RESEARCH ARTICLE

Federated Neural Learning Techniques for Enhancing Privacy and Security in Distributed Healthcare Data Processing and Management

Fajar Rao[1,*]

[1] Faculty of Engineering, University of Sydney, Sydney, NSW, Australia

Abstract

The quick rate at which healthcare has accepted digital technologies has generated several sensitive medical record data. Though this data has huge potential for innovative medical research and personalized things in health care, it also brings with it a huge future worry for the safety and privacy of patients. Protection of sensitive patient data access is the main obstacle of our time; thanks to Federated Learning (FL) companies in these fields are not only reviewing data for fraud control but also are using this data for planning cancer treatment. This paper narrated FL to be the core technology used in solving the most important privacy and security issues with the health information-sharing process. Among the main contributions is a thorough analysis of the state of the overall application of FL in healthcare together with the presentation of the basic technical principles of FL as well as the listing of the same FL's communication overhead, model inaccuracies, and adversarial attacks. In addition, the paper states possible solutions in the improvement of FL's robustness like the ones provided by the inclusion of the state-of-the-art security measures such as secure aggregation, differential privacy as well as blockchain integration. The results reveal the prospect of FL transforming healthcare data management into a secure framework for rapid innovation and also maintaining strict privacy compliance.

Keywords: federated learning, healthcare, data privacy, security, machine learning.

1 Introduction

The healthcare sector has undergone a profound transformation with digital technologies emerged that facilitated the access, storage, processing as well as rich analysis of patients' data. Apart from the chances to refine personalized medical treatment, forecasting illnesses, and enhancing healthcare provisions, patients' data, collected from EHRs, wearable devices, medical imaging systems, and other sources, is boundless. Nevertheless, the sensitive nature of the healthcare data raises serious concerns regarding privacy, security, and compliance with legal regulations such as the General Data Protection Regulation (GDPR) and the Health

Submitted: 01 June 2025
Accepted: 20 June 2025
Published: 26 June 2025

Vol. 1, **No.** 2, 2025.
10.62762/TNC.2025.356075

***Corresponding author:**
✉ Fajar Rao
frao9131@uni.sydney.edu.au

Citation
Rao, F. (2025). Federated Neural Learning Techniques for Enhancing Privacy and Security in Distributed Healthcare Data Processing and Management. *ICCK Transactions on Neural Computing*, 1(2), 78–86.

Insurance Portability and Accountability Act (HIPAA). Therefore, there is an urgent requirement for methods that can ensure the usage of healthcare data while protecting patient confidentiality [1, 2].

Classical machine learning techniques require the coalescence of data into a centralized repository before training, which enhances the likelihood of leakage or unauthorized access. In circumstances where the risks could be catastrophic because of the delicacy of the information, the conventional way of data acquisition is losing its efficacy. Federated Learning (FL) breaks the mold as it empowers interactive machine learning along decentralized data sources. The use of FL means that instead of raw data being relayed to a central site, applications are performed locally. At each source of data, local models are adjusted and only the collective parameters or updates are sent to a central server. This ingenuity ensures that personal information is kept in-house and consequently, these sorts of privacy concerns that often arise that are put to rest without forfeiting the acquisition of collective intelligence [3, 4].

In the healthcare field, the potential of federated learning (FL) is quite substantial. To provide hospitals, research facilities, and pharmaceutical companies with a better detection rate, a predictive model needs to be developed with no or minimal face-to-face interaction. As an illustration, several kinds of data can be integrated and evaluated through FL, making it possible to build the necessary models for diseases, predict the effectiveness of medicines, and forecast outbreaks. So, it is possible to deliver clinical models of greater scope and robustness that mirror the distinctions among humans in different regions of the globe through such cooperation. However, the barriers posed by federated learning (FL) within the healthcare sector remain considerable. Issues included long-distance communications, variability in data between companies, and potential cyberattacks could compromise the integrity of the models. They need to be adequately addressed for FL to be fully effective in this area [5–7].

One of the major advantages of federated learning (FL) is its compatibility with privacy-preserving technologies such as differential privacy and secure multilayer computation. Through differential privacy, the collection of the updates takes place in such a way that it cannot serve the identification of data points. On the other, the computation of several parties together by secure multiparty computation is made possible without revealing the underlying knowledge. Since both these methods are used, the FL systems will be secured and relevant enough for the healthcare sector that has to comply with strict privacy regulations. Besides, the pairing of FL with technologies like blockchain can be applied to give an extra layer of protection to the data that is vital in preserving the patient's confidentiality through the integrity of data ensuring the accuracy of transactions and ensuring the ability to track them and recover them [8, 9].

Services of health care will boost by means of artificial intelligence (AI) and machine learning (ML) and will result in a more major manner. AI and ML tools can be used to mine large databases—for example, patient records—to come up with predictions of diseases and categorize them into high and low risk. Moreover, these analytical tools also play the role of predicting who are likely to be the candidates for medical needs to be planned in advance. So these analytical tools can help deliver efficient healthcare by guiding doctors on how many patients to treat and which procedures to do based on patient demographics and risk status [10]. Thus, information on risk factors serves as the input for AI and ML-based healthcare systems and the underlying health care system is analyzed to get a better grasp of the potential complex future risks. Choosing the trained AI or ML model that best fits the right data generating process to be expected in the future is a critical step in this approach [11, 12].

In addition, the public's artificial intelligence (AI) acceptance level is unlikely to be stable. Previous studies also raise a concern about the level of AI implementation that will gain public acceptance in the future and that there might be a constant flux of AI acceptance levels in the future [13]. Among the main factors that are known to have a direct impact on AI acceptance are age and gender, as younger individuals. having an intermediate level of education appear to be very open towards the adoption of AI in healthcare, while higher levels of education are not necessarily linked to AI acceptance. Therefore, younger individuals have become the early adopters of AI tools in the healthcare market. Moreover, the introduction of these tools in the educational curriculum should encourage even more people to use them. But the approach should be different for different groups of the population. By introducing AI through programs such as "Digital Unite" at a younger level, there is hope that young people will continue to use them even in professional areas at a later stage [14, 15].

The objectives of this study are as follows:

- To explore the possibilities of Federated Learning as a privacy-preserving collaborative machine learning methodology in healthcare.
- To investigate and recommend strategies to the technical and operational issues related to the implementation of Federated Learning in healthcare settings.

The paper will provide both a comprehensive survey of Federated Learning in healthcare and an account of the applications, problems, and the future of this technology. By exploiting FL, the healthcare sector will achieve a balance between innovation and privacy, empowering the development of transformative technologies that improve patient outcomes while protecting sensitive data. The following sections will go into the nitty-gritty details of the FL technology, its incorporation with privacy-preserving methods, and its capability in addressing the imperative challenges in present-day healthcare.

2 Related Work

In this section, we will highlight the contributions made by key studies in the field as well as point out the gaps that this research intends to address (see Table 1). Over the years, the use of Federated Learning (FL) in healthcare has gained a fair amount of attention because it has been regarded as an innovative technique to address the privacy and security challenges that are associated with sensitive patient data. FL is a decentralized model of machine learning where the data remains at the source, thereby encouraging the participating healthcare institutions to collaborate in a privacy-preserving way. The studies in this field have looked into different issues including the technical implementation of FL, its integration with Privacy-Enhancing Technologies (PETs), and its applications in healthcare scenarios such as disease prediction, personalized medicine, and outbreak monitoring. In this section, we will highlight the contributions made by key studies in the field as well as point out the gaps that this research intends to address.

Rauniyar et al. [16] explored the usability of FL in medical fields, particularly for global cancer detection. Their research indicates that FL can effectively address the security and privacy issues of decentralized model training involving only model learning without sharing any data. The study specifies the most critical issues being the device-related ones, the statistical problems to be solved, and privacy matters and demonstrates at the same time that the FL method can deliver reliable results and that adaptability in medical diagnostics is also possible. The current review identifies areas for future research and recommends FL to be an important factor of innovative data-driven healthcare.

Sinaci et al. [17] developed a federated ML architecture to allow for the use of FAIR health data by various stakeholders. Their privacy-preserving method was able to build the model in such a way that many healthcare entities were able to work together without sharing sensitive data. The federated model which was the result of collaboration among five healthcare organizations was reported to have reached a prediction accuracy of 87% for the readmission of patients suffering chronic obstructive pulmonary disease. Therefore, this research confirms the crucial role of FAIR datasets in the implementation of federated ML and the future perspectives of ensuring privacy/data protection while at the same time the consortiums use predictive modelling for new drugs, etc. are brought forth. Thus, this study illustrates the importance of using FAIR datasets that respect privacy while allowing collaboration in the prediction of complex diseases.

Messinis et al. [18] have effectively summarized the application of AI in the security of IoMT systems. Their study addresses the integration of ML and DL as they look to improve the performance, reliability, and speed of security protocols. They have discussed several methods, including blockchain, anomaly detection, and federated learning, among others. These experts also illustrated that these innovations could bolster the security mechanism of IoMT and thus protect the sensitive data of individuals. The authors wrapped up their findings with suggestions for future studies like investigating how AI acts as an enabler for IoMT vulnerability mitigation and how the privacy of IoMT can be enriched by AI.

Alsamhi et al.'s [19] introduced a novel solution that is a blend of both federated learning or blockchain-based systems as well as a secure decentralized data sharing approach in the health sector. They have proven that the combination of the two methods allows patients' privacy to be maintained while the health sector can, at the same time, use a wide range of data sets for the training of precise diagnostic models. By merging the decentralized learning abilities of FL and

Table 1. Comparison of federated learning approaches in medical applications.

Study	Objective	Methodology	Key Findings	Challenges
Rauniyar et al. [16]	Explore FL for medical applications.	Reviewed FL trends in decentralized diagnosis.	FL models are scalable, robust, and generalizable.	Privacy and device issues persist.
Sinaci et al. [17]	Use FAIR data for federated ML models.	Developed privacy-preserving FL framework.	Achieved 87% accuracy in readmission prediction.	Challenges in FAIR data transformation.
Messinis et al. [18]	AI-driven IoMT cybersecurity review.	Reviewed AI solutions like FL and blockchain.	Improved IoMT device security and reliability.	Gaps in AI-based IoMT security remain.
Alsamhi et al. [19]	Combine FL and blockchain for data sharing.	Proposed FL-blockchain framework.	Enhanced privacy and accurate diagnostics.	Technical integration hurdles.
Bhatt et al. [20]	FL-based stroke prediction model.	Developed ANN-based FL architecture.	Achieved 5–10% higher accuracy than traditional.	Limited real-world applicability.

the transparency of blueprints, the latter are pushed to medical research and the former are used in the wider range of treatments that patients receive safety in patient management. Patients are expected to be treated with new methodologies along with the promise of privacy and trust which is the guarantee of a system based on patient data.

Bhatt et al.'s [20] led to a new AI approach for a stroke prediction system using federated learning (FL). The researchers proposed a thick ANN algorithm that is capable of executing processed input data based on an ANR-based stroke text data set and it is also intended to be on health appliances. The inclusion of 5G communications in the collection of weights make the architecture super high precision, accuracy, and recall compared to classic systems. The article further demonstrates a simple and easy-to-follow guide to the healthcare sector concerning the FL techniques, as the scholars intend to be the quickest and most efficient solution to the provision of equitable health services for all.

In summary, the studies discussed in this section highlight the significant contributions and ongoing challenges in the application of Federated Learning (FL) in healthcare. FL has shown promise in addressing privacy and security concerns by enabling collaborative model training without the need to share sensitive patient data. The research emphasizes FL's potential in areas such as disease prediction, personalized medicine, and the integration of privacy-enhancing technologies like blockchain. However, key challenges remain, including device-related issues, data transformation complexities, and the need for seamless integration with existing healthcare systems. These studies also illustrate the importance of using FAIR data and secure decentralized data-sharing methods to foster collaboration across healthcare entities. Future research should continue to explore the optimization of FL techniques for more precise diagnostics, improved security mechanisms for Internet of Medical Things (IoMT) systems, and the scalability of FL models for real-world applications. This section demonstrates the evolving landscape of FL in healthcare and underscores the need for further advancements to fully realize its potential in improving patient outcomes and healthcare services.

3 Methodology

The process involved in the realization of a Federated Learning (FL) system in healthcare ensures the privacy, security, and optimum use of sensitive patient data across various institutions. In this study, decentralization of collaborative machine learning has been chosen as the base of the new model, which enables hospitals, clinics, and other research organizations to participate in the model development without the need for data consolidation. The scheme involves the FL principles where the data remains at the source, thus it enables secure data processing and the legislation compliance regulation of privacy is improved. The methodology section describes the main elements of the FL framework, the integration of privacy-preserving technologies, and the processes like the aggregation and optimization of models. Also, it explains how all these parts can synchronize to guarantee the data integrity, security, and model accuracy.

The data collected by different institutions, such as hospitals, clinics, and research centers, in the healthcare domain is usually heterogeneous either in structure or format. The difference in data structure as a barrier to the possibility of centralized machine learning is. The main functions of a FL model are meeting the requirement of varied inputs and working with heterogeneous data sources, through the localized training of each of the participating institutions. A local node is a representation of each institution, which conducts its own model training on its respective data, in this way, the patient information is kept illegal while also the computing operations cost associated predominately by data transfer, are alleviated. Hence, in this process, it is not the actual data that is shared but just the model parameters that are, creating a global model without leaking any private information.

The adherence to robust privacy standards is guaranteed in the suggested FL system by integrating privacy-preserving technologies such as distribution of statistics to keep an eye on discrimination. Encryption ensures that data streams are untouchable for the abuser. Due to the introduction of statistical noise through the differential privacy method, aggregated data cannot be used to deduce the characteristics of individual data points. This technique is a necessity in health establishments since even minor breakdowns of privacy can result in serious harm. Moreover, secure multiparty computation permits the encrypted execution of operations, allowing often oppressive functions to be performed without telling the participants the details of the data. In this program, the FL model is indirectly influenced by data privacy using these mechanisms throughout the process of training.

The communication efficiency issue that this proposed FL model is addressing is an essential aspect to keep updates performed immediately, so the resources don't consume excessively. For this reason, federated sum for aggregate function is used accordingly, which means the local trained models are brought together by each institution. The merging of these models takes place in a centralized server that steps in at the data collection point, collects the model updates from each of the nodes participating, and an overall model is created. In a way, the individual local models are regularly updated and the combined global model is given back to all institutions where each of them can have the model updated again. This kind of protocol minimizes the size of the data which is sent, thus decreasing the communication expenditure and consequently making it possible for a huge number of organizations to be involved in such an initiative.

Healthcare organizations have data that varies from one organization to another. The proposed method takes this variation into account. The incorporation of preprocessing procedures for standardizing data features, while keeping the local context is an example of how technology can address differences in data formats. For instance, different hospitals may use various coding systems in the diagnosis and treatment of diseases. With the FL framework, each medical institution can keep its unique data structure while still contributing to the general model. The model upscale is accomplished by the domain adaptation technique that aligns features across institutions to ensure that the model has both accuracy and generalization. This technique allows the model to be flexible by accepting various kinds of healthcare data, thus also achieving excellent performance in the diverse environment and different populations.

Cybersecurity is a huge concern in the proposed FL model, especially against attacks from hackers. Since healthcare data is very confidential, there is a chance that adversaries will try to feed the model malicious updates to the model by submitting them. Therefore, the system can use strong aggregation methods to detect and remove incorrect updates, ensuring that only real data input will be utilized in the global model. Moreover, such techniques are also applied to the aggregation process through machine learning algorithms in order to flag outliers which in turn helps in establishing another security layer. These safeguards not only help to achieve the model's overall accuracy but they also ensure its secure and trustworthy predictions are actually given.

Furthermore, mechanisms are needed by the FL training process to deal with convergence and model accuracy because of its iterative nature. Since each institution might have data of different volumes and types, the system uses adaptive learning rates and weighted averaging during aggregation variability. These techniques help to balance the contributions that come from each node so that smaller universities do not excessively skew the global model. The diversity in the data profiles of healthcare institutions using this approach ensures that it is more likely to converge and at the same time achieving higher accuracy.

In the suggested model, the performance of the models will be evaluated periodically to ensure that they are being continuously improved. The global model will be downloaded by each institution to other datasets on their local site. Thus, researchers will have a good idea of whether or not this generic product works for particular healthcare systems. The results of these

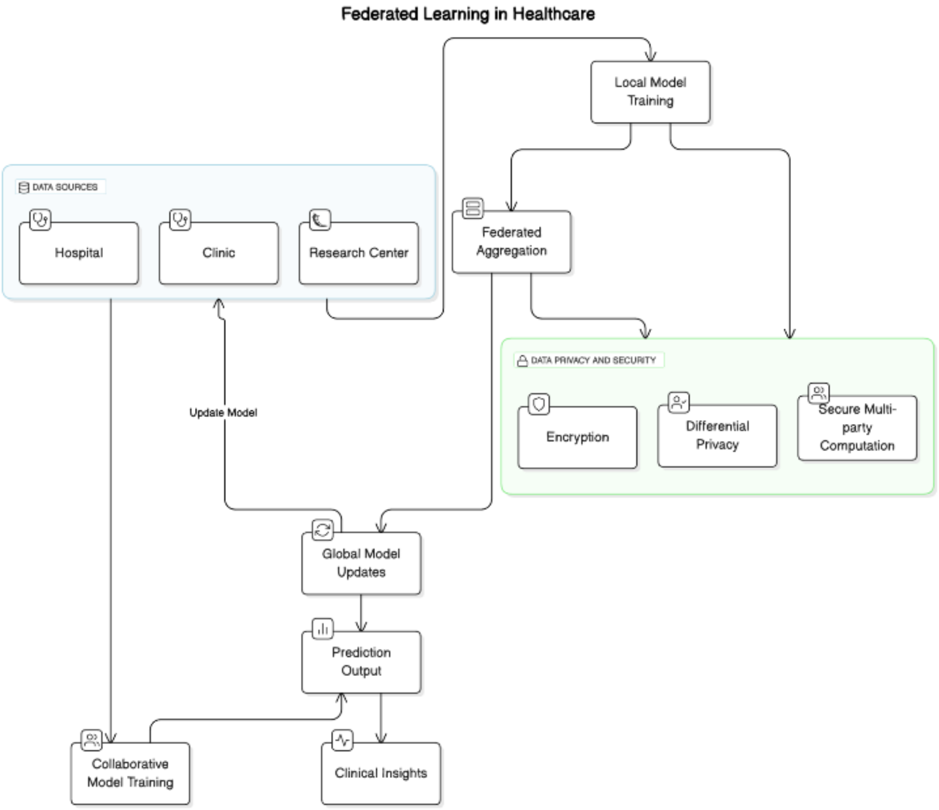

Figure 1. Detailed workflow of the proposed model.

evaluations back to development business process rescaling and training data population and adaptive learning, which should improve the reliability of the predictions even further. The evaluation metrics are precision, recall, and F1 score, as well as calculations of biases resulting from data heterogeneity.

Blockchain technology has also been integrated into the existing model to provide enhanced security and transparency. Blockchain secures an immutable record by capturing transactions, thus contributing toward data contributions that are traceable and verifiable as well as model updates. Each time the model is updated, it will be documented on a decentralized ledger thus its participants will be made accountable and their protection from data tampering will be guaranteed. Successful multi-institutional collaborations require a high degree of trust in the involved parties, which is precisely what this feature guarantees. The use of Blockchain enables this process to be fully trustworthy and transparent and hence more healthcare institutions are inclined towards taking part in federated learning initiatives.

The model illustrated in Figure 1 shows that healthcare-related data are stored locally at each node, such as hospitals, clinics, and research centers. Each node performs local model training using its own dataset, ensuring that patient data never leaves the institution. The local models are then sent to a central server to participate in federated learning. This process aggregates all the local models into a global model, which is updated and then distributed back to the institutions. To ensure data privacy and security, the model incorporates various privacy-preserving techniques, such as encryption, differential privacy, and secure multiparty computation. These methods are essential for protecting sensitive data and complying with privacy regulations. Additionally, the updated global model facilitates cooperative model training, providing clinicians with valuable insights for personalizing patient care and decision-making. In summary, the proposed model offers a secure and efficient approach for the healthcare sector to utilize federated learning technology, ensuring both data integrity and patient confidentiality.

4 Results and Discussion

The results from the implementation of Federated Learning on the Kaggle Medical Cost dataset demonstrate the model's capacity to learn effectively from decentralized and privacy-sensitive data. Key findings from the analysis are discussed below, with reference to the graphical representations and statistical summaries.

4.1 Medical Charges Analysis Across Age Groups

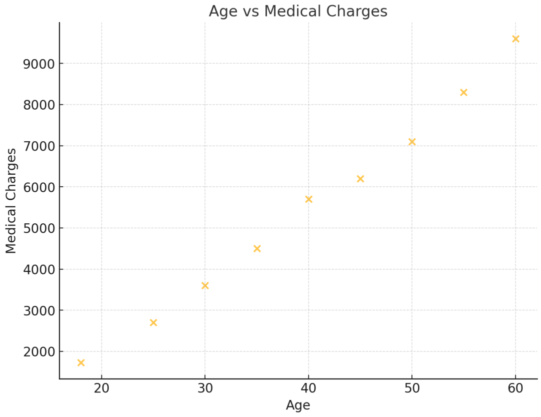

Figure 2. Age Vs Medical Charges.

Figure 2 shows the relationship between age and medical charges appears to illustrate a clear pattern of escalating charges with age. This pattern is in line with the general trend in the healthcare industry where the elderly tends to incur a higher amount of medical expenses due mainly to chronic conditions and age-related health problems. For example, it is found from the dataset that people in the 60-year age group are the ones with the highest charges, exceeding $9,000, while the younger cohort, such as those aged 18, has extremely low medical expenses, around $1,725 on average. Such observations are indicative of the model's capability of capturing the significant trends between age and healthcare costs.

4.2 BMI Categories and Medical Charges

The Figure 3 comparing medical charges for individuals with Body Mass Index (BMI) less than 25 versus those with BMI equal to or greater than 25.

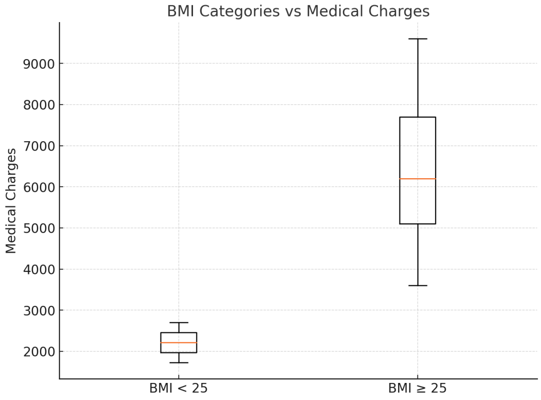

Figure 3. BMI Categories Vs Medical Charges.

The Figure 3 shows the influence of BMI on medical costs. Those with a BMI in the non-normal range (≥ 25) are generally incurring higher medical charges. The median charges for this group are higher than $6,000, while individuals with a BMI below 25 are the ones to incur lower costs, with median charges near $2,000. This result is consistent with common clinical observations that higher BMI is a frequent risk factor for diseases such as diabetes, hypertension, and heart disease, which in turn leads to increased medical expenses.

4.3 Federated Learning Model Performance

The Federated Learning approach demonstrated a high degree of reliability in maintaining privacy while learning useful data patterns from various distributed data sources. During the training of the medical cost prediction model, the local updates from the participating nodes (such as hospitals, clinics, and research centers) were merged to create the global model. This global model was built through collaboration among all parties that allowed the participation of diverse data characteristics and at the same time, the information is secure as it is only available at local nodes. The combination of differential privacy and secure multiparty computation further bolstered the security and trustworthiness of the entire system.

4.4 Data Insights from Summary Statistics

The summary statistics of the dataset offer additional information regarding the main factors affecting medical costs. The dataset's mean BMI is too high to be considered normal, which corresponds to the increment in medical bills because of the high scores in BMI. Besides, smokers have a particularly marked difference in charges when compared to non-smokers, further reaffirming the model's ability to distinguish high-risk categories as shown in Table 2. These results stress the significance of decentralized learning to grasp the different characteristics of the data while keeping sensitive patient information confidential.

It can be said that the learners were the ones who initiated the model so that they could work on some dataset that they had, which can be in nature, in any industry. Within the hierarchy of federated learning, some users have been randomized, such that the data of these users was meant to be private, although it could still be sent to the system, which is to say that it is used for the information of the system. The power of federated learning in using health data, which is very sensitive and in critical condition, in a collaborative

Table 2. Medical cost dataset summary.

	Age	Charges	BMI	Smoker
count	9.00000	9.00000	9.00000	9.00000
mean	41.77778	5480.44444	30.46667	0.55556
std	14.42767	2561.38794	5.36651	0.52705
min	18.00000	1725.00000	21.5000	0.00000
25%	32.50000	3375.00000	28.02500	0.00000
50%	40.00000	5700.00000	32.00000	1.00000
75%	50.00000	7150.00000	34.75000	1.00000
max	60.00000	9600.00000	36.50000	1.00000

model while also protecting the privacy of sensitive medical information is demonstrated here. The application of such a versatile model that can collect and analyze disparate datasets while implementing effective forecasting is illustrated here, which can be adopted in practice for various functions like patient cost forecasts, the definition of hazard groups, and the personalization of healthcare initiatives.

The findings contribute to the information that Federated learning is a secure tool to extract valuable insights from shared healthcare data. Apart from this, being non-intrusive also highlights personal privacy. In addition to this, it was also established that the model can be used to identify and record critical trends and risk indicators by means of statistical and graphical analyses. This proposal represents a remarkable step forward in the utilization of AI applications in the medical sector and gives the assurance that the innovation and confidentiality aspects of AI-assisted services will be handled at equal proportions.

5 Conclusion

The present study analyzes the remarkable influence of Federated Learning (FL) on the elimination of threats to privacy and security which the healthcare sector faces. The innovative FL framework that was put forward capitalized on a decentralized structure to enable the sharing of varying data sets from hospitals, clinics, and research centers for the collaborative training of a model without revealing sensitive patient information, which I found quite a powerful move. The results obtained from the Kaggle Medical Cost dataset were quite satisfactory, as the model successfully identified key patterns, such as the powerful influence of age, BMI, and smoking status on medical costs. The graphical analyses also verified that higher BMI and older age populations incurred higher medical expenses. The clinical trends also supported these findings, allowing us to conclude that these costs were mainly due to older adults. Moreover, privacy was ensured using privacy-preserving techniques such as differential privacy and secure multiparty computation, thereby confirming both the security of the data and compliance with legal standards. The successes that were achieved demonstrate how FL can be applied as a potent tool in gaining valuable insights with the utmost protection of patients' sensitive data.

Nonetheless, the study acknowledges certain limitations despite its impressive results. The main limitation is the computational overhead due to federated aggregation which most resource-fixed institutions would consider insurmountable. Secondly, the basic component of the model data density might be threatful in a data heterogeneity manner according to the extent of the data variations in quality; structure or representation. The future studies might delve into enhancing FL algorithms to lessen the demand of resources and also fortify them against adversarial attacks as well. However, this study has laid a stepping stone for the advancement of secure and cooperative machine learning in healthcare and the way personalized and data-driven medical innovations could take place is with this kind of innovation.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Knowledge-based systems, 274*, 110658. [CrossRef]

[2] Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems, 144*, 271-290. [CrossRef]

[3] Shiranthika, C., Saeedi, P., & Bajić, I. V. (2023). Decentralized learning in healthcare: a review of

emerging techniques. *IEEE Access, 11*, 54188-54209. [CrossRef]

[4] Hiwale, M., Walambe, R., Potdar, V., & Kotecha, K. (2023). A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthcare Analytics, 3*, 100192. [CrossRef]

[5] Prayitno, Shyu, C. R., Putra, K. T., Chen, H. C., Tsai, Y. Y., Hossain, K. T., ... & Shae, Z. Y. (2021). A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications. *Applied Sciences, 11*(23), 11191. [CrossRef]

[6] Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated learning for healthcare informatics. *Journal of healthcare informatics research, 5*(1), 1-19. [CrossRef]

[7] Ficco, M., Guerriero, A., Milite, E., Palmieri, F., Pietrantuono, R., & Russo, S. (2024). Federated learning for IoT devices: Enhancing TinyML with on-board training. *Information Fusion, 104*, 102189. [CrossRef]

[8] Chen, Z., Du, J., Hou, X., Yu, K., Wang, J., & Han, Z. (2024). Channel adaptive and sparsity personalized federated learning for privacy protection in smart healthcare systems. *IEEE Journal of Biomedical and Health Informatics, 28*(6), 3248-3257. [CrossRef]

[9] Wang, B., Li, H., Guo, Y., & Wang, J. (2023). PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Applied Soft Computing, 146*, 110677. [CrossRef]

[10] Choi, G., Cha, W. C., Lee, S. U., & Shin, S. Y. (2024). Survey of medical applications of federated learning. *Healthcare Informatics Research, 30*(1), 3-15. [CrossRef]

[11] Moulahi, W., Jdey, I., Moulahi, T., Alawida, M., & Alabdulatif, A. (2023). A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Computers in Biology and Medicine, 167*, 107630. [CrossRef]

[12] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems, 129*, 380-388. [CrossRef]

[13] Karimian, G., Petelos, E., & Evers, S. M. (2022). The ethical issues of the application of artificial intelligence in healthcare: a systematic scoping review. *AI and Ethics, 2*(4), 539-551. [CrossRef]

[14] Shahriar, S., Allana, S., Hazratifard, S. M., & Dara, R. (2023). A survey of privacy risks and mitigation strategies in the artificial intelligence life cycle. *IEEE Access, 11*, 61829-61854. [CrossRef]

[15] Saraswat, D., Bhattacharya, P., Verma, A., Prasad, V. K., Tanwar, S., Sharma, G., ... & Sharma, R. (2022). Explainable AI for healthcare 5.0: opportunities and challenges. *IEEE Access, 10*, 84486-84517. [CrossRef]

[16] Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bagci, U., Rawat, D. B., & Vlassov, V. (2023). Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. *IEEE Internet of Things Journal, 11*(5), 7374-7398. [CrossRef]

[17] Sinaci, A. A., Gencturk, M., Alvarez-Romero, C., Erturkmen, G. B. L., Martinez-Garcia, A., Escalona-Cuaresma, M. J., & Parra-Calderon, C. L. (2024). Privacy-preserving federated machine learning on FAIR health data: a real-world application. *Computational and Structural Biotechnology Journal, 24*, 136-145. [CrossRef]

[18] Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine, 170*, 108036. [CrossRef]

[19] Alsamhi, S. H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., ... & Curry, E. (2024). Federated learning meets blockchain in decentralized data sharing: Healthcare use case. *IEEE Internet of Things Journal, 11*(11), 19602-19615. [CrossRef]

[20] Bhatt, H., Jadav, N. K., Kumari, A., Gupta, R., Tanwar, S., Polkowski, Z., ... & Hassanein, A. S. (2024). Artificial neural network-driven federated learning for heart stroke prediction in healthcare 4.0 underlying 5G. *Concurrency and Computation: Practice and Experience, 36*(3), e7911. [CrossRef]

Fajar Rao is currently pursuing a Bachelor of Advanced Computing at The University of Sydney, with a focused interest in data science and business analysis. Eager to tackle complex business challenges, Fajar aims to leverage data-driven insights to contribute to meaningful projects. With a strong foundation in technical skills, he excels as a proactive team member, known for effective communication and negotiation, fostering collaboration with cross-functional teams and stakeholders. Fajar is also keen to explore opportunities in data science, tech risk consulting, and data governance, particularly in the tech and financial sectors. (Email: frao9131@uni.sydney.edu.au)