- To evaluate the efficiency of data security-preserving AI technologies in managing compliance with healthcare rules and regulations at the time of collaborative model training.
- To analyze the effects of adding high-volume datasets of patients from numerous healthcare centers on the accuracy and applicability of disease risk models.
- To recommend best practices for integrating effective and secure federated learning frameworks into numerous hospital settings to increase disease risk assessment abilities.

Research Questions

- What is the process of examining the federated learning in accelerating multi-specialty hospital cooperation for disease risk assessment while enabling limited use of patient data?

● How can to evaluate the effectiveness of data security-preserving AI technologies in managing compliance with healthcare rules and regulations at the time of collaborative model training?
● How to analyze the effects of adding high-volume datasets of patients from numerous healthcare centers on the accuracy and applicability of disease risk models?
● What are the proposals of best practices for integrating effective and secure federated learning frameworks into numerous hospital settings to increase disease risk assessment abilities?

RESEARCH RATIONALE

Multi-hospital disease risk assessment is an impending future requirement in healthcare analytics. AI can resolve this issue by enabling institutions to collectively train predictive models without accessing sensitive patient data in healthcare analytics [1]. The challenges to deal with the issues in healthcare patient data management are regulatory compliance, data privacy concerns, and large as well as huge amounts of datasets for better prediction with the help of this methodology. In this context, federated learning is a significant technology that secures the structure of robust AI models without adjusting patient privacy and it can enhance the trust of shareholders and strengths of disease risk forecasting across various hospital settings [2]. The result of this approach reduces security risk and strengthens innovation in disease prediction and customized treatment strategies for each patient applying decentralized data processing.

LITERATURE REVIEW

Key Approaches for Enabling Multi-Hospital Cooperation Without Outsourcing Sensitive Patient Data

Innovative methods for maintaining patient data confidentiality are significant in collaborative artificial intelligence (AI) depending on multi-hospital disease risk assessment. The capability to train AI models collaboratively by organizations without outsourcing sensitive patient data fosters Federated learning. The data is owned by individual hospitals and the model is updated at each hospital. Though there are no privacy concerns at each hospital, as well as observing rules and regulations such as “HIPAA” and “GDPR” [3]. Ultimately, FL frameworks are also integrated with numerous privacy policies and secure multi-party computation to strengthen privacy.

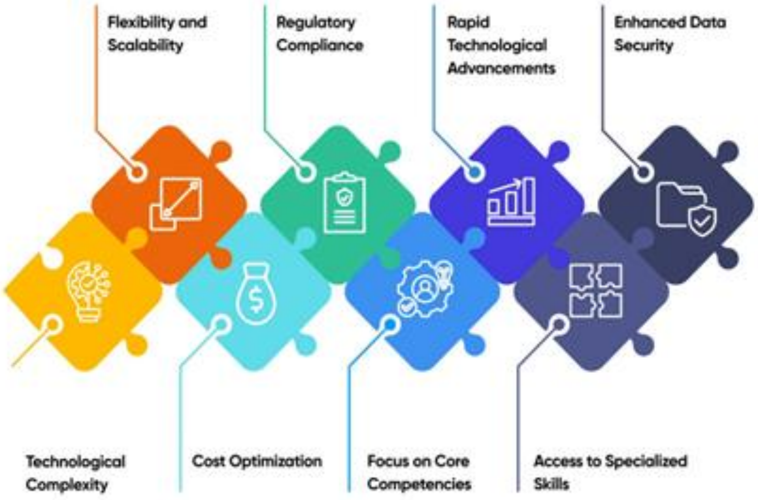
Flexibility and Scalability
Regulatory Compliance
Rapid Technological Advancements
Enhanced Data Security
Technological Complexity
Cost Optimization
Focus on Core Competencies
Access to Specialized Skills

Figure 1: Factors for outsourcing Healthcare IT Outsourcing

These methods of FL framework are meant to add volume to information or computations while providing some data about the original data that is being trained to be applied for structuring but without revealing patient information [4]. Real-world implementations of Multi-Hospital Cooperation, such as the coordination among 20 global organizations to forecast COVID-19 patient progress, represent the feasibility and efficiency of these approaches. Hospitals can increase disease risk assessment abilities while following privacy measures of patient data by strengthening FL and associated privacy-preserving technologies.

Data-Protected AI Technologies Assure Compliance with Healthcare Rules During Model Training

The privacy of the patient's sensitive data must be secured in collaborative artificial intelligence (AI) for multi-hospital disease risk assessment. Federated learning (FL) permits numerous healthcare institutions to train a single AI model together by sharing no patient data [5]. This position is consistent with HIPAA and GDPR that guide patient information. FL can mitigate privacy risks and comply with data protection regulations because if the local data only sends model updates, there is no requirement to outsource the data [6]. Moreover, the training of the model is further secured by combining privacy-preserving techniques like differential privacy, so that individual patient information remains confidential while helping to develop robust disease risk models.

Implementing Diverse Patient Datasets Increases the Applicability and Accuracy of Disease Risk Models

The durability and generalizability of disease risk prediction models are enhanced by implementing numerous patient datasets from numerous healthcare institutions. FL accelerates the implementation by allowing training of collaborative models without the requirement to outsource sensitive patient data, by following security measures. The application of diverse patient datasets to collaboratively learn disease risk models is implemented toward enhancing the applicability and accuracy of disease risk models by learning across multiple healthcare institutions [7].

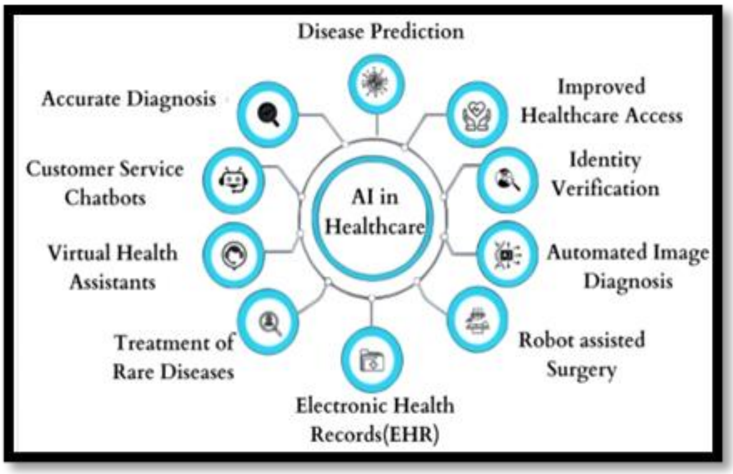
Disease Prediction
Improved Healthcare Access
Identity Verification
Automated Image Diagnosis
Robot assisted Surgery
Electronic Health Records(EHR)
Treatment of Rare Diseases
Virtual Health Assistants
Customer Service Chatbots
Accurate Diagnosis
AI in Healthcare

Figure 2: Role of AI in healthcare

It has been shown that FL modifies the model performance compared to local models with a 6% improvement on the area under receiver operating characteristic of the curve with diverse patient data Analysis has showcased that FL models trained on information from multiple sources exceed, guiding to modified accuracy in forecasting clinical outputs like acute kidney injury and sepsis [8]. For example, an adaptive "FL" framework used to compute health records from numerous hospitals represented a massive modification in prediction performance compared to local data models. Additionally, the capability of FL to tackle data diversity across multiple organizations ensures that the generated models are more useful across multiple patient populations.

Integrating Secure Federated Learning Frameworks modifies disease Risk Assessment abilities. 150

Federated learning technology associates healthcare organizations with better disease risk approximation while keeping the data of patients secure across multiple hospitals. Hospital networks train AI models together by applying their data sets which follow both HIPAA and GDPR rules [9]. The systems can predict diseases more accurately thanks to their ability to use medical data from different healthcare organizations. The secure framework of federated learning enables healthcare experts to base their decisions on complete protected patient insights which enhance medical treatment at the individual level [10]. For example, the APPFLx framework accelerates high-volume, cost-efficient collaboration in biomedical instrument studying projects, ensuring the sensitive data of patients remains private while increasing model efficiency and applicability.

Literature Gap

Most research on FL in multi-hospital disease risk assessment examines theoretical approaches and one application only. The scientific community requires large-scale practical research on FL execution at multiple healthcare sectors of organizations because present studies do not resolve challenges with inconsistent medical data and incompatible IT systems. Reports require more practical research into the workflow of security methods with advanced FL tools in actual healthcare settings. Institutions cannot build top-level AI systems for disease risk prediction because of this missing link in this research.

METHODOLOGY

This report follows "Secondary data sources" because detailed information from publications, studies, and reports exists about collaborative artificial Intelligence for multi-hospital disease risk assessment ensuring patient data in the healthcare management sector. The existing report examines this method that fosters best practices for integrating effective and secure federated learning frameworks into numerous hospital settings [11]. Secondary data is a useful data source in this report due to ultimate privacy policies and secure multi-party computation of the FL framework and the effectiveness of data security-preserving AI technologies. The researcher selected “interpretivism philosophy” because it aims at evaluating the usages of diverse patient datasets to collaboratively learn disease risk models [12].

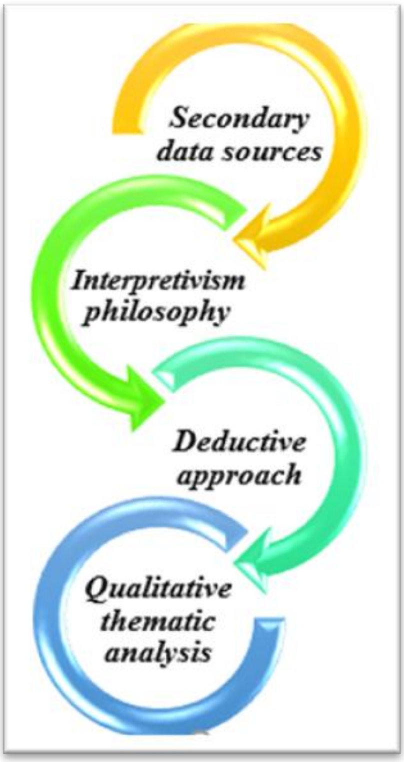

Figure 3: Methodology

The interpretivist philosophy investigates the provisional meaning of Collaborative Artificial Intelligence for Multi-Hospital Disease Risk Assessment. The selected approach has singular significance in investigating complicated phenomena developed through social interactions within technological environments. This report applies a **deductive approach** to evaluate the most applicable approaches to best practices of Collaborative Artificial Intelligence. The existing report supervises the developed modification of a starting theorem that is approved by evaluating secondary information sources. The collected information in this report goes through "**Qualitative thematic analysis**” that enables researchers to determine and analyze major themes together with a unique pattern to collaborate with AI for Multi-Hospital Disease Risk Assessment [13]. The thematic analysis utilizes this analysis method because it offers a comprehensive analysis of the qualitative clues concerning the collaboration of Artificial Intelligence for multi-hospital disease risk assessment. Data patterns in the gathered information qualify researchers to demonstrate significant findings about best practices and challenges along with innovations within collaborative Artificial Intelligence to ensure patient data confidentiality.

DATA ANALYSIS

Theme 1: Function of Federated learning in securing inclusive hospital coordination for disease risk assessment while ensuring restricted application of patient data.

Federated Learning provides healthcare systems with a way to combine disease risk assessments from many hospitals through its collaborative structure while protecting patient privacy. The FL technology enables different hospitals to train AI models while maintaining patient data privacy regulations at their locations [14]. The system keeps patient information protected in each medical facility which prevents possible threats from centralizing patient data storage. Multi-specialty hospital FL setups enable the joining of different patient data to make disease risk models more resistant to errors across different patient populations [15]. Hospitals can participate in the shared model development process by giving their local medical records for training and then sharing the updated model instead of raw patient data. In this context, the method is associated with securing patients' privacy and associating healthcare groups to build better medical observations together during the work on predictive models.

Federated Learning platforms work best with advanced methods to maintain the privacy of patient data involving private systems and secure numerous data-sharing tools. The security integrations make it impossible for anyone to put together patient information from the updated sharing models [16]. These connections allow organizations to meet their legal obligations to protect patient data as specified in HIPAA and GDPR.

Theme 2: Efficiency of confidentiality-focused AI techniques in preserving compliance with patient safety protocols during collaborative AI model training.

Organizations use distributed learning technology and follow strict medical and personal data protection rules to build joint disease risk analysis tools across multiple healthcare facilities. FL distributes training processes to different hospitals keeping patient data stored in separate locations [17]. Multiple hospitals can team up to make AI models through this method which keeps patient information private according to law. Homomorphic encryption and differential privacy including high-level encryption methods protect patient information all over the training sessions. Data samples receive intentional distortions under differential privacy which protects patient identities better than homomorphic encryption does even though encrypted calculations happen on those samples.

The actual use of several healthcare facilities working together shows these privacy-preserving AI systems work correctly in practice. The combination of federated learning with secure privacy methods shows great promise as a way for multiple hospitals to work together in disease risk assessment [18]. Developers build AI systems associated with healthcare regulations and maintain the privacy of the patient increasing medical options for the patient.

Theme 3: The effects of combining various patient datasets from numerous medical centers on the perfection and relevancy of disease risk models.

Combined patient data from many healthcare centers helps make disease risk models more precise and helpful by using FL training methods. FL facilitates AI training by several healthcare organizations with patient data protection through secure data sharing [19]. AI systems produce better predictions across different types of patients by processing medical and patient information from many different healthcare centers. Large-scale datasets are associated to determine the patterns that each hospital avoids assisting better predictions in multiple healthcare populations. Research shows that FL models trained with information from 20 organizations globally returned better medical projections explicitly for COVID-19 patient oxygen than models applying only local data systems. Technically gathering healthcare center data resolves both data inequality and majority patient representation issues [20]. FL combines healthcare data from different sources to make models that benefit a larger variety of patients and provide equal opportunities in healthcare delivery. Applying federated learning both disease risk models work better and cover all population groups by integrating patient data from multiple healthcare centers. In summary, the implementation of large datasets through federated learning increases the perfection of disease risk AI models and widens their applicability at the same time ensuring that predictive tools are more efficient and relevant to the normal population.

Theme 4: Best practices to implement secure federated learning frameworks across numerous hospital settings for enhancing disease risk assessment abilities.

To protect patient data in FL systems used by multiple hospitals you must follow security standards that keep information private and models working as intended. The methods protect patient privacy and guarantee legal compliance with healthcare rules including HIPAA and GDPR when applied to FL training systems.

To maintain security patients, need advanced identity controls and protected model sharing protocols. APPFLx framework helps secure and encrypt data exchanges between various healthcare facilities which builds better trust levels among academic partners [21]. The strategy needs to handle different data types. FL frameworks that adapt to different data patterns across institutions show better model results and transferability from experiments on clinical risks across multiple facilities. FATE and Open FL create customizable secure platforms with features for deploying FL models that develop institutions' personalized solutions. Healthcare organizations that follow these rules can build secure federated learning frameworks and work with others better to check disease risk.

FUTURE DIRECTIONS

Proactive tools like AWS X-Ray can play a big role in detecting issues in the multi-hospital disease risk assessment framework. These tools enable real-time monitoring, monitoring, and feedback to the problem itself rather than that of the collaborators, which enables the problem to be identified before it escalates to the point of failing the collaborative efforts [22]. In addition, the incorporation of state-of-art privacy protection mechanisms such as differential and secure multi-party computation, can enhance data privacy of patients, consistent with the HIPAA or GDPR standards. This integration achieves not only higher efficiency and flexibility of disease risk assessments but also enables a more secure and compliant collaborative environment.

CONCLUSION

In conclusion, federated learning frameworks turn out to be a transformative means to integrate collaborative artificial intelligence (AI) and to perform multi-hospital disease risk assessment with privacy conditions guaranteed at the patient's level. At the same time, these frameworks allow hospitals to mutually train AI models without patients' sensitive data by keeping technical information there. A more sophisticated piece of algorithms is also added such as differential privacy and homomorphic encryption to make data more secure. The advent of the digital age has brought forth healthcare systems that are moving towards embracing digital transformation to develop disease risk assessment capabilities while always safeguarding patients 'privacy.

REFERENCES

[1]. Vyas, A., Abimannan, S. and Hwang, R.H., 2021. Sensitive Healthcare Data: Privacy and Security Issues and Proposed Solutions. Emerging Technologies for Healthcare: Internet of Things and Deep Learning Models, pp.93-127.

[2]. Uddin, S., Haque, I., Lu, H., Moni, M.A. and Gide, E., 2022. Comparative performance analysis of K-nearest neighbor (KNN) algorithm and its different variants for disease prediction. Scientific Reports, 12(1), p.6256.

[3]. Voss, W.G. and Houser, K.A., 2019. Personal data and the GDPR: providing a competitive advantage for US companies. American Business Law Journal, 56(2), pp.287-344.

[4]. Tayefi, M., Ngo, P., Chomutare, T., Dalianis, H., Salvi, E., Budrionis, A. and Godtliebsen, F., 2021. Challenges and opportunities beyond structured data in the analysis of electronic health records. Wiley Interdisciplinary Reviews: Computational Statistics, 13(6), p.e1549.

[5]. Kumar, Y. and Singla, R., 2021. Federated learning systems for healthcare: perspective and recent progress. Federated learning systems: Towards next-generation AI, pp.141-156.

[6]. Hartzog, W. and Richards, N., 2020. Privacy's constitutional moment and the limits of data protection. BCL Rev., 61, p.1687.

[7]. Sheller, M.J., Edwards, B., Reina, G.A., Martin, J., Pati, S., Kotrotsou, A., Milchenko, M., Xu, W., Marcus, D., Colen, R.R. and Bakas, S., 2020. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Scientific reports, 10(1), p.12598.

[8]. De Hond, A.A., Steyerberg, E.W. and Van Calster, B., 2022. Interpreting area under the receiver operating characteristic curve. The Lancet Digital Health, 4(12), pp.e853-e855.

[9]. Edward, A., 2020. AI-Enhanced IAM Strategies for Ensuring HIPAA and GDPR Compliance in Healthcare.

[10]. Nguyen, D.C., Pham, Q.V., Pathirana, P.N., Ding, M., Seneviratne, A., Lin, Z., Dobre, O. and Hwang, W.J., 2022. Federated learning for smart healthcare: A survey. ACM Computing Surveys (Csur), 55(3), pp.1-37.

[11]. Kumar, Y. and Singla, R., 2021. Federated learning systems for healthcare: perspective and recent progress. Federated learning systems: Towards next-generation AI, pp.141-156.

[12]. Zhang, A., Xing, L., Zou, J. and Wu, J.C., 2022. Shifting machine learning for healthcare from development to deployment and from models to data. Nature Biomedical Engineering, 6(12), pp.1330-1345.

[13]. Varley, P.R., Borrebach, J.D., Arya, S., Massarweh, N.N., Bilderback, A.L., Wisniewski, M.K., Nelson, J.B., Johnson, J.T., Johanning, J.M. and Hall, D.E., 2021. Clinical utility of the risk analysis index as a prospective frailty screening tool within a multi-practice, multi-hospital integrated healthcare system. Annals of surgery, 274(6), pp.e1230-e1237.

[14]. Rustad, M.L. and Koenig, T.H., 2019. Towards a global data privacy standard. Fla. L. Rev., 71, p.365.

[15]. Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H.R., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B.A., Maier-Hein, K. and Ourselin, S., 2020. The future of digital health with federated learning. NPJ digital medicine, 3(1), p.119.

[16]. Sheller, M.J., Edwards, B., Reina, G.A., Martin, J., Pati, S., Kotrotsou, A., Milchenko, M., Xu, W., Marcus, D., Colen, R.R. and Bakas, S., 2020. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Scientific reports, 10(1), p.12598.

[17]. Antunes, R.S., André da Costa, C., Küderle, A., Yari, I.A. and Eskofier, B., 2022. Federated learning for healthcare: Systematic review and architecture proposal. ACM Transactions on Intelligent Systems and Technology (TIST), 13(4), pp.1-23.

[18]. Lloyd-Jones, D.M., Braun, L.T., Ndumele, C.E., Smith, S.C., Sperling, L.S., Virani, S.S. and Blumenthal, R.S., 2019. Use of risk assessment tools to guide decision-making in the primary prevention of atherosclerotic cardiovascular disease: a special report from the American Heart Association and American College of Cardiology. Journal of the American College of Cardiology, 73(24), pp.3153-3167.

[19]. Jin, H., Luo, Y., Li, P. and Mathew, J., 2019. A review of secure and privacy-preserving medical data sharing. IEEE Access, 7, pp.61656-61669.

[20]. Paulus, J.K. and Kent, D.M., 2020. Predictably unequal: understanding and addressing concerns that algorithmic clinical prediction may increase health disparities. NPJ digital medicine, 3(1), p.99.

[21]. Marks, J.H., 2019. The perils of partnership: industry influence, institutional integrity, and public health. Oxford University Press.

[22]. Andriole, K.P., 2022. SPIE medical imaging 50th anniversary: history of the picture archiving and communication systems conference. Journal of Medical Imaging, 9(S1), pp.S12210-S12210.