Advancing Medical Recommendations With Federated Learning on Decentralized Data: A Roadmap for Implementation

Rani Kumari, Dinesh Kumar Sah, *Member, IEEE*, Shivani Gupta, Korhan Cengiz, *Senior Member, IEEE*, and Nikola Ivković, *Senior Member, IEEE*

***Abstract*—This proposal presents a road-map for implementing federated learning (FL) for personalized medical recommendations on decentralized data. FL is a privacy-preserving technique allowing multiple parties to train machine learning models collaboratively without sharing their data. Our proposed framework incorporates differential privacy techniques to protect patient privacy. We discuss several evaluation metrics, including KL divergence, fairness, confidence intervals, top-N hit rate, sensitivity analysis, and novelty to evaluate the performance of the federated learning system. These metrics collectively serve as a robust toolbox for assessing Space needed the performance of the federated learning system. The proposed framework and evaluation metrics can provide valuable insights into the system's effectiveness and guide the selection of optimal hyperparameters and model architectures.**

***Index Terms*—Federated learning, personalized medical recommendations, decentralized data, model architecture, and sensitivity analysis.**

I. Introduction

HEALTHCARE providers and patients increasingly rely on medical recommendations personalized to individual patients' needs and medical histories. The availability of large amounts of medical data has made it possible to develop personalized recommendation models that can improve the quality of care and health outcomes for patients [1], [2], [3]. However, using sensitive medical data also raises privacy and security concerns, and sharing such data can be subject to legal and regulatory restrictions. Federated learning, a distributed machine learning approach that allows the training of models on decentralized data, has emerged as a promising solution to address these concerns [4], [5]. By training models on data distributed across multiple sites, federated learning enables the development of personalized medical recommendations while preserving the privacy and security of sensitive medical data.

In the realm of healthcare, personalized medical recommendations have become increasingly crucial for ensuring the best patient outcomes. As medical data continues to proliferate across decentralized sources, the need for effective, privacy-conscious machine learning approaches has grown substantially. The digital transformation of healthcare has led to an explosion of healthcare data. Electronic health records (EHRs), medical imaging, wearable devices, and patient-generated data all contribute to this wealth of information. While these data sources offer invaluable insights, they often remain within healthcare institutions, creating a barrier to comprehensive analysis [6], [7]. Personalized medicine, where medical decisions, practices, and treatments are tailored to the individual patient, holds the potential to significantly enhance patient care. Machine learning plays a pivotal role in realizing this promise by offering predictive models for early disease detection, treatment recommendations, and drug prescription based on individual patient characteristics. However, to build robust, generalized models, access to diverse and extensive medical data is essential [6], [8]. Maintaining the privacy and security of healthcare data is non-negotiable. Medical data is among the most sensitive, often protected by stringent regulations like HIPAA (Health Insurance Portability and Accountability Act) in the United States and GDPR (General Data Protection Regulation) in Europe. Federated learning emerges as a solution that marries the demand for data access with the need for privacy.

Recently, interest has been increasing in developing federated learning frameworks for personalized medical recommendations. However, several challenges still need to be addressed to enable the widespread adoption of this approach. These challenges include data heterogeneity, communication efficiency, privacy and security, and legal and regulatory requirements. We aim to provide a comprehensive guide for healthcare providers, data scientists, and other stakeholders interested in developing personalized medical recommendation systems using federated learning.

Manuscript received 6 May 2023; revised 21 October 2023; accepted 3 November 2023. Date of publication 28 November 2023; date of current version 26 April 2024. *(Corresponding author: Dinesh Kumar Sah.)*

Rani Kumari is with the Department of Computer Science, Birla Institute of Technology, Ranchi 847226, India (e-mail: rkd.bit@gmail.com).

Dinesh kumar sah is with the Data Communication Group, Division of Networked and Embedded Systems, Mälardalens University, 722 20 Västerås, Sweden (e-mail: dinesh.16dr000267@cse.ism.ac.in).

Shivani Gupta is with the School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology (Chennai), Chennai 600127, India (e-mail: gshivani554@gmail.com).

Korhan Cengiz is with the Department of Electrical-Electronics Engineering, Istinye University, 34010 Istanbul, Turkey, and also with the Department of Information Technologies, Faculty of Informatics and Management, University of Hradec Kralove, 500 03 Hradec Kralove, Czech Republic (e-mail: korhan.cengiz@istinye.edu.tr).

Nikola Ivković is with the Faculty of Organization and Informatics, University of Zagreb, 42000 Varaždin, Croatia (e-mail: nikola.ivkovic@foi.hr).

Digital Object Identifier 10.1109/TCE.2023.3334159

Instead of sharing data with a centralized server for model training, the data remains on local devices or servers, and only model updates are exchanged between the devices. On the other hand, personalized medical recommendations are tailored to individual patient's needs and medical history [9], [10].

Personalized recommendation models can be developed using various techniques, including collaborative filtering, content-based filtering, and matrix factorization. The availability of large amounts of medical data, such as electronic health records (EHRs), has made it possible to develop personalized recommendation models for various healthcare applications, including diagnosis, treatment, and disease prevention.

The advantages for developing personalized medical recommendations on decentralized data are as followings:

1) *Data privacy and security:* This framework facilitates the creation of personalized medical recommendations while upholding the confidentiality and security of critical medical data. Rather than transmitting data to a central server, it remains localized on devices or servers, with only model updates exchanged between these systems. This approach effectively mitigates the potential threats of data breaches and unauthorised access to sensitive medical information
2) *Data heterogeneity:* Medical data is often distributed across different healthcare providers and is characterized by data types, formats, and quality heterogeneity. It can address this heterogeneity by training models on data that is distributed across multiple sites without the need for data sharing [11].
3) *Scalability:* It can be scaled to large datasets and can accommodate changes in the data distribution over time.
4) *Reduced bias:* It can reduce the bias in personalized medical recommendation models by training models on data distributed across multiple sites. This can help to mitigate the risk of bias introduced by data collected from a single site or population.

We operates on decentralized data, which inherently brings about challenges in terms of data sources, types, and quality.

1) *Data Distribution Heterogeneity:* In the context of personalized medical recommendations, data distribution heterogeneity across different healthcare institutions may significantly affect model training. Variations in data types (e.g., EHRs, medical imaging, wearable data) and patient populations can introduce biases and negatively impact model generalization. To tackle data distribution heterogeneity, a comprehensive data preprocessing and harmonization strategy should be employed. This may include data normalization techniques, data augmentation, and feature engineering to make data sources more compatible. Additionally, federated learning methods like Federated Averaging and Federated Proximal Gradient can be adapted to handle data heterogeneity more effectively [12].
2) *Concept Drift:* It is a critical challenge in federated learning for personalized medical recommendations, especially in healthcare, where data distributions can evolve over time. For example, changes in treatment guidelines, new medical devices, or shifts in population health can lead to concept drift. This can result in a decrease in model performance, as the model may not adapt well to these evolving data distributions. It deals with concept drift requires continuous monitoring of model performance and regular model updates. Techniques such as incremental learning and ensemble methods can be employed to adapt the model to changing data distributions over time. It's crucial to establish a robust feedback loop between healthcare institutions, data providers, and the federated learning system to ensure timely updates based on evolving medical practices.
3) *Privacy-Preserving Aggregation:* While privacy is a fundamental concern, the process of aggregating model updates in federated learning must ensure privacy preservation. Conventional aggregation methods might not be robust against sophisticated attacks. Ensuring that aggregated updates do not leak any sensitive information is an ongoing challenge. Techniques such as secure aggregation and differential privacy can be integrated to enhance privacy-preserving aggregation. Secure multiparty computation (SMPC) can be used to perform aggregation while keeping individual updates encrypted. Differential privacy adds noise to the aggregation process, making it more challenging for adversaries to infer details about individual updates.
4) *Scalability:* As federated learning scales to accommodate numerous healthcare institutions, ensuring the system's scalability becomes a challenge. Large numbers of clients, data sources, and communication overhead can strain the system's resources. Employ distributed computing frameworks and optimizations to handle scalability. Strategies like model parallelism, efficient communication protocols, and cloud-based federated learning can manage the computational and communication demands as the system expands [11], [13].
5) *Interoperability:* Healthcare institutions use diverse technologies and systems. Achieving interoperability to integrate these systems into the federated learning framework is complex. Adherence to health data standards, such as HL7 FHIR, can facilitate data exchange between different systems. Additionally, developing adapters and connectors for various EHRs and medical devices can bridge the interoperability gap [14], [15].

By addressing these challenges, the federated learning system can become more resilient and adaptable to the complexities of decentralized healthcare data.

II. Decentralized Data for Medical Recommendations

Decentralized data refers to data that is distributed across multiple locations or devices. Medical data is often distributed across healthcare providers, hospitals, clinics, and research institutions. Medical data collected from different healthcare providers and institutions can help to reduce bias and improve the generalizability of personalized medical recommendation models [16]. Decentralized data can facilitate collaboration and sharing among healthcare providers, leading to more comprehensive and accurate medical recommendation models.

The data may also be collected and stored using different systems and technologies. Integrating and preprocessing the data for personalized medical recommendation models can make it difficult. Another challenge is the potential for data privacy and security breaches. Decentralized data can increase the risk of unauthorized access to sensitive medical data. This can be particularly concerning when the data is subject to legal and regulatory restrictions or where data privacy and security concerns are paramount.

A. Overview of Decentralized Data in Healthcare

Decentralized healthcare data can include various data types, such as electronic health records (EHRs), medical images, genomics data, and wearable sensor data [17]. EHRs are one of the most common medical data sources, containing information on patient's medical history, diagnoses, treatments, and medications. Medical images, such as X-rays and MRIs, can also provide valuable information for diagnosis and treatment. Genomics data, which refers to information about patients' genetic makeup, can help to identify genetic risk factors for disease and guide personalized treatments. Wearable sensor data can provide real-time information on patients' physical activity, sleep, and other health behaviors.

B. Considerations for Data Selection and Pre-Processing

When using decentralized data for personalized medical recommendations, it is important to consider several factors related to data selection and preprocessing. These factors include data quality, data heterogeneity, and data distribution along with data types, formats, and quality heterogeneity which can characterize medical data. To address this challenge, selecting the data sources and performing appropriate preprocessing steps carefully is important. For example, data normalization and feature selection can help reduce data heterogeneity's impact on personalized medical recommendation models [18]. Another consideration for data selection is data quality. The quality of medical data can vary depending on the source and the collection method. It is important to perform data quality checks and apply appropriate quality control measures to ensure the data quality used in personalized medical recommendation models.

In addition, it is also important to consider the distribution of the data when using decentralized data for medical recommendations. The distribution of the data can impact the performance of personalized medical recommendation models. For example, if the data is imbalanced or skewed towards a particular population, the resulting personalized medical recommendation models may not represent the entire population. It is important to carefully select the data sources and perform appropriate data preprocessing steps to address this challenge.

III. Federated Learning Framework

This section will discuss the key components of a federated learning framework for personalized medical recommendations on decentralized data.

1) *Data Selection and Pre-processing:* It is the first step in developing a federated learning framework for personalized medical recommendations. As discussed in the previous section, careful consideration of data selection and preprocessing is critical for developing effective personalized medical recommendation models. The data selection and preprocessing steps should be performed on each site before training the model.
2) *Model Training:* After the data selection and preprocessing steps, the next step is to train the model on the decentralized data. The model is trained locally on each site using the local data, and only the model updates are sent to a centralized server for aggregation. The aggregated model updates are then used to update the global model, which is sent back to each site for further local training. This process is repeated until the model converges.
3) *Model Evaluation:* Once the model is trained, the next step is to evaluate the performance of the model. It can be performed on a held-out test set or using cross-validation. The evaluation metrics can include precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC).
4) *Model Deployment:* Model deployment is the final step in the federated learning framework for personalized medical recommendations. The deployed model should be privacy-preserving and comply with relevant legal and regulatory requirements. The deployed model can provide personalized medical recommendations to individual patients based on their medical history and other relevant factors.
5) *Considerations for Implementation:* These considerations include data privacy and security, regulatory and legal requirements, and technical infrastructure. It is important to ensure that the federated learning framework complies with relevant legal and regulatory requirements and that appropriate technical infrastructure is in place to support the federated learning process.

A. Algorithm Selection and Model Architecture

The algorithm and model architecture choice can impact the model's performance and the computational resources required for training and inference. In algorithm selection for federated learning is the need to balance privacy and accuracy. Privacy-preserving federated learning techniques, such as secure aggregation and differential privacy, can help to protect sensitive medical data while enabling the development of accurate, personalized medical recommendation models. In addition, algorithms designed for distributed learning, such as federated averaging and kernel ridge regression, can be well-suited for federated learning on decentralized medical data.

The choice of model architecture can also impact the performance of personalized medical recommendation models. Deep learning architectures, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), effectively develop personalized medical recommendation models. However, these models can be computationally expensive to train and may require significant amounts of data.

Several approaches have been proposed to address these challenges for developing lightweight and efficient personalized medical recommendation models [19], [20], [21], [22]. For example, transfer learning can adapt pre-trained models to new medical data. In contrast, model compression techniques, such as pruning and quantization, can reduce the computational resources required for training and inference. Careful algorithm selection and model architecture design are critical for developing effective federated learning frameworks for personalized medical recommendations on decentralized data. The next section will provide a roadmap for implementing such frameworks.

B. Algorithm Selection

Algorithm selection involves choosing an appropriate algorithm for training personalized medical recommendation models on decentralized data. One of the key challenges in algorithm selection for federated learning is balancing privacy and accuracy. This can be achieved through privacy-preserving techniques, such as secure aggregation and differential privacy.

Let $D = D_1, D_2, \ldots, D_n$ denote the decentralized medical data, where D_i represents the data at the i-th site. Let $f(\theta)$ represent the personalized medical recommendation model with parameters θ. The goal is to learn the optimal parameters θ^* that minimize the expected risk, $R(f(\theta))$, given by:

$$\theta^* = \arg\min_{\theta} \mathbb{E}x, y \sim D\big[L(f\theta(x), y)\big], \tag{1}$$

where $L(\cdot)$ is the loss function and x and y represent the input and output, respectively.

Federated learning algorithms, such as federated averaging and federated kernel ridge regression, can be used to train the personalized medical recommendation model on decentralized data. These algorithms involve iteratively updating the model parameters based on the local data at each site and aggregating the updates to obtain a global model.

C. Model Architecture

Let x denote the input to the personalized medical recommendation model and y denote the output. The goal is to learn a function $f(x) = y$ that maps the input to the output. The model architecture involves choosing the appropriate number of layers, the size of each layer, and the activation functions used in each layer.

$$p(x) = \int p(x|z)p(z)dz \tag{2}$$

The Eqn. (2) calculates the probability distribution $p(x)$ as an integral over $p(x|z)$ and $p(z)$. It is often used in probabilistic modeling to represent the overall distribution $p(x)$ as a combination of conditional probabilities $p(x|z)$ and prior probabilities $p(z)$.

$$KL(p||q) = \int p(x) \log \frac{p(x)}{q(x)} dx \tag{3}$$

The Eqn. (3) defines the KL divergence between probability distributions p and q. It quantifies the difference between two distributions $p(x)$ and $q(x)$ by measuring the information lost when $p(x)$ is approximated by $q(x)$.

$$z_i = f(W_i x_i + b_i) \tag{4}$$

In the Eqn. (4), z_i represents the output of a neural network layer, computed as the result of applying an activation function f to a weighted sum of input features x_i, where W_i are the weights and b_i is the bias.

$$y = g(W_2 z + b_2) \tag{5}$$

In Eqn. (5), we calculates the final output y of a neural network. It involves applying another activation function g to a weighted sum of intermediate features z, where W_2 represents the weights and b_2 is the bias of the output layer.

$$H_t = \phi(W_h x_t + U_h h_{t-1} + b_h) \tag{6}$$

In Eqn. (6), we describes the hidden state H_t update in a recurrent neural network (RNN). It is based on the current input x_t, the previous state h_{t-1}, and the weights W_h, U_h, and bias b_h. RNNs are often used for sequential data modeling.

$$O_t = \sigma(W_o H_t + U_o h_{t-1} + b_o) \tag{7}$$

In Eqn. (7), we computes the output O_t of a recurrent neural network (RNN) at time step t. This output is calculated using an activation function σ applied to a combination of the current hidden state H_t, the previous hidden state h_{t-1}, and the weights W_o, U_o, and bias b_o. RNNs are widely used for sequential data processing.

$$L(f_\theta(x), y) \ = -\sum_{c=1}^{C} y_c \log(f_\theta(x)_c) \tag{8}$$

In Eqn. (8), we represents a typical loss function used in machine learning, particularly in the context of classification problems. It measures the loss, or error, between the predicted values $f_\theta(x)$ and the true values y. The loss is calculated as the negative logarithm of the predicted class probabilities $(f_\theta(x)_c)$ for each class c, weighted by the true class labels y_c.

$$\theta^{(t+1)} = \theta^{(t)} - \eta_t \nabla_\theta \mathbb{E}(x, y) \sim D_i\big[L(f\theta(x), y)\big] \tag{9}$$

In Eqn. (9), we represents a gradient descent update for model parameters θ in the context of machine learning. It describes how the model parameters are updated iteratively $(\theta^{(t+1)})$ based on the current parameters $(\theta^{(t)})$, a learning rate η_t, and the gradient of the expected loss $\mathbb{E}(x, y) \sim D_i[L(f_\theta(x), y)]$ with respect to the parameters θ. This update is used to minimize the loss function and improve model performance.

$$W_{ij} = \sum_{k=1}^{n} a_{ik} x_{kj} \tag{10}$$

In Eqn. (10), we calculates the weighted sum W_{ij} as the sum of products between the elements of two matrices, a_{ik} and x_{kj}. This operation is commonly used in linear algebra and matrix computations and can be relevant for various aspects of machine learning, including neural network operations.

$$\hat{y} = f(\mathbf{x}; \theta) = \sigma\left(\theta_0 + \sum_{i=1}^{d} \theta_i x_i\right) \tag{11}$$

In Eqn. (11), we defines a logistic regression model. The model calculates the predicted output $\hat{y}$ based on the input features x_i, model parameters θ_i, and a bias term θ_0. The sigmoid activation function σ is applied to the linear combination of input features, making it suitable for binary classification tasks.

$$\hat{y} = f(\mathbf{x}; \theta) = \sum_{i=1}^{m} w_i g(\mathbf{x}; \alpha_i) \tag{12}$$

In Eqn. (12), we defines an ensemble model for making predictions. The predicted output $\hat{y}$ is obtained as the sum of individual predictions from m base models. Each base model uses different weight w_i and transformation function $g(\mathbf{x}; \alpha_i)$ for the input features $\mathbf{x}$. Ensemble methods combine multiple models to improve prediction accuracy.

$$H_{t,i} = \max(0, W_i \cdot x_t + b_i) \tag{13}$$

In Eqn. (13), we describes the calculation of an element $H_{t,i}$ in a neural network layer using Rectified Linear Unit (ReLU) activation. It applies the ReLU function to a linear combination of the input x_t with weight W_i and bias b_i. ReLU is a common activation function that introduces non-linearity in neural networks.

$$h_t = f(h_{t-1}, x_t) = \tanh(W_{hh} h_{t-1} + W_{xh} x_t + b_h) \tag{14}$$

In Eqn. (14), we represents the update of a hidden state h_t in a Recurrent Neural Network (RNN). The hidden state at time step t is calculated as a function of the previous hidden state h_{t-1}, the current input x_t, and weights and biases (W_{hh}, W_{xh}, b_h) using the hyperbolic tangent (tanh) activation function. RNNs are used for sequential data modeling.

$$\theta^{(t+1)} = \theta^{(t)} - \eta_t \nabla L(f_\theta(x), y) \tag{15}$$

In Eqn. (15), we represents a gradient descent update for model parameters θ in the case where there is no expectation operator. It describes how the model parameters are updated iteratively ($\theta^{(t+1)}$) based on the current parameters ($\theta^{(t)}$), a learning rate η_t, and the gradient of the loss function $\nabla L(f_\theta(x), y)$ with respect to the parameters θ. This is a fundamental step in training machine learning models.

$$\theta^{(t+1)} = \theta^{(t)} - \eta_t \nabla_\theta L(f_\theta(x), y) \tag{16}$$

In Eqn. (16), we presents an alternative form of the gradient descent update for model parameters θ. It is similar to Equation (8) but explicitly denotes the gradient with respect to the parameters θ as ∇_θ. The update is based on the learning rate η_t and the gradient of the loss function $\nabla_\theta L(f_\theta(x), y)$. This equation can be used in various machine learning algorithms.

We demonstrated the different concepts relevant to algorithm selection and model architecture in the context of federated learning such as loss functions, gradient descent updates, weight matrix calculations, and activation functions used in various neural network architectures.

D. Federated Optimization Methods

Federated optimization methods have gained popularity in recent years due to the increasing amount of data generated by mobile and Internet of Things (IoT) devices, which are typically not centralized and cannot be easily aggregated for model training. The goal of federated optimization is to learn a global model by aggregating the local models trained on each device while preserving the privacy and security of the local data. Federated optimization methods typically involve a server and a set of clients. Each client has a local dataset and computes updates to the global model based on its local data. The server aggregates these updates to update the global model and distributes it back to the clients.

One of the key challenges in federated optimization is the heterogeneity of the local datasets and the computing resources of the clients. Several optimization methods have been proposed to address this, such as federated averaging, federated stochastic gradient descent (SGD), and federated proximal gradient methods. Federated averaging is a simple and widely used optimization method in federated learning. It involves averaging the local model updates from the clients to update the global model. Formally, at each round t, the server sends the current global model $\mathbf{w}^{(t)}$ to the clients, and each client i computes a local update $\Delta \mathbf{w}_i^{(t)}$ based on its local data. The server then aggregates the local updates by computing the weighted average:

$$\mathbf{w}^{(t+1)} = \sum_{i=1}^{n} \frac{|\mathcal{D}_i|}{|\mathcal{D}|} \Delta \mathbf{w}_i^{(t)}, \tag{17}$$

where $\mathcal{D}$ is the union of all local datasets and $|\mathcal{D}_i|$ is the size of the local dataset of client i.

Federated SGD is a variant of SGD that is designed for federated learning. It involves computing stochastic gradient updates on the local data of each client and aggregating the updates to update the global model. Federated proximal gradient methods are a class of optimization methods that involve proximal operators to handle non-smooth objectives in federated learning. The federated optimization methods are a promising approach for training models on decentralized data while preserving the privacy and security of the data. Further research is needed to explore the effectiveness of these methods on different types of datasets and applications.

E. Addressing Data Heterogeneity and Distribution

The clients may have different types of data, different amounts of data, or different data distributions. Several methods have been proposed to address this challenge, such as federated transfer learning, personalized federated learning, and adaptive federated optimization. Federated transfer learning is a method that enables clients to transfer knowledge from pre-trained models to the current model being trained. This can be done by fine-tuning the pre-trained model on the local data of each client or by transferring specific layers of the pre-trained model to the current model being trained. Mathematically, federated transfer learning can be

represented as:

$$\mathbf{w}^{(t+1)}i = \mathbf{w}^{(t+1)}i, pre - \eta \nabla L\Big(\mathbf{w}_i^{(t+1)}; \mathcal{D}_i\Big), \tag{18}$$

where $\mathbf{w}_{i,pre}^{(t+1)}$ is the pre-trained model, η is the learning rate, $\nabla L(\mathbf{w}_i^{(t+1)}; \mathcal{D}_i)$ is the gradient of the loss function on the local dataset $\mathcal{D}_i$, and $\mathbf{w}_i^{(t+1)}$ is the updated model parameters.

Personalized federated learning is a method that enables clients to learn personalized models based on their local data. This can be done by assigning different weights to the local updates based on the similarity of the local data to the global data. Mathematically, personalized federated learning can be represented as:

$$\mathbf{w}^{(t+1)} = \sum_{i=1}^{n} w_i \Delta \mathbf{w}_i^{(t)}, \tag{19}$$

where w_i is the weight assigned to the local update of client i based on the similarity of its local data to the global data, and $\Delta \mathbf{w}_i^{(t)}$ is the local update of client i at round t.

Adaptive federated optimization is a method that enables the server to adaptively adjust the learning rate or the aggregation weights based on the heterogeneity of the local datasets or the convergence of the global model. Mathematically, adaptive federated optimization can be represented as:

$$\mathbf{w}^{(t+1)} = \mathbf{w}^{(t)} - \eta_t \nabla L\Big(\mathbf{w}^{(t)}; \mathcal{D}\Big) + \epsilon_t, \tag{20}$$

where η_t is the learning rate at round t, $\nabla L(\mathbf{w}^{(t)}; \mathcal{D})$ is the gradient of the loss function on the global dataset $\mathcal{D}$, and ϵ_t is the noise added to the update to account for the heterogeneity of the local datasets, the data heterogeneity and distribution in federated optimization require careful consideration of the local datasets' characteristics and the global model's goals and the development of appropriate mathematical models and optimization algorithms.

IV. Privacy and Security Considerations

In federated learning, preserving the privacy and security of local data is a critical concern. As the local data is decentralized and distributed across multiple clients, it is vulnerable to various privacy and security attacks, such as membership inference attacks, model inversion attacks, and poisoning attacks. Therefore, several techniques have been proposed to address the privacy and security concerns in federated learning. One of the most common techniques used in federated learning for privacy preservation is differential privacy. It is a mathematical framework that guarantees that the computation results do not reveal sensitive information about the local data. The basic idea of differential privacy is to add noise to the computation, which makes it difficult for an attacker to distinguish between the computations performed on the local data of different clients [23].

Another technique used in FL for privacy preservation is secure aggregation. Secure aggregation involves encrypting the local model updates before sending them to the server and then decrypting them at the server to compute the global update. This ensures that the local updates are not exposed to the server or other clients and that the global update is computed securely. In addition to privacy preservation, security is also a concern and several techniques have been proposed to ensure the security, such as secure computation and communication. Secure computation involves performing computations on encrypted data, ensuring the data remains private and secure throughout the computation. Secure communication involves using secure protocols, such as secure socket layer (SSL), transport layer security (TLS), and virtual private network (VPN), to protect the communication between the clients and the server. Privacy and security considerations are critical in federated learning, and several techniques have been proposed to address these concerns.

Future research in FL should focus on developing more robust and scalable privacy and security techniques and on evaluating the effectiveness of these techniques on different types of datasets and applications [24], [25].

V. Result and Discussion

The evaluation metrics and analysis methods can be used for federated learning in personalized medical recommendations.

1) *Differential Privacy:* It is a measure of privacy protection that ensures that individual patient data is not exposed during training. Differential privacy techniques, such as adding noise to the local updates, can be used to protect the privacy of the local data while still enabling effective model training. Evaluating the effectiveness of differential privacy techniques can provide insight into the level of privacy protection the federated learning system provides and ensure that patient data is kept secure and confidential. In addition to the epsilon value, we can also use other measures of differential privacy, such as mutual information and Kullback-Leibler (KL) divergence, to evaluate the privacy performance of federated learning models. Mutual information measures the information shared between the local data and the global model. In contrast, KL divergence measures the distance between the probability distributions of the local data and the global model. It measures the difference between two probability distributions. In the context of federated learning, we can use KL divergence to evaluate the privacy performance of the federated learning model by comparing the distribution of the local data to the distribution of the global model. Let $P(X)$ and $Q(X)$ be the probability distributions of the local data and global model, respectively. The KL divergence between these two distributions is defined as:

$$KL(P||Q) = \sum_{X} P(X) \log\left(\frac{P(X)}{Q(X)}\right) \tag{21}$$

where the sum is taken over all possible values of X, the KL divergence measures the amount of information lost when the global model approximates the local data distribution. A smaller KL divergence value indicates that the global model better approximates the local data distribution, providing better privacy protection. The KL

divergence is asymmetric, i.e., $KL(P||Q) \neq KL(Q||P)$, so the order of the probability distributions matters.

2) *Fairness:* We can also use other metrics, such as equal opportunity or equalized odds, to evaluate fairness. Equal opportunity measures the difference in true positive rates between different demographic groups, while equalized odds measure the difference in false positive rates. A value of 0 indicates perfect fairness, while greater than 0 indicates that the recommendations disproportionately impact certain groups. It is another important metric that can be used to evaluate the performance of federated learning models for personalized medical recommendations. Fairness measures can be used to evaluate the distribution of recommendations across different demographic and socioeconomic groups. For example, demographic parity can measure whether the distribution of recommendations is consistent across different racial or ethnic groups. Evaluating the fairness of the recommendations can ensure that the system is not biased towards any particular group and provides equitable recommendations to all patients.
3) *Confidence Intervals:* Confidence intervals can be calculated using various statistical methods, such as the t-distribution or the bootstrap. By calculating confidence intervals for each recommendation, we can estimate the range of values that the true recommendation score is likely to fall within with a certain confidence level, such as 95%. It is useful for evaluating the uncertainty of the recommendation model's predictions. By calculating confidence intervals for each recommendation, the system can provide more transparent recommendations to patients and help them understand the level of confidence that the system has in each recommendation.
4) *Top-N Hit Rate:* The top-N hit rate can be calculated using the precision or recall at N metric, which measures the percentage of correct recommendations among the top-N recommendations. A higher precision or recall at N indicates that the system provides more accurate and relevant patient recommendations. The metric for evaluating the effectiveness of recommendation systems with large item catalogs. It measures the percentage of recommendations included in each user's top-N recommendations. By evaluating the top-N hit rate, the system can ensure that it is providing relevant recommendations to patients and can improve the quality of the recommendations.
5) Sensitivity analysis can be used to evaluate the impact of different hyperparameters and model architectures on the performance of the federated learning system. This can help identify the most effective configurations for the model and optimize the system's performance. It can involve varying hyperparameters or model architectures, such as the number of hidden layers or the activation function, and measuring the resulting impact on evaluation metrics such as accuracy or F1-score. We can also use techniques such as grid search or randomized search to systematically explore the hyperparameter space and identify the optimal configuration for the model.

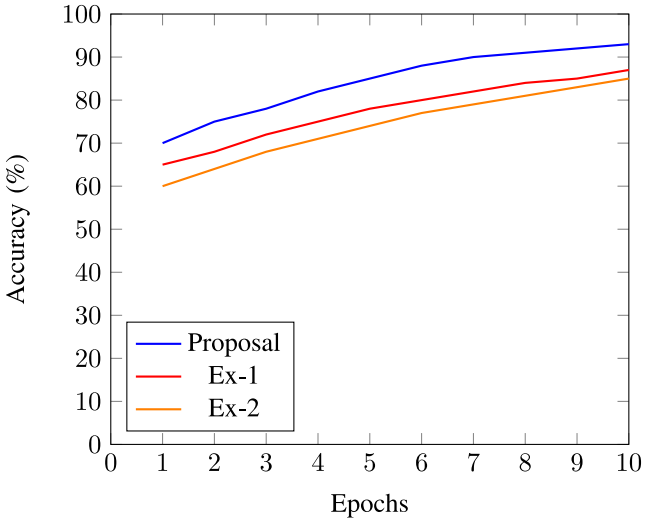

Fig. 1. The accuracy of the proposal with different iterations.

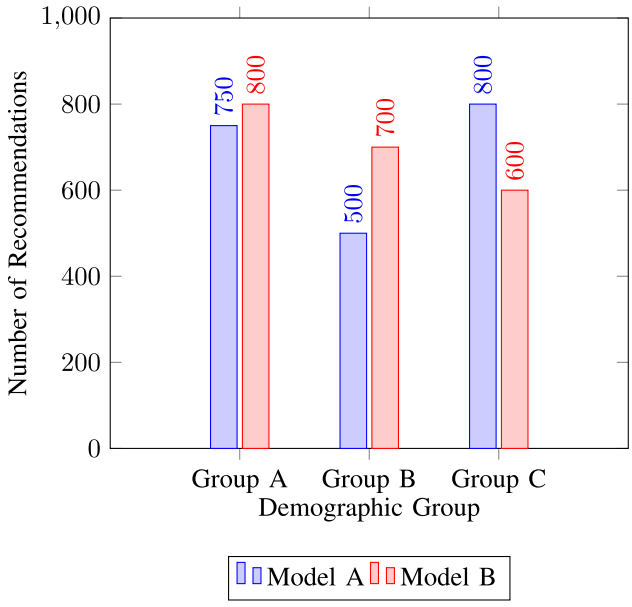

Fig. 2. The number of Recommendations vs. Demographic Group.

The combined graph for Top-N Hit Rate and Sensitivity Analysis shows the performance of the federated learning system with varying hyperparameter values. The blue bars represent the Top-N hit rate, which measures the percentage of recommendations included in the top-N recommendations for each user. The red bars represent the sensitivity analysis, which measures the impact of different hyperparameters and model architectures on the performance of the federated learning system. The graph shows that as the hyperparameter value increases, the Top-N hit rate also increases, indicating that the system provides more accurate recommendations. However, the sensitivity analysis shows a threshold beyond which further increases in the hyperparameter value do not improve the system's performance. This suggests the system should be configured with an optimal hyperparameter value to achieve the best balance between accuracy and performance.

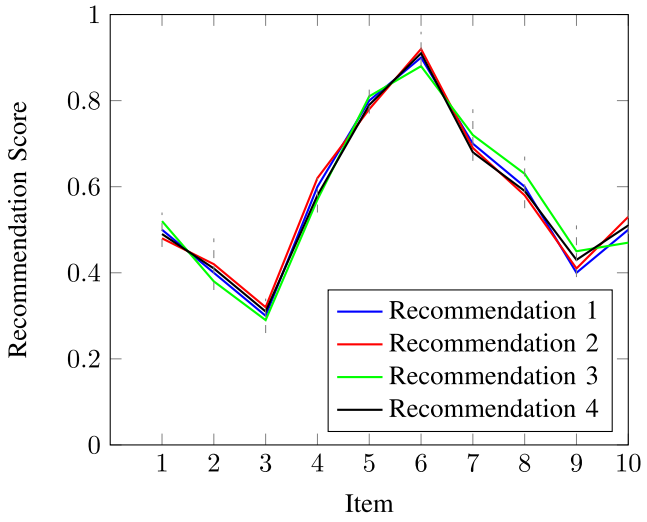

Fig. 3. Recommendations score for confidence interval.

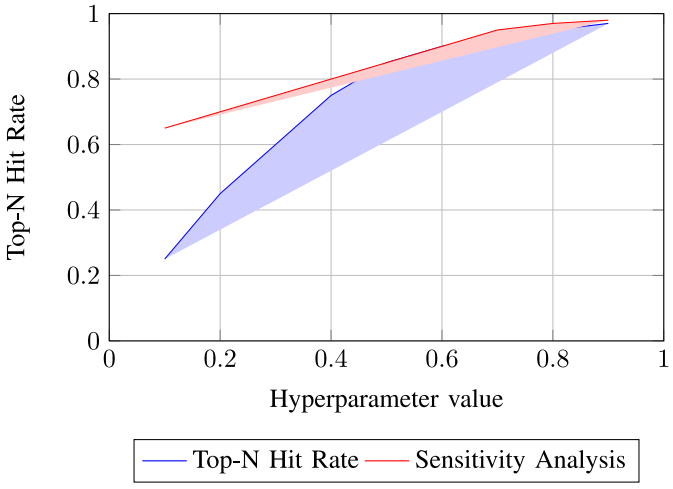

Fig. 4. Combined graph for Top-N Hit Rate and Sensitivity Analysis.

VI. Conclusion

In conclusion, federated learning on decentralized medical data has the potential to revolutionize personalized medical recommendations while ensuring the privacy and security of patient data. We have covered the key considerations such as data selection, preprocessing, model architecture, privacy, fairness, and evaluation metrics. Our proposed framework incorporates differential privacy techniques to protect patient privacy. We have discussed several evaluation metrics, including KL divergence, fairness, confidence intervals, top-N hit rate, sensitivity analysis, and novelty, to evaluate the performance of the federated learning system. we have addressing several challenges, about FL system which can become more resilient and adaptable to the complexities of decentralized healthcare data We believe the proposed framework and evaluation metrics can provide valuable insights into the system's effectiveness and guide the selection of optimal hyperparameters and model architectures.

References

[1] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, Oct. 2021, Art. no. 103164.

[2] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[3] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, "Secure healthcare data aggregation and transmission in IoT—A survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[4] A. Ullah, M. Azeem, H. Ashraf, N. Jhanjhi, L. Nkenyereye, and M. Humayun, "Secure critical data reclamation scheme for isolated clusters in IoT-enabled WSN," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2669–2677, Feb. 2022.

[5] S. Niknam, H. Dhillon, and J. Reed, "Federated learning for wireless communications: Motivation, opportunities and challenges," 2019, *arXiv:1908.06847*.

[6] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[7] Y. Shi, K. Yang, T. Jiang, J. Zhang, and K. B. Letaief, "Communication-efficient edge AI: Algorithms and systems," 2020, *arXiv:2002.09668*.

[8] J. Konecń, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Strategies for improving communication efficiency," 2016, *arXiv:1610.05492*.

[9] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, "A secure federated learning framework for 5G networks," 2020, *arXiv:2005.05752*.

[10] Y. Lin, S. Han, H. Mao, Y. Wang, and B. Dally, "Deep gradient compression: Reducing the communication bandwidth for distributed training," in *Proc. Int. Conf. Learn. Rep.*, 2018, pp. 1–14.

[11] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.

[12] G. Yang, Q. Zhang, and Y.-C. Liang, "Cooperative ambient backscatter communications for green Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1116–1130, Apr. 2018.

[13] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 72–80, Apr. 2020.

[14] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies," *IEEE Access*, vol. 7, pp. 175758–175768, 2019.

[15] R. Long, H. Guo, L. Zhang, and Y.-C. Liang, "Full-duplex backscatter communications in symbiotic radio systems," *IEEE Access*, vol. 7, pp. 21597–21608, 2019.

[16] Z. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[17] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[18] S. Nayak and R. Patgiri, "6G communication technology: A vision on intelligent healthcare," 2020, *arXiv:2005.07532*.

[19] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55– 61, Mar. 2020.

[20] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-preserving traffic flow prediction: A federated learning approach," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7751–7763, Aug. 2000.

[21] S. Gu, J. Jiao, Z. Huang, and S. Wu, "ARMA-based adaptive codlearning methods for 6G communications, transmission over millimeter-wave channel for integrated satellite-terrestrial networks," *IEEE Access*, vol. 6, pp. 21635–21645, 2018.

[22] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," 2022, *arXiv:1909.07972*.

[23] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, "A systematic review of IoT communication strategies for an efficient smart environment," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, 2022, Art. no. e3736.

[24] L. U. Khan et al., "Federated learning for edge networks: Resource optimization and incentive mechanism," 2019, *arXiv:1911.05642*.

[25] J. Kang, Z. Xiong, D. Niyato, H. Yu, Y.-C. Liang, and D. I. Kim, "Incentive design for efficient federated learning in mobile networks: A contract theory approach," in *Proc. IEEE VTS Asia–Pac. Wireless Commun. Symp.*, 2019, pp. 1–5.

Rani Kumari received the B.Tech. degree in computer science from the National Institute of Science and Technology, the M.Tech. degree in computer science from the Maulana Abul Kalam Azad University of Technology, and the Ph.D. degree from the Birla Institute of Technology, Ranchi, focused on optimizing digital image watermarking in the Fractional Fourier Domain, employing innovative metaheuristic approaches. She is a Seasoned Researcher and an Expert in the field of Computer Science, specializing in image and signal processing, heuristic algorithms, and machine learning. She has contributed significantly to scientific literature with several impactful journal articles and conference proceedings. Her involvement in sponsored projects, such as the Promotion of University Research and Scientific Excellence, reflects her commitment to advancing technology. Her enthusiasm for innovation extends to her recent certification through Coursera. She has made significant contributions to the academic community through her prolific publications in reputable journals and conferences. Her research endeavours span various domains, including wireless networks, sustainable energy technologies, medical recommendations, and digital watermarking. Notable journals, such as *Physical Communication*, *Sustainable Energy Technologies*, and *Assessments*, *ACM Transactions on Asian and Low-Resource Language Information Processing*, *Optik*, and *Frontiers in Neurorobotics*.

Dinesh Kumar Sah (Member, IEEE) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (Indian School of Mines) Dhanbad. He is actively seeking opportunities for significant research in organizations fostering professional development. With extensive coding experience across diverse technologies, he specializes in cross-layer and machine learning-based algorithms for wireless sensor networks and the Internet of Things. His research evidenced by nine journal articles, seven conference papers, and four book chapters published in renowned venues like *Computer Science Review* (Elsevier), *ACM Transactions on Sensor Networks*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Sustainable Energy Technologies and Assessments*, and *Computers and Electrical Engineering*. His work delves into diverse topics, such as sensor networks, TDMA-driven MAC for nodes scheduling, and acoustic signal-based indigenous real-time rainfall monitoring systems.

Shivani Gupta received the B.E. degree in computer science and engineering from the Madhav Institute of Technology and Science, Gwalior, India, in 2006, the M.Tech. degree from RGPV, Bhopal, India, in 2010, and the Ph.D. degree in machine learning from the Computer Science Program, Indian Institute of Information Technology, Design and Manufacturing Jabalpur in 2019. She is currently working as a Senior Assistant Professor with the Vellore Institute of Technology (Chennai), Chennai. Her current research interests include deep learning, machine learning, software defect prediction, data mining, and data analysis and data complexity measures.

Korhan Cengiz (Senior Member, IEEE) was born in Edirne, Turkey, in 1986. He received the B.Sc. degrees in electronics and communication engineering from Kocaeli University and in business administration from Anadolu University, Turkey, in 2008 and 2009, respectively, the M.Sc. degree in electronics and communication engineering from Namik Kemal University, Turkey, in 2011, and the Ph.D. degree in electronics engineering from Kadir Has University, Turkey, in 2016. Since March 2023, he has been a Senior Researcher with the Department of Information Technologies, University of Hradec Kralove, Kralove, Czech Republic. Since September 2022, He has been an Associate Professor with the Department of Computer Engineering, Istinye University, Istanbul, Turkey. Since April 2022, he has been the Chair of the Research Committee of the University of Fujairah, UAE. Since August 2021, he has been an Assistant Professor with the College of Information Technology, University of Fujairah, UAE. He is the author of more than 40 SCI/SCI-E articles, including IEEE INTERNET OF THINGS JOURNAL, IEEE ACCESS, *Expert Systems with Applications*, *Knowledge-Based Systems*, and *ACM Transactions on Sensor Networks*, five international patents, more than ten book chapters, and one book in Turkish. He is an editor of more than 20 books. His research interests include wireless sensor networks, wireless communications, statistical signal processing, indoor positioning systems, Internet of Things, power electronics, and 5G. His awards and honors include the Tubitak Priority Areas Ph.D. Scholarship, the Kadir Has University Ph.D. Student Scholarship, the Best Presentation Award in ICAT 2016 Conference, and the Best Paper Award in ICAT 2018 Conference. He is an Associate Editor of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *IEEE Potentials Magazine*, a Handling Editor of *Microprocessors and Microsystems* (Elsevier), an Associate Editor of *IET Electronics Letters*, and *IET Networks*. He serves several reviewer positions for IEEE INTERNET OF THINGS JOURNAL, IEEE SENSORS JOURNAL, and IEEE ACCESS. He serves several book editor positions in IEEE, Springer, Elsevier, Wiley, and CRC. He presented 40+ keynote talks in reputed IEEE and Springer Conferences about WSNs, IoT, and 5G. He is a Professional Member of ACM.

Nikola Ivković (Senior Member, IEEE) was born in Zagreb, Croatia, in 1979. He received the M.S. degree in computing and the Ph.D. degree in computer science from the Faculty of Electrical Engineering and Computing, University of Zagreb. His doctoral thesis was around swarm and evolutionary computation. He was the Head of the Department of Computing and Technology, Faculty of Organization and Informatics, University of Zagreb, where he is currently working as an Associate Professor. He teaches computer networks, operating systems, and computational intelligence related courses. He is a member of two research Laboratories - Artificial Intelligence Laboratory and the Laboratory for Generative Programming and Machine Learning, both with the Faculty of Organization and Informatics, University of Zagreb. His research interests include computational intelligence and optimization, computer networks, and security. He was a member of committees for creating new university study programs. He serves as a regular reviewer for high quality scientific journals and takes part in a number of international conference committees. He gave several invited talks at international scientific conferences and guest lectures on different universities in Europe and Asia. He joined Association for Computing Machinery and the Institute of Electrical and Electronics Engineers in 2008.