Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 2 (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Privacy- Enhanced Fungal Infection Detection: Leveraging Differential Privacy and Federated Learning in Healthcare System

Mr. Kanhaiya Jee Jha[1], Dr. Gaurav Kumar Ameta[2], Dr. Esan P Panchal[3], Keyurbhai A. Jani[4], Pramod Tripathi[5], Dr. Shruti B. Yagnik[6]

[1]Swarrnim Startup University, Ahmedabad, India
Email ID: Kanhaiya.jeejha19@gmail.com
[2]Parul University, Vadodara, India
Email ID: gauravameta1@gmail.com
[3,4,5]Lecturer, Information Technology Department, Gujarat Technological University, Ahmedabad, India
Email ID: esan.gpg@gmail.com, keyur.soft@gmail.com, csharp.pramod@gmail.com
[6]Associate Professor, Information Technology, Indus University, Ahmedabad - 382115, Gujarat, India
Email ID: shrutiyagnik.ce@indusuni.ac.in
[1]0009-0007-2804-1778,
[2]0000-0002-7463-2583,
[3]0000-0002-1667-0864,
[4]0000-0002-6050-9365,
[5]0000-0003-3464-7446,
[6]0000-0002-9514-9283

Cite this paper as: Mr. Kanhaiya Jee Jha, Dr. Gaurav Kumar Ameta, Dr. Esan P Panchal, Keyurbhai A. Jani, Pramod Tripathi, Dr. Shruti B. Yagnik, (2025) Privacy- Enhanced Fungal Infection Detection: Leveraging Differential Privacy and Federated Learning in Healthcare System. *Journal of Neonatal Surgery*, 14 (2), 142-153.

ABSTRACT

In the era of big data, safeguarding the privacy and security of sensitive healthcare information is predominant. This research paper investigates the integration of differential privacy and federated learning to create a robust framework for privacy-preserving analysis of fungal infection data. The proposed framework ensures the confidentiality of individual patient data while enabling collaborative analysis across multiple healthcare organizations. Differential privacy mechanisms are employed to provide strong privacy guarantees, ensuring that the inclusion of individual data does not compromise overall privacy. Federated learning facilitates decentralized data processing, minimizing the risk of data breaches by keeping data on local premises.

Extensive experiments and simulations were conducted using real-world fungal infection datasets to assess the framework's effectiveness and feasibility. The results indicate that the framework effectively preserves data privacy while maintaining better performance metrics in fungal infection detection. The framework demonstrated a significant reduction in privacy risks without compromising the quality of the analytical outcomes. This study's findings contribute to advancing privacy-preserving methodologies in healthcare data analysis, promoting secure data-sharing and collaborative efforts within the healthcare system.

Keywords: *Differential Privacy, FedAvg, Federated learning, Health data privacy, Privacy Protection.*

1. INTRODUCTION

Differential privacy is a concept and framework in the field of privacy-preserving data analysis and statistics. It addresses the challenge of extracting valuable insights from sensitive datasets while protecting the privacy of individual contributors. The fundamental goal of differential privacy is to ensure that the inclusion or exclusion of a single individual's data does not significantly affect the outcome of a computation or analysis.

In simpler terms, it provides a mathematical definition of privacy that allows for the robust analysis of data while minimizing the risk of revealing sensitive information about any specific individual within the dataset. This is particularly crucial in today's data-driven world, where vast amounts of personal information are collected and analyzed for various purposes, such as research, policy-making, and machine learning.

The core principle of differential privacy is based on the concept of adding controlled noise to the data or the results of computations, making it more challenging for an external observer to identify the contribution of any single individual. The noise ensures that the statistical properties of the data remain intact while providing a level of protection against potential privacy breaches (al. D. C., 2022).

Key components and principles of differential privacy include:

- **Privacy Guarantee**: Differential privacy provides a quantifiable measure of privacy, typically denoted by a parameter ε (epsilon). A smaller ε value implies a stronger privacy guarantee.
- **Randomized Response**: To achieve differential privacy, data is often randomized or perturbed through techniques like adding noise, shuffling, or introducing randomness into the data collection process.
- **Data Aggregation**: Aggregating data at a higher level, such as summarizing statistics, can help in protecting individual privacy by preventing the extraction of detailed information about specific individuals.
- **Formal Framework**: The concept is formalized through mathematical definitions and equations, allowing researchers and practitioners to rigorously evaluate and guarantee the level of privacy provided by a particular mechanism.

Differential privacy has gained significant attention and adoption, especially in contexts where privacy concerns are paramount, such as healthcare, finance, and government data analysis. As technology continues to advance, the importance of differential privacy in balancing data utility and individual privacy is expected to grow. Researchers and practitioners continually explore new techniques and applications to enhance the effectiveness and practicality of differential privacy in real-world scenarios (al. C. W., 2020).

Federated Learning is a machine learning approach that enables training models across decentralized and distributed devices or servers while keeping data localized. The central idea is to train a global model collaboratively without exchanging raw data between devices or a central server. This approach is particularly valuable in scenarios where data privacy and security are crucial, such as in healthcare, finance, and Internet of Things (IoT) applications.

One of the key challenges addressed by Federated Learning is the need to train models on data that cannot be easily centralized due to privacy concerns, legal constraints, or the sheer volume of information distributed across multiple devices. Instead of sending raw data to a central server for training, Federated Learning allows devices to compute model updates locally and share only the updates with the central server or other devices. This way, the raw data remains on the local devices, providing a higher level of privacy and security (Welling, 2013).

"Fed Avg" or Federated Averaging is a specific algorithm used in Federated Learning to aggregate model updates from multiple devices. The process involves the following steps:

Step -1 Initialization: A global model is initialized on a central server.

Step -2 Local Training: Each device or client trains the model locally on its own data. This local training can involve multiple iterations to improve the model's performance.

Step -3 Model Update: After local training, the device computes the difference or update between its local model and the global model.

Step -4 Aggregation: The model updates from all participating devices are aggregated on the central server. In Federated Averaging, this aggregation is often done by computing the average of the model updates.

Step -5 Global Model Update: The aggregated update is applied to the global model on the central server.

Iterative Process: Steps 2 to 5 are repeated for multiple rounds, allowing the global model to gradually improve without the need for centralizing raw data.

Federated Averaging provides a mechanism for collaborative learning while preserving privacy. By averaging the updates from multiple devices, it mitigates the impact of potentially noisy or outlier updates, ensuring a more robust and accurate global model.

Federated Learning, including algorithms like Federated Averaging, has gained attention for its applications in various domains, offering a privacy-preserving alternative to traditional centralized machine learning approaches.

2. PROPOSED WORK

Federated learning has proven to be a potent tool for handling diverse medical datasets in real-world scenarios, employing a cluster of machines for its operations. Through experiments conducted on CloudLab, a dedicated testbed for research in networking and distributed computing, various deep learning models and federated optimization strategies were assessed. Notably, Inception-v3 and EfficientNetB0 consistently emerged as the top-performing models, achieving high accuracy on test sets. Among the federated optimization strategies, FedAvg demonstrated superior performance, with FedAvgM closely following as the second-best strategy in the evaluations. This research underscores the effectiveness of federated learning in the medical domain and the significance of selecting appropriate models and optimization techniques for optimal outcomes. (1. M. Abadi, 2016)

To safeguard patient data, a proposed solution integrates homomorphic encryption with federated learning to design and implement a privacy-protected diabetes prediction system. Experimental results reveal that this approach not only overcomes information silos among hospitals but also successfully gathers patient information from various healthcare institutions while ensuring robust privacy protection. This innovative and practical work holds significant relevance in the current social context, offering potential solutions for diabetes treatment in the medical domain. Furthermore, it is poised to provide novel insights into multi-party data integration across diverse fields in the future. (Islam)

Due to the escalating number of privacy breaches concerning personal data, there's a growing necessity to develop methods that prioritize user privacy. In response, an algorithm has been introduced, employing a federated approach to predict whether a patient is experiencing breast cancer by utilizing data from multiple hospitals. This method ensures the protection of user data by allowing hospitals to securely train their models without transmitting sensitive information to a central server. A comparison with the standard approach was conducted to assess the performance of the federated approach. The results indicated that the federated learning model achieved accuracy levels comparable to the traditional model. While this approach has advantages, it also has limitations, which are comprehensively discussed in this paper, providing an overview of the concept of federated learning. (Adam)

The integration of Federated Learning and Software-Defined Networking (SDN) aims to establish an effective malware detection method and implement a mitigation mechanism, fostering the creation of a robust and automated healthcare sector network system with enhanced privacy preservation features. The constant evolution of new malware attacks on hospital Information and Communication Technologies (ICEs) has left the healthcare industry in a perpetual state of uncertainty. The vast array of opportunities presented by daily advancements in medical devices and their interconnected coordination remains largely overlooked by many healthcare operators and patients, contributing to a lack of focused direction. (Deng, 2012)

This solution involves the participation of four clients in the form of hospital networks, constructing a federated learning experimental architecture with diverse geographical representation to achieve the highest possible accuracy rate while ensuring privacy preservation. Leveraging logistic regression with cross-entropy for detection, SDN plays a crucial role in the latter part of the research, facilitating the initial development phases of the system and implementing malware mitigation based on policy enforcement. (Mammen, 2021)

The comprehensive evaluation concludes with a system that not only demonstrates accuracy but also emphasizes the importance of privacy. This challenges the necessity of continuing with traditional centralized systems that, despite offering various functionalities, fall short in ensuring privacy. (S. Vishnu, 2020)

Federated Learning (FL) is a decentralized approach to machine learning, allowing individual devices to train global models without exchanging raw data. This work extends the original FL algorithm, Federated Averaging (FedAvg), by incorporating consensus theory. In contrast to typical FL algorithms, the resulting approach, termed FedLCon, eliminates the need for a coordinating server—preventing a single point of failure and the necessity for universal trust among clients. Additionally, the consensus framework is applied to the Adaptive Federated Learning (AdaFed) algorithm, an extension of FedAvg featuring an adaptive model averaging procedure. Performance comparison tests are conducted within the context of a real-world COVID-19 detection scenario. (Goyal, 2019)Federated Learning (FL) facilitates the collaborative learning of a global predictive model among multiple users without revealing their individual datasets. Despite the adoption of privacy-preserving schemes to safeguard local updates, a significant challenge arises when users with suboptimal updates impede the convergence rate and compromise the model's utility. While some recent efforts aim to address both privacy and irregular user issues simultaneously, existing methods still fall short in terms of accuracy and efficiency. This is primarily attributed to the inefficiency caused by complex cryptographic algorithms and the inadequacy of strategies to effectively remove irregular users, impacting model usability.

To tackle these challenges, we introduce SAP-IU, a novel and efficient federated learning scheme that concurrently addresses irregular user removal and privacy protection. Our approach begins with the design of TrustIU, a unique removal algorithm for irregular users, which calculates user weights using the cosine metric. This ensures that the global model predominantly reflects the contributions of high-quality data. We further implement a secure weighted aggregation protocol for TrustIU to safeguard users' sensitive information, including local updates and data quality. Additionally, our scheme remains robust to user dropouts throughout the entire training process. Comprehensive experiments demonstrate that SAP-IU outperforms

previous approaches in terms of training accuracy and efficiency (AB, 2020).

The present computer-aided diagnosis systems utilizing deep learning methods have become crucial in the realm of medical imaging. Collaborative disease diagnosis across multiple medical institutions has gained popularity, but the extensive annotations required impose a substantial burden on medical experts. Moreover, centralized learning systems face challenges related to privacy protection and model generalization. In response to these issues, we introduce two federated active learning approaches for collaborative disease diagnosis across multiple centers: Labeling Efficient Federated Active Learning (LEFAL) and Training Efficient Federated Active Learning (TEFAL) (R. Shao, 2019).

LEFAL employs a task-agnostic hybrid sampling strategy, considering data uncertainty and diversity simultaneously, to enhance data efficiency. TEFAL assesses client informativeness using a discriminator to improve client efficiency. Evaluation on the Hyper-Kvasir dataset for gastrointestinal disease diagnosis reveals that, with only 65% of labeled data, LEFAL achieves 95% performance on the segmentation task compared to using the entire labeled dataset. Additionally, on the CC-CCII dataset for COVID-19 diagnosis, TEFAL attains an accuracy of 0.90 and an F1-score of 0.95 with only 50 iterations in the classification task. Extensive experimental results demonstrate that our proposed federated active learning methods surpass state-of-the-art approaches in both segmentation and classification tasks for collaborative disease diagnosis across multiple centers (Perepu, 2020).

The historical medical data of patients plays a crucial role in advancing healthcare by enabling intelligent health diagnosis and disease prediction. Traditional intelligent health diagnosis systems often collect data from various medical institutions or laboratories and utilize machine learning algorithms for disease prediction. However, these systems face challenges as medical institutions may possess incomplete patient data due to consultations with different specialists across various hospitals during the treatment process (B. Liu, 2020).

To address this issue, we introduce a secure and intelligent federated learning framework for health diagnosis, integrating a blockchain-based incentive mechanism and a marketplace facilitated by non-fungible tokens (NFTs). NFTs are utilized to establish clear ownership and accessibility parameters for patient data, with an NFT marketplace managing access to historical medical records. An elaborate incentive mechanism, considering factors like data quality, relevance, and frequency of data uploads, etc., is implemented to reward or penalize patients based on their contributions to the global model. (T. Li, 2018)

The Polyak-averaging technique is employed for aggregating local models into a cohesive global model. Extensive analysis demonstrates that our proposed model achieves performance comparable to centralized machine learning models while ensuring enhanced security and access to superior data. The results highlight the effectiveness of the blockchain-based incentive mechanism in promoting patient participation and improving the overall quality of the global model (Agarap, 2018).

The Industrial Internet of Things (IIoT) is a vital part of Industry 4.0, where smart technologies play a big role. When we use machine learning along with IIoT, we get a thriving smart industry. But there's a challenge: the data used to train these machine learning models has sensitive information. Sharing this data can lead to leaks of important information, putting data security and privacy at risk in IIoT (Y. Zhao, 2018).

To tackle this issue, we suggest a privacy-preserving data aggregation scheme for IIoT called FLPDA, which is based on federated learning. The idea is to aggregate data while protecting individual user model changes, preventing reverse analysis attacks from industry administration centers. In each round of data aggregation, we use the PBFT consensus algorithm to choose an IIoT device in the aggregation area as the starting point and aggregation node. To ensure data fault tolerance and secure sharing, we combine the Paillier cryptosystem and secret sharing (al., 2019).

Through security analysis and performance evaluation, we find that our scheme effectively safeguards data privacy and can withstand various attacks. Importantly, it has lower communication, computational, and storage requirements compared to existing schemes. In simpler terms, our approach helps keep your data private and secure, and it's more efficient than other methods currently in use (W. Luo, 2013).

When we connect the Internet of Things (IoT) deeply with the medical field, it creates what we call the Internet of Medical Things (IoMT). In IoMT, doctors use patient data collected from mobile devices, analyzed with the help of smart systems using artificial intelligence (AI), to treat diseases. But sometimes, the traditional AI systems can have flaws that might accidentally share patient privacy data (al, 2020).

To solve this, we suggest using a privacy-focused method called federated learning (FL) for IoMT. FL helps create a global model for disease diagnosis by bringing together data from different parties. However, FL still has trouble defending against inference attacks where someone tries to figure out sensitive information. In our approach, we propose a way to enhance privacy in disease diagnosis using FL for IoMT.

Here's how it works: First, we rebuild medical data using a special technique called a variational autoencoder. Then, we add a layer of differential privacy noise to protect against inference attacks. This data is used to train local disease diagnosis

models, keeping patients' information private. Additionally, to encourage people to join in and share their data for FL, we suggest a reward system (Goetz, 2020).

We tested our method using the arrhythmia database from the Massachusetts Institute of Technology and Beth Israel Hospital (MIT-BIH). The results showed that our approach lowers the chances of reconstructing patient medical data while still maintaining accurate heart disease diagnosis. In simple terms, our method makes sure patient data stays private while effectively diagnosing heart diseases (al K. K.-Q., 2022).

3. MOTIVATION FOR PROPOSAL

With the increase in data breaches and privacy concerns related to the sharing of sensitive information, there is a pressing need for secure methods of data analysis and sharing. By focusing on privacy-enhancing techniques for disease data, you can address a relevant and timely issue.

Exploring the intersection of differential privacy, federated learning, and federated averaging in the context of disease data privacy may lead to new insights, approaches, and solutions that could have a significant impact on the field and drive innovation in privacy-preserving technologies.

By combining these privacy-enhancing techniques in the analysis of disease data, researchers can unlock new possibilities for collaboration and insights while upholding the privacy rights of individuals. This approach not only addresses current concerns regarding data privacy but also has the potential to drive innovation in the development of privacy-preserving technologies for a range of applications beyond disease data.

4. DATASET

Dataset contains 4920 data points with 134 attributes. Attributes data types include float64 (1), int64 (132) and object (1). Few attributes are listed below

Itching	high_fever	Phlegm
skin_rash	sunken_eyes	throat_irritation
nodal_skin_eruptions	Breathlessness	redness_of_eyes
continuous_sneezing	Sweating	sinus_pressure
Shivering	Dehydration	runny_nose
Chills	Indigestion	Congestion
joint_pain	Headache	chest_pain
stomach_pain	yellowish_skin	weakness_in_limbs
Acidity	dark_urine	fast_heart_rate
ulcers_on_tongue	Nausea	pain_during_bowel_movements
muscle_wasting	loss_of_appetite	pain_in_anal_region
Vomiting	pain_behind_the_eyes	bloody_stool
burning_micturition	back_pain	irritation_in_anus

The target variable ‘Prognosis’ having following class names

['Fungal infection' 'Allergy' 'GERD' 'Chronic cholestasis' 'Drug Reaction’ ‘Peptic ulcer disease' 'AIDS' 'Diabetes "Gastroenteritis' 'Bronchial Asthma' 'Hypertension ' 'Migraine' 'Cervical spondylitis’ ‘Paralysis (brain hemorrhage)' 'Jaundice' 'Malaria' 'Chicken pox "Dengue' 'Typhoid' 'hepatitis A' 'Hepatitis B' 'Hepatitis C "Hepatitis D' 'Hepatitis E' 'Alcoholic hepatitis' 'Tuberculosis "Common Cold' 'Pneumonia' 'Dimorphic hemorrhoids(piles)' 'Heart attack "Varicose veins' 'Hypothyroidism' 'Hyperthyroidism' 'Hypoglycemia "Osteoarthristis' 'Arthritis' '(vertigo) Paroymsal Positional Vertigo "Acne' 'Urinary tract infection' 'Psoriasis' 'Impetigo']. Fig 1 shows the data distribution over each class of target variable ‘prognosis’ and fig 2 shows Correlation between various attributes.

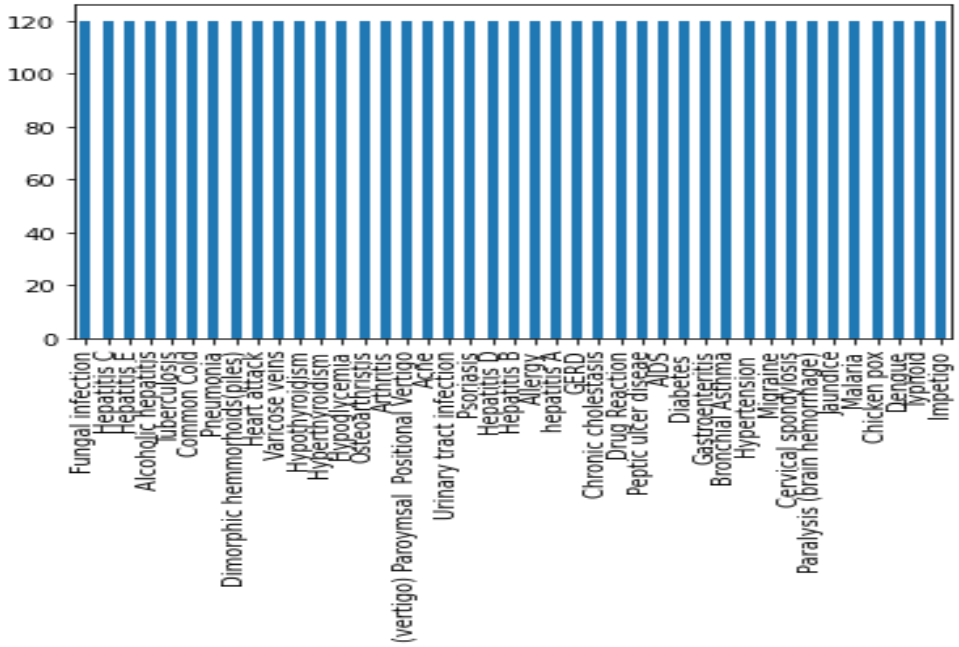

Fig 1– Data distribution over each class of target variable 'prognosis' (kaggle, n.d.)

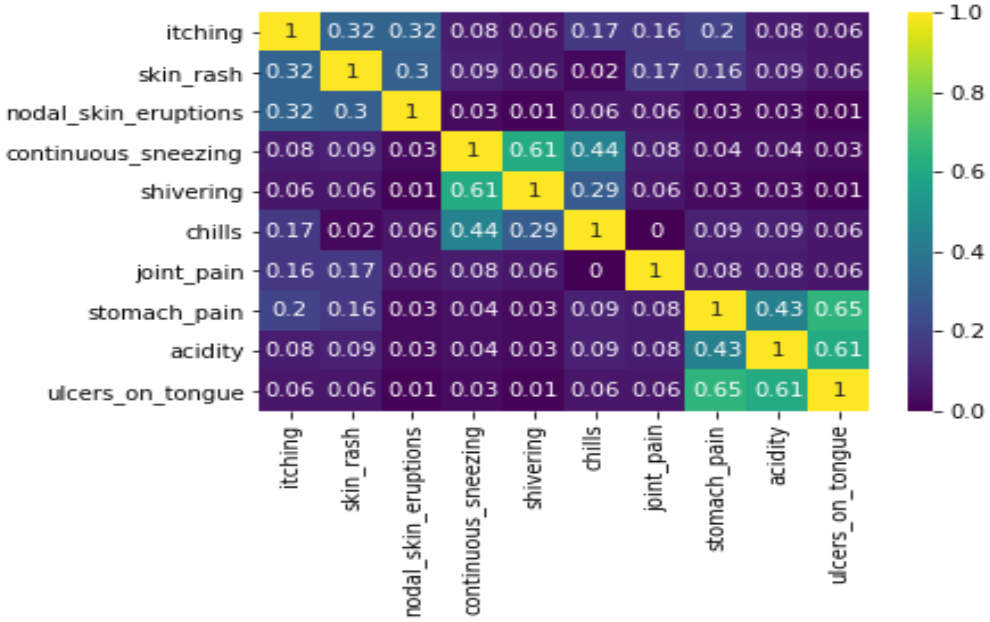

Fig 2 – Correlation between various attributes (kaggle, n.d.)

5. PROPOSED ARCHITECTURE AND SOLUTION

Federated Learning is a machine learning approach that enables model training across decentralized devices or servers without exchanging raw data. Privacy is a significant concern in federated learning, and the data transfer process is designed to protect sensitive information. Here's an overview of the data transfer process in federated learning with a focus on privacy.

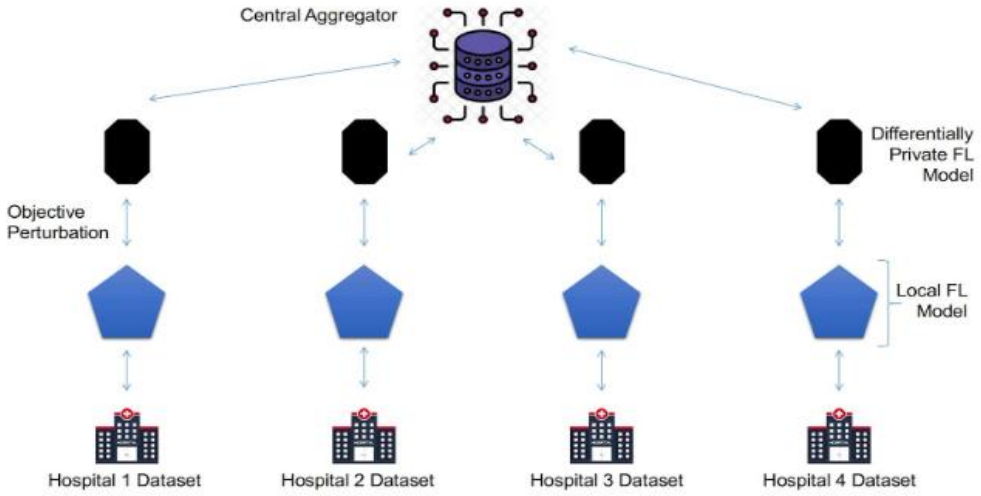

Fig-3 Proposed architecture: Send perturbed model to central aggregator and receive updated central model

In the model above, in the first step, Hospital 1 data will be used to create a model with differential privacy by adding noise. This model will then be transferred to the central aggregator. At the central aggregator, FedAvg will be applied, resulting in the creation of the central model. In the next step, the central model will be transferred back to Hospital 1 from the central aggregator. Same process will be repeated for hospital 2 & hospital 3 and result will be checked. Here, every model sent from the hospital are sent with added Gaussian noise such that patient health records cannot be re-constructed.

Algorithm -1 (Federated Averaging)

Algorithm 1: Federated Averaging

Result: Returns final model to clients

The k clients are indexed by k.
B is the local minibatch size.
E is the local number of epoch.
η_t is the learning rate.
Server Executes:-
initialization w_0;
foreach *round* t=1,2,3..... **do**
  $m \longleftarrow max(C.K, 1)$
  $S_i \longleftarrow randomsetofmclients$
  foreach *client* $k \in S_t$ *in parallel* **do**
    $w_{t+1}^k \longleftarrow clientupdate(k, w_t)$
    $w_{t+1} \longleftarrow \sum_{k=1} \frac{n_k}{n} w_{t+1}^k$
  end
end
Client Update(k,w): //Run on client k
$\beta \longleftarrow (splitp_k intobatchesofsizeB)$
foreach *local epoch i from 1 to E* **do**
  foreach *batch* $b \in \beta$ **do**
    $w \longleftarrow w - \eta \nabla l(w : b) + \theta_t$
  end
  return w *to server*
end

In the federated optimization setup, the central aggregator computes the average of the client model parameters, with each client's contribution being weighted, after every communication round. In our proposed method, we transmit model parameters to the central aggregator with added differential privacy, concealing each client's individual contribution during the aggregation process. We adopted the following method to produce model parameters with differential privacy:

Figure 2 is derived from a variant of Stochastic Gradient Descent known as DP-SGD, which incorporates differential privacy. This modified algorithm adjusts the traditional mini-batch stochastic optimization process to ensure differential privacy guarantees.

To ensure privacy for each data point in the batch, the algorithm includes Gaussian noise that obscures the most substantial gradient. Let's denote C as the intended limit for the maximum gradient norm. For every data point in the sample, the algorithm calculates its parameter gradient. If the norm of this gradient exceeds the value of C, it is scaled down or "clipped" to match C.

Algorithm -2 (Differentially Private SGD Algorithm)

Algorithm 2: Differentially Private SGD (Outline)

Result: θ_T and compute the overall privacy cost (ϵ, δ) using a privacy accounting method.

Input:-Examples x_0,.....,x_n,

loss function

$$\mathcal{L}(\theta) = \frac{1}{n}\sum_{i}^{n}\mathcal{L}(\theta), x_i$$

Parameters: learning rate η_t,noise scale σ, group size L, gradient norm bound C.

initialization θ_o randomly;

foreach $t\ \epsilon[T]$ **do**

Take a random sample L_t *with sampling probability* $\frac{L}{N}$

Compute gradient

For each $i\epsilon L_t$

$$computeg_t(x_i) \longleftarrow \Delta\theta_t\mathcal{L}(\theta_t, x_i)$$

Clip gradient

$$\widetilde{g}_t \longleftarrow \frac{g_t(x_i)}{max(1, \frac{||g_t(x_i)||2}{C})}$$

Add noise

$$\widetilde{g}_t \longleftarrow \frac{1}{L}(\sum_{i}\widetilde{g}_t(x_i) + N(0, \sigma^2C^2I)$$

Descent

$$\theta_{t+1} \longleftarrow \theta_t - \eta_t\widetilde{g}_t$$

end

Objective perturbation methods are implemented on the local model before sending it to the central aggregator. The primary aim of the client-trained model is to determine parameters that effectively map inputs to outputs while minimizing an error function. Stochastic gradient descent is employed as a method to iteratively adjust these parameters towards optimal values.

To ensure data security, we've utilized a variant of differentially private stochastic gradient descent. This approach is defined by the following update rule, where the parameter C represents the clipping parameter, setting the maximum limit on the l2-norm for each gradient update, represents a function that adjusts a given vector to ensure its 12-norm does not exceed the value C. Additionally, it denotes the noise multiplier, which signifies the relationship between the clipping parameter and the standard deviation of the noise added to each gradient update.

$$[x]c = \frac{x}{\left(1, \frac{||x||2}{c}\right)}$$

We've employed a straightforward approach involving clients that are independent and identically distributed (IID), each equipped with local models. Gaussian noise is added to the gradient of these models before transmitting them to the central aggregators. The central aggregators utilize the FedAvg algorithm to combine these gradients and construct the final model, which is then distributed to all IID nodes.

Algorithm-3 (Differentially Private Federated Learning Algo)

Algorithm 3: Differentially private Federated Learning

Result: Returns final model to clients
The k clients are indexed by k.
B is the local minibatch size.
E is the local number of epoch.
η_t is the learning rate.
Server Executes:-
initialization w_0;
foreach *round t=1,2,3.....* **do**
  $m \longleftarrow max(C.K, 1)$
  $S_i \longleftarrow randomsetofmclients$
  foreach *client* $k \in S_t$ *in parallel* **do**
    $w_{t+1}^k \longleftarrow clientupdate(k, w_t)$
    $w_{t+1} \longleftarrow \sum_{k=1}^{n} \frac{n_k}{n} w_{t+1}^k$
  end
end
Client Update(k,w): //Run on client k
$\beta \longleftarrow (split p_k$ into batches of size $B)$
foreach *local epoch i from 1 to E* **do**
  foreach *batch* $b \in \beta$ **do**
    $w \longleftarrow w - \eta \nabla l(w : b) + \theta_t$
    $\theta_t \longleftarrow assignrandomly$
    $\theta_{t+1} \longleftarrow \theta_t - \eta_t \tilde{g}_t$
    $\tilde{g}_t \longleftarrow Gaussiannoise$
  end
  return w to server
end

To create the privacy-preserving model, we have employed an objective perturbation technique. This involves adding noise to the objective function prior to optimizing across classifier spaces. At each node, DP-SGD collects gradient updates aggregated over mini batches, and then manages the process of clipping and applying noise to these gradients. It gets input C and σ and makes sure that the 12-norm of each gradient update is at mot C, and subsequently applies Gaussian noise with standard deviation σC to the gradient.

The primary model utilizes the Federated Averaging algorithm (FedAvg) to compute a weighted average based on the received model parameters, thereby constructing a new model. Subsequently, the central aggregator redistributes the newly weighted parameters of the main model to all nodes for continued learning. This iterative process can be repeated multiple times to enhance the performance of the main model.

6. RESULTS AND DISCUSSION

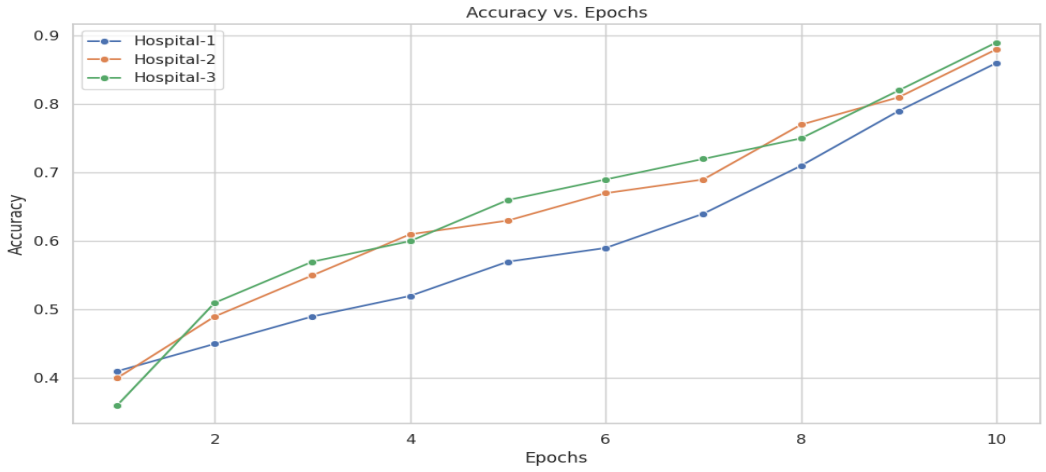

Fig-4 Accuracy of model on individual hospital data

Fig-4 shows the accuracy of a machine learning model trained on data from three different hospitals (Hospital-1, Hospital-2, and Hospital-3) over 10 epochs. The accuracy metric, which ranges from 0 to 0.9, is plotted on the y-axis, while the number of epochs is plotted on the x-axis.

Hospital-1 Starts with the lowest initial accuracy (~0.4) but improves steadily, achieving around 0.8 accuracy at the 10th epoch. Hospital-2 Begins with slightly higher accuracy than Hospital-1 and shows a steady increase, reaching close to 0.85 accuracy by the 10th epoch. Hospital-3 Starts with the highest initial accuracy (~0.45) and shows the fastest improvement initially. By the 10th epoch, its accuracy is similar to Hospital-2, around 0.85.

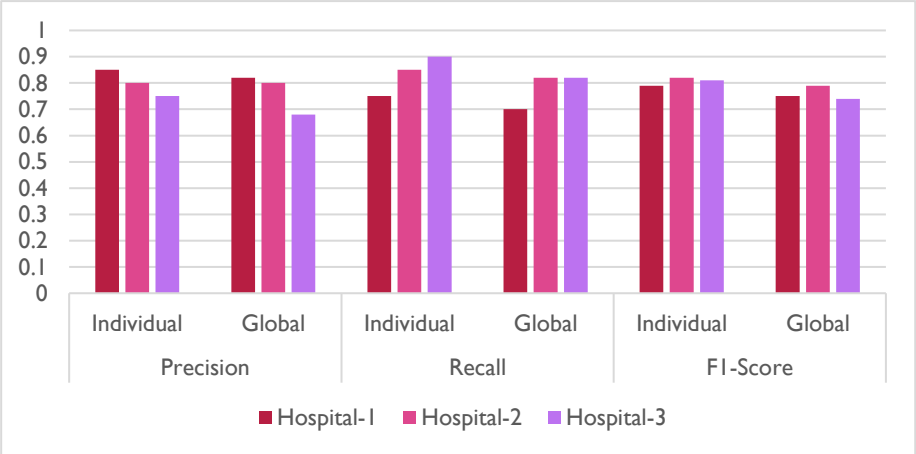

Fig-5 Performance comparison on Central aggregated Model

Fig-5 compares the performance of three hospitals (Hospital-1, Hospital-2, and Hospital-3) using different models (Individual and Global) across three performance metrics: Precision, Recall, and F1-Score.

Metrics:

Precision: Measures the accuracy of the positive predictions. High precision indicates that the model returns more relevant results than irrelevant ones.

Recall: Measures the ability of the model to identify all relevant instances. High recall indicates that the model returns most of the relevant results.

F1-Score: The harmonic mean of precision and recall, providing a single metric that balances both concerns.

Performance Comparisons:

Individual vs. Global Models:

The "Individual" model represents performance metrics for each hospital's unique model. The "Global" model represents performance metrics for a centralized aggregated model, likely combining data from all hospitals.

Hospital-1:

Precision: The individual model has slightly higher precision compared to the global model.

Recall: Both models show comparable performance.

F1-Score: Similar performance in both individual and global models, with the global model being slightly better.

Hospital-2:

Precision: The global model performs better than the individual model.

Recall: Slightly better recall in the global model compared to the individual.

F1-Score: The global model shows better performance.

Hospital-3:

Precision: The global model performs significantly better than the individual model.

Recall: The individual model has lower recall compared to the global model.

F1-Score: The global model performs better than the individual model.

Overall Observations:

The global model generally shows improved or comparable performance across all metrics and hospitals.

There is variability in the performance gains from the global model among the hospitals, with Hospital-3 benefiting the most. The individual models for each hospital show strong performance but do not consistently outperform the global model.

7. CONCLUSION

In this paper, we have explored the use of differential privacy, federated learning, and federated averaging to preserve the privacy of disease data. Our experimental results demonstrate the feasibility and effectiveness of this approach in protecting the privacy of sensitive healthcare information. Future work could involve applying these techniques to real-world healthcare datasets to evaluate their performance in practical settings. By leveraging these privacy-preserving techniques, we can ensure that individuals' privacy is protected while still enabling valuable analysis of disease data.

REFERENCES

[1] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard, et al. Tensorflow: a system for large-scale machine learning. In 12th USENIX symposium on operating systems design and implementation (OSDI 16), pages 265–283, 2016.

[2] D. J. Beutel, T. Topal, A. Mathur, X. Qiu, T. Parcollet, P. P. de Gusm˜ao, and N. D. Lane. Flower: A friendly federated learning research framework. arXiv preprint arXiv:2007.14390, 2020.

[3] M. Gharibi and P. Rao. Refinedfed: A refining algorithm for federated learning. In 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), pages 1–5, 2020.

[4] M. N. Islam. CT Kidney Dataset: Normal-Cyst-Tumor and Stone, 2020.

[5] Kaggle. Diabetic retinopathy detection, 2015.

[6] D. P. Kingma and J. Ba. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980, 2014.

[7] Larxel. Lung and colon cancer histopathological images, 2020.

[8] P. Patel. Chest X-ray (Covid-19 & Pneumonia), 2020.

[9] Substra Foundation, HealthChain Project, Retrieved July 1,2021,from https://www.substra.ai/en/healthchain-project.

[10] Deng, L. (2012). The mnist database of handwritten digit images for machine learning research. IEEE Signal Processing Magazine, 29(6), 141–142.

[11] Tian Li and Anit Kumar Sahu and Ameet Talwalkar and Virginia Smith (2019). Federated Learning: Challenges, Methods, and Future Directions. CoRR, abs/1908.07873.

[12] Priyanka Mary Mammen (2021). Federated Learning: Opportunities and Challenges. CoRR, abs/2101.05428.

[13] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity”, Journal of Computer and System Sciences, vol. 80. 2014, pp.974-999.

[14] S. Vishnu, S. R. J. Ramson, R. Jegan, “Internet of Medical Things (IoMT) - An overview”, Mar 2020.

[15] M. M. Nair and A. K. Tyagi and R. Goyal, “Medical Cyber Physical Systems and Its Issues”, vol. 165. Jan 2019.

[16] “Data Protection” [Internet]. TheICE. [cited 2022 Mar 12] Available from: https://www.theice.com/data-protection.

[17] Federated Learning, Ekkono Solutions AB. 2020 May.

[18] M. Hao, H. Li, G. Xu, Z. Liu, and Z. Chen, ``Privacy-aware and resourcesaving collaborative learning for healthcare in cloud computing," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2020, pp. 1_6.

[19] R. Shao, H. He, H. Liu, and D. Liu, ``Stochastic channel-based federated learning for medical data privacy preserving," 2019, arXiv:1910.11160.

[20] G. K. Gudur and S. K. Perepu, ``Federated learning with heterogeneous labels and models for mobile activity monitoring," 2020, arXiv:2012.02539.

[21] B. Liu, B. Yan, Y. Zhou, Y. Yang, and Y. Zhang, ``Experiments of federated learning for COVID-19 chest X-ray images," Tech. Rep., 2020.

[22] K. Ogata, Discrete-Time Control Systems. Upper Saddle River, NJ, USA: Prentice-Hall, 1995.

[23] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, andV. Smith, ``Federated optimization in heterogeneous networks," 2018, arXiv:1812.06127.

[24] A. F. Agarap, ``Deep learning using recti_ed linear units (ReLU)," 2018, arXiv:1803.08375.

[25] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated learning with non-iid data," arXiv preprint arXiv:1806.00582, 2018.

[26] X. Mei et al., "Artificial intelligence for rapid identification of the coronavirus disease 2019 (COVID-19)," medRxiv, 2020.

[27] W. Luo, A. Schwing, and R. Urtasun, "Latent structured active learning," in Proc. Adv. Neural Inf. Process. Syst., vol. 26, 2013, pp. 1–9.

[28] Y. Xu et al., "A collaborative online AI engine for ct-based COVID-19 diagnosis," medRxiv, 2020.

[29] J. Goetz, "Active learning in non-parametric and federated settings," Ph.D. thesis, 2020.

[30] H. T. Nguyen and A. Smeulders, "Active learning using pre-clustering," in Proc. 21st Int. Conf. Mach. Learn., 2004, p. 79.

[31] D. D. Lewis and W. A. Gale, "A sequential algorithm for training text classifiers," in Proc. SIGIR. Springer, 1994, pp. 3–12.

[32] K. Kostick-Quenet et al., "How NFTs could transform health information exchange," Science, vol. 375, no. 6580, pp. 500–502, 2022.

[33] L. Da Xu, W. He, and S. Li, ``Internet of Things in industries: A survey," IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2233_2243, Nov. 2014.

[34] J. Xu et al., "Federated learning for healthcare informatics," J. Healthcare Informat. Res., vol. 5, no. 1, pp. 1–19, 2021.

[35] D. C. Nguyen et al., "Federated learning for smart healthcare: A survey," ACM Comput. Surv., vol. 55, no. 3, pp. 1–37, 2022.

[36] L. Zhu and S. Han, "Deep leakage from gradients," in Federated Learning. Cham, Switzerland: Springer, 2020, pp. 17–31.

[37] C. Wu et al., "Mitigating backdoor attacks in federated learning," 2020, arXiv:2011.01767.

[38] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," 2013, arXiv:1312.6114.