Securing Healthcare Data: Federated Learning for Privacy-Preserving AI in Medical Applications

Venkatesh Popuri
Master's Degree in Information Systems Engineering and Management
Harrisburg University of Science and Technology, PA

doi: https://doi.org/10.37745/ijmt.2013/vol11n36482 Published August 06, 2024

Citation: Popuri V. (2024) Securing Healthcare Data: Federated Learning for Privacy-Preserving AI in Medical Applications, *International Journal of Management Technology*, Vol.11, No 3, pp.64-82

Abstract: *Federated Learning (FL) is a technique used when sharing raw data cannot be done because of privacy laws. FL is used to train machine learning algorithms on decentralized data. Electronic health records, which hold private patient data, are one type of such data. In FL, local models are trained, and the model parameters are then combined on a central server instead of sharing sensitive data. But this approach poses privacy risks, so before disclosing the model parameters, privacy protection measures such data confidentiality must be put in existence. During the pandemic, there is a need to improve the healthcare system. Numerous advancements in Artificial Intelligence (AI) technology are continuously being utilized in several healthcare domains. Federated Learning (FL), one such development, has gained popularity mostly because of its decentralized, cooperative approach to creating AI models. Since integrating privacy algorithms can affect the utility, it is important to strike a balance when it comes to privacy and utility in FL research. The goal is to use strategies such as data generalizing, feature selection for reducing dimensions, and reduction in the confidentiality process to maximize FL's effectiveness while preserving privacy. To create a predictive model for healthcare applications, this study also explores the idea of segmenting data based on attributes rather than records. It assesses the effectiveness of the model recommended by utilizing actual medical data.*

Keywords: federated learning, healthcare data security, privacy-preserving AI, medical applications, data protection, secure machine learning

INTRODUCTION

The analysis of sensitive data, particularly in the healthcare industry, is greatly enhanced by machine learning models. Diagnoses and treatment decisions can be supported by these algorithms' capacity to evaluate patient data and medical imagery. To enable early prevention, ML models can also be used to forecast the chance that patients would experience specific problems or consequences. Furthermore, through the provision of real-time, evidence-based suggestions, the integration of machine learning into medical systems can help healthcare providers make well-informed judgments. One study used machine learning to diagnose type 2 diabetes in patients using Electronic Health Records (EHR) [1]. Blockchain (BC) technology, which is renowned for its dependability and decentralized structure, can provide the security and trust components that the FL puzzle is missing. BC's architecture, which includes consensus methods and an immutable ledger, can make previously opaque FL operations verifiable and transparent. It guarantees that an action cannot be changed once it is recorded on the BC, allowing for a tamper-proof record of all transactions and model modifications. To create a foundation of verifiable confidence and allay worries over the integrity of data and models, this permanence is essential [2]. In the case of a pandemic, the smart healthcare system is anticipated to be crucial since it may offer senior patients remote medical care and shield them from potentially contagious illnesses like COVID-19 while they are in person at hospitals [3]. In this configuration, HE is only used following each local training cycle of the sites that are involved.

The encrypted updated weights are returned to the clients for decryption and integration into their models after the weight aggregation on the encrypted values is completed by the central server. Crucially, because the central server lacks access to the decryption key, it is unable to deduce which computations were carried out at specific peer locations and, as a result, cannot collect confidential or sensitive data [5]. In other words, homomorphic cryptography is the best method for handling personal health data in low-trust contexts because all model parameter processing takes place in the encrypted domain.

The healthcare system's extensive acceptance is nevertheless plagued by problems, despite its numerous potential benefits. To share health information, all parties engaged in the telemedicine system now rely on centralized storage. Many issues, including data breaches, a lack of trust and transparency, excessive costs, a lack of a patient-centric approach, and data privacy, are brought on by centralized data storage [6]. Consequently, proper handling of data privacy and security issues is crucial for any cloud-based service. In 2016, Google unveiled their approach to federated learning. Using this method, the client never transmits the raw data to the central or coordinating server. On the coordinating server, the model updates are posted [7]. Federated learning makes it possible for entities to work together to develop a global model without sending raw data to outside parties [8]. Cooperation and collaborative research between various research institutes and healthcare organizations are essential to improving health outcomes in global health emergencies. Cooperation and joint research may be made possible via federated learning [9]. Nevertheless, innocent federated learning systems are vulnerable to privacy and accountability risks, like model poisoning [10].

LITERATURE REVIEW

Federated learning has a wide range of applications in the healthcare industry, including drug development, medical imaging analysis, disease prediction, and customized therapy suggestions. Federated learning, for example, has been shown to be effective in enhancing disease diagnosis accuracy while protecting patient privacy across various healthcare facilities.

A medical privacy, also referred to as health privacy, is the practice of keeping records of patients secure and private. It involves maintaining the privacy of professional discussions among healthcare providers as well as the security of health data. The phrases can also be used to discuss modesty in medical settings as well as patients' physical seclusion from other individuals and healthcare providers while they are at a facility. Considerations in modern times include the extent of disclosure to businesses, insurance providers, and other outside parties. Increasing privacy issues brought forth by patient care management systems (PCMS) and electronic health records (EHR) must be addressed with initiatives to reduce medical errors and redundancy of services [11]. Many nations, including Australia, Canada, Turkey, the United States, New Zealand, and the Netherlands, have enacted legislation aimed at protecting people's privacy. Even so, numerous laws work better in theory than in reality. In order to fortify the legislation safeguarding healthcare facilities, the United States created the Health Insurance Portability and Accountability Act (HIPAA) in 1996. In 2018, the Information Security Regulation was superseded by the GDPR [12]. The EU Commission presented a proposal in 2012 to replace the EU Data Protection Directive with a European Data Security Regulations.EU citizens are allowed by regulation to request that search engines remove any identifiable data that may be linked to their name[13].GDPR went into force as a data security and privacy policy in the EU and the EEA on May 25, 2018. Furthermore, it applies to private information transfers outside of the EU and EEA [14].

Regarding machine learning and big data, privacy pertains to preventing hostile attempts that aim to obtain sensitive information from their target by deducing it from them, which may lead to unintentional data leaks[15].A growing number of businesses now rely on analytics using big data to complete their daily operations, changing the world of technology as big data's effects become increasingly confidential in the age of technology depends on our ability to control how our data is stored, updated, shared is becoming an urgent social problem as a result of the development of strong internet-based methods for data mining in recent years. The hazards for private security are increased by the essential elements of security for privacy and artificial intelligence (AI), which are being exacerbated by the growth of big data and the need for the management of confidential data. Large dataset analysis is a natural fit for modern AI techniques like DL, which are likely among the most effective ways to examine significant volumes of data in a reasonable length of time [16]. The powers of AI extend beyond data and analysis. Additionally, it can be used to rank, assess, classify, score, and sort people while feeding the gathered data into AI model training. The person's classified usually does not consent to this, and they usually have limited ability to change or challenge the conclusions of these assignments. One example of how such information could be used to impose restrictions on access to social assistance, housing, work, and money is China's social score system [17]. Two developments that characterize the modern medical landscape for patient characterization are electronic medical records and medical evidence-based practices [18]. However, privacy issues will arise from attacks on electronic health records. Artificial intelligence (AI) may predict or infer sensitive information from non-sensitive data using sophisticated methodologies. Keyboard typing patterns, for instance, can be utilized to deduce emotional states including anxiety, confidence, sorrow, and unease. Even more concerning are the possibilities that information about an individual's political beliefs, ethnic identity, sexual orientation, and even general health could be ascertained using activity logs, location data (COVID-19 tracing and track applications are excellent examples), and comparable measures [19-20].

RESEARCH METHODOLOGY

Data Collection and Pre-processing

The process of obtaining and quantifying information about a variable of interest is known as data collecting. Machines initially pick up knowledge from the data that humans provide them. The most crucial step in enabling our machine learning model to identify the right patterns is data collection. The precision of our model's outcome prediction also depends on the caliber of the data we supply to the system. A dataset that uses blood samples or other parameters to determine a person's health and whether or not they have a specific disease. The data is hand-made, and you can use it only for educational purposes. I looked up the percentage of each parameter, what would happen if it was high or low, and what diseases you might have if it was high or low. Based on all of this information and my searches, Furthermore, the data is already scaled inside the range (0,1).

The process of converting unprocessed data into a comprehensible format is known as data preparation. The first, and most important, stage in preparing the data for use is data preprocessing. The dataset has a large number of data points, so it is necessary to filter out uncertainties like missing values, null values, and irrelevant data. Remove the uncertainties from the dataset because they will negatively affect the accuracy of the results.

Dimensionality Reduction

The process of minimizing the number of features (or dimensions) in a dataset while preserving the maximum amount of information is called dimension reduction. This can be carried out for multiple purposes, including: Simplifying a model's complexity; Enhancing a learning algorithm's performance; or facilitating the data's visual representation. The AutoEncoder is a type of unsupervised artificial neural network that compresses data into smaller dimensions, often known as the bottleneck layer or code, and then uses decoding to recreate the original input. The bottleneck layer is extracted and used to reduce the dimensions when utilizing AutoEncoders for dimensionality reduction.

Auto Encoder: An unsupervised artificial neural network that compresses data into lower dimensions (bottleneck layer or code) in an attempt to encode it; to reconstruct the original input, it must first be decoded. Typically, an encoder and a decoder make up an auto encoder. The data is first encoded into a reduced dimension, representing the size of the bottleneck layer, by the encoder. The compressed data is then decoded by the decoder back into its original form. Because Auto Encoder is trying to recreate the input data, the number of output units must match the number of input units. The input data's compressed representation is stored in the bottleneck layer, also known as the code. Dimensionality reduction is carried out by extracting the compressed data representation from the input feature, or bottleneck layer (24--------> 22).

Handling Class Imbalance

The primary difficulty with decentralized learning is that each client's training data is class-imbalanced, which lowers learning accuracy. The worldwide imbalance in decentralized learning that is, the unequal collection of data across all clientsis the authors' primary area of concern. Since most machinery functions normally and defects are uncommon in machines, fault identification is very common [9]. Several advancements in class-imbalance learning have been developed in an attempt to address the issue. The FL framework incorporates a balanced cross entropy loss to mitigate privacy leakage and address the issue of class imbalance. The strategy used at the decision-making level modifies the discriminant probability and attempts to shift the output threshold in favor of minority classes. In order to have the same amount of examples as the class with the most examples, all classes will be oversampled using the Synthetic Minority Oversampling Technique (SMOTE).
Class differences also arise because certain illnesses may be far less common than others. To solve this, we provide a novel loss function that uses classical exercise to assign greater weight to the alternative class:

$$L=-\frac{1}{n}\sum_{i=1}^{n}[y_i \log \hat{y_i}\, wpos + (1-y_i)\log(1-\hat{y_i})\, wneg] \qquad 1$$

The masses in this case are determined based on their occurrences in the statistics and are represented by the symbols wpos and wneg, respectively, for the progressive (minority) and destructive (majority) sessions.
The proposed loss function, which up-weights the alternative class, successfully addresses the lesson difference during the ideal preparation process for requests. We propose a new loss function that

assigns more weight to the minority class during model training, thereby mitigating the observed class imbalance in the data. The binary class labels (y) in dataset D have values between 0 and 1, and they match the input features (X). The objective is to create a model that accurately classifies classes into majority and minority. We propose to add class weights and adjust the loss function to account for the class imbalance. The loss function has the following definition:

$$\text{L=-}\frac{1}{n}\sum_{i=1}^{n}[y_i \log \hat{y\imath}\, wpos + (1-y_i)\log(1-\hat{y\imath})\, wneg] \qquad 2$$

where $y_i$is the correct session identifier of the i-th segment and wpos and wneg are the loads assigned to the constructive (minority) and destructive (majority) lessons, respectively. For the i-th model, $\hat{y\imath}$ is the predicted possibility of the optimistic session.

Implementation of Privacy Preserving Federated Learning Architecture

The concept behind federated learning is that, in the event of data asymmetry, one can leverage the information from the other party's data to optimize their own model by means of the interactions of intermediate variables during the training phase. Federated learning may be further classified into two types based on the various data split: vertical federated learning (feature expansions) and horizontal federated learning (sample expansions).

Horizontal federated learning can be conceptualized as machine learning with sample extensions. Considering that D stands for data, X for features, Y for samples, and I for the data index. Federal learning that is horizontal can be shown as:

$$X_i = X_j, Y_i = Y_j, I_i \neq I_j \forall\, D_i, D_j, i \neq j \qquad 3$$

It indicates that various users have unique data that might or might not interact. The primary goal of horizontal federated learning is to support numerous users in jointly training a dependable model with their own data while maintaining data confidentiality and privacy. To guarantee that everyone participating in the training has the same feature domain, all parties' data must first be aligned before sample expansions can be made. This facilitates synchronous iteration and the development of the same model architecture by all stakeholders. In a similar vein, each participant in vertical federated learning has samples with unique properties.

Federated Network Algorithm: The primary goal of the federated learning network this research proposes is to facilitate the cooperative training of the same model by passing intermediate variables during the training phase. Here, we select gradients to be its intermediate variables in light of the fact that gradient descent trains the majority of neural networks. The gradient can depict the relationship between the model and the data, which helps in model training even though it cannot directly represent all of the data. A computational server and several learning clients make up the federated learning network's architecture, which is seen in Figure 1.

Learning Client: Learning customers possess their own confidential data and, provided that all the data is in alignment, their quantitative dimensions with those of other learners. The primary tasks of the learning client are to initialize the same initial model with other clients, train locally, extract gradients during training, compute gradients with the computing server, gather responses from the server, pass the results, update the model, and repeat the process until the model converges.

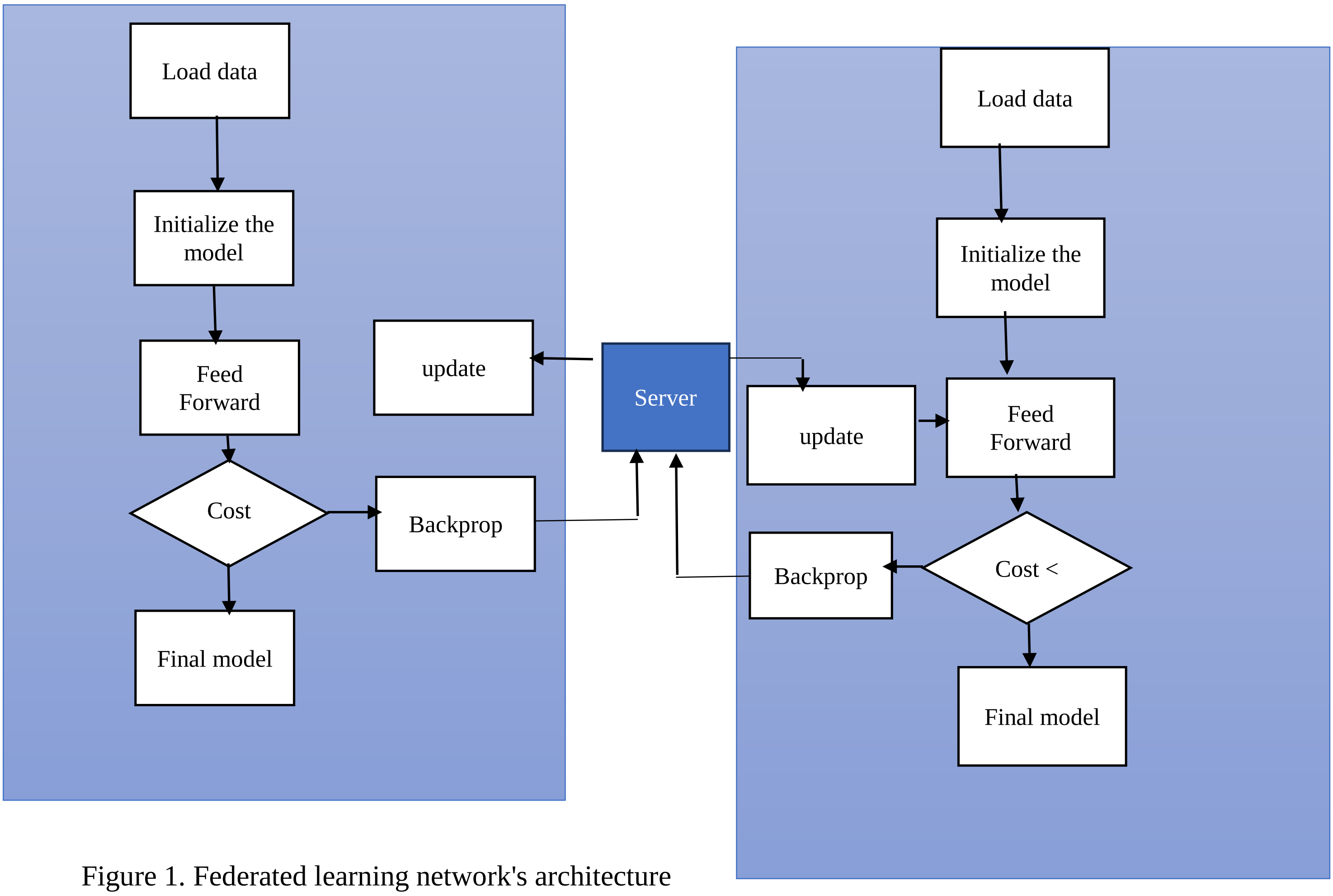


Figure 1. Federated learning network's architecture

Computing Server: An intermediary platform in the learning process is the computing server. Receiving the gradient information from various learning clients, calculating the gradients, combining the knowledge acquired by several models, and sending the outcome to each learning client independently are the primary tasks.

Homomorphic encryption and Secure Multi-Party Computation (SMPC) are two methods that are frequently employed in federated learning to guarantee security and privacy. SPDZ (pronounced "Speeds") is a particular protocol that enables safe calculations on encrypted data. Conversely, Federated Learning is a machine learning technique in which several parties work together to train a model without exchanging local data.

These methods seek to preserve the confidentiality of the training data while maintaining the efficacy of the model's training. Differential privacy is a popular method that preserves individual privacy by adding noise to the data while enabling the model to identify valuable trends. Additional methods include encrypting the data and enabling the model to be trained on it without disclosing the underlying data through homomorphic encryption and secure multi-party computation (SMC), which enables multiple parties to collaboratively compute the model without disclosing their data to one another. In the corporation situation, it is crucial for each partner to share their own distinct feature information in order for the group to collaboratively learn and train any classification algorithm. The SMC approach is employed by most currently in use technologies to transmit feature information with clients. Some methods safeguard privacy while sharing this feature information by using homomorphic encryption or distributed parity (DP) for data perturbation or cleaning.

Training and Testing Strategies

In the context of federated learning, privacy loss pertains to the inadvertent disclosure of confidential data regarding participants or training data via shared model updates or gradients. Membership inference attacks seek to ascertain if a certain data item was utilized during a model's training phase. One measure that indicates the probability or certainty that a specific data point was a part of the training set is the membership inference score. An adversary attempts to determine if a particular input was included in the training dataset by analyzing the model's predictions in the context of these assaults.

Simulation Results

The efficacy and evaluation of the proposed Federated Learning (FL) models that incorporate privacy preservation mechanisms are presented and discussed in this section. We plan to compare our proposed approach with eminent works in the field in order to assess our development. Using a lengthy simulation, our goal is to shed light on issues related to the accuracy, computational skill, and resilience in privacy safeguarding our models. We hope to increase our knowledge of the viability and potential of these models in real-world healthcare settings by providing a cohesive picture of these characteristics.

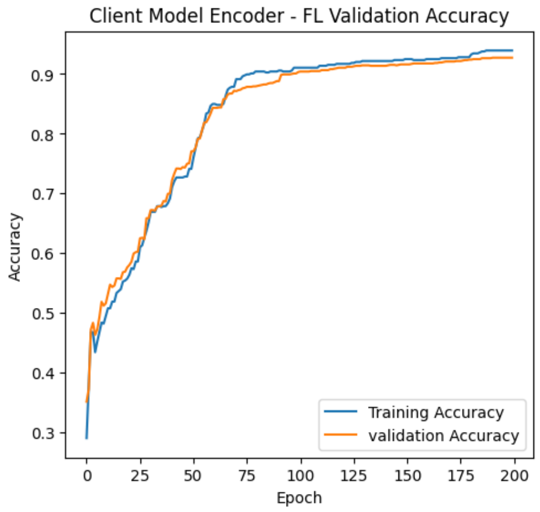
Performance Evaluation:

The application of advanced privacy-preserving techniques. The reduced privacy leakage measure attained by our proposed FL models, including local differential privacy, global differential privacy, secure multi-party computing, and aggregated gradient perturbation, may be attributed to them. When considered collectively, these techniques help to preserve personal privacy more and limit the leakage of sensitive information, both separately and collectively. It is clear from a comparison of the various approaches that our proposed FL models are more capable of safeguarding people' privacy. They are appropriate for secure and privacy-preserving applications in the healthcare industry because of their capacity to lower the risk of privacy breaches and safeguard the confidentiality of sensitive data, as demonstrated by the reduced privacy leakage measure companies.

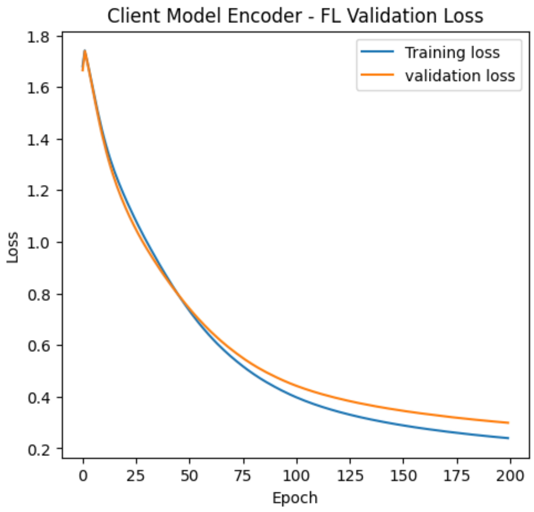
Table 1. Classification report client and global model

1.	**Precision**	**Recall**	**F1_score**	**Support**
0	0.91	0.99	0.95	192
1	0.93	0.78	0.84	209
2	0.95	0.95	0.95	219
3	0.91	0.93	0.92	210
4	0.99	0.98	0.98	207
	0.98	0.93	0.91	214
Accuracy			0.93	1251
Macro avg	0.96	0.94	0.95	1251
Weighted avg	0.96	0.96	0.96	1251

	Precision	**Recall**	**F1_score**	**Support**
0	0.91	0.99	0.95	192
1	0.92	0.81	0.86	209
2	0.96	0.95	0.96	219
3	0.92	0.93	0.93	210
4	0.99	0.98	0.98	207
5	0.90	0.93	0.92	214
Accuracy			0.93	1251
Macro avg	0.93	0.93	0.93	1251
Weighted avg	0.93	0.93	0.93	1251



Client Model Encoder - FL Validation Accuracy



Client Model Encoder - FL Validation Loss

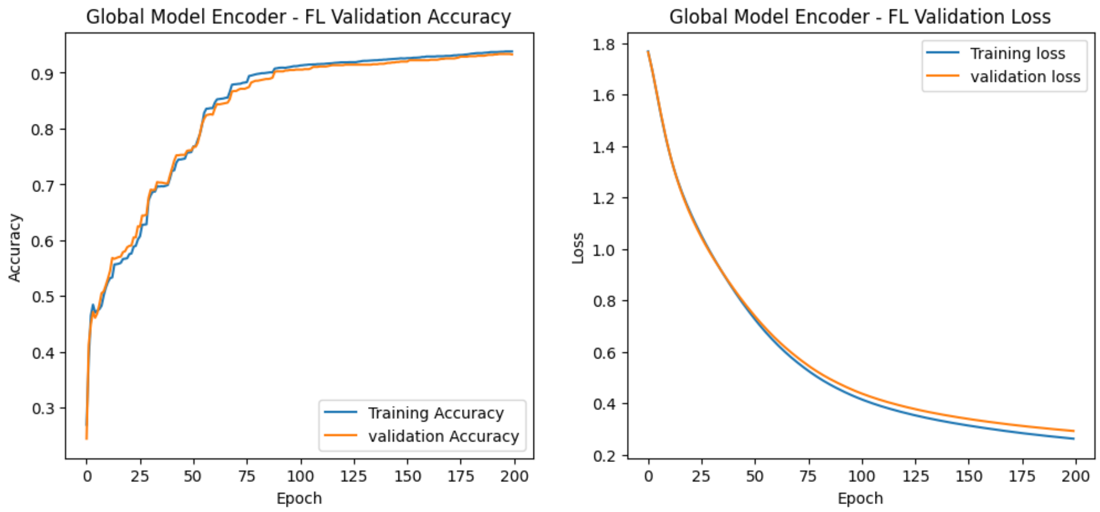


Figure 2.

The execution strategy of the ML group includes this indirect method. We may gain a better understanding of the illustration approach's accuracy and the types of faults it generates by computing the chaotic grid. It is used to evaluate how accurate the depiction is, just like the arrangement of true and prescient markings. They provide a clear explanation of the classifier's representation. Figure 3 shows SPDZ Homomorphic Encryption utilizing Federated Learning. This graphic shows the metric of our model. The total number of real and forecast components for a given technique is displayed in the confusion matrix. The disordered dot matrix accounts for both the total number of marks and the names that will be used for arranging.

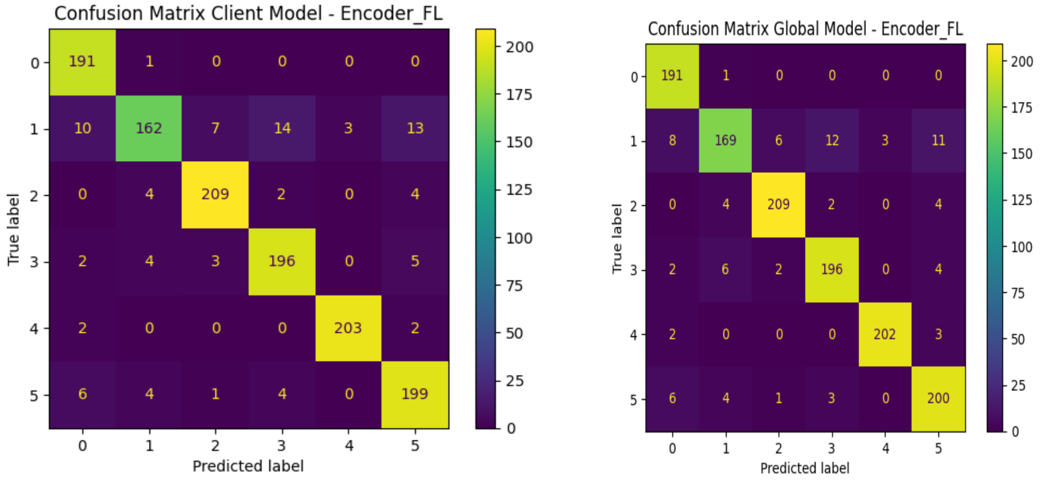


Figure 3. SPDZ Homomorphic Encryption utilizing Federated Learning.

Computational time on Client model and global model

Figure 5 presents the results, which indicate that our proposed FL models are computationally more efficient than local and global models. Our models require significantly less time to train on average, indicating a faster convergence rate and less demand on our computational resources. Modern techniques include resource allocation that has been enhanced, adaptive learning algorithms, and parallel computing procedures make this productivity gain conceivable. Furthermore, the proposed FL models that we have developed leverage efficient communication protocols, which decrease data transfer overhead and delay. This leads to improved system performance and real-time response capabilities, which are essential in circumstances requiring quick decisions in the healthcare sector.

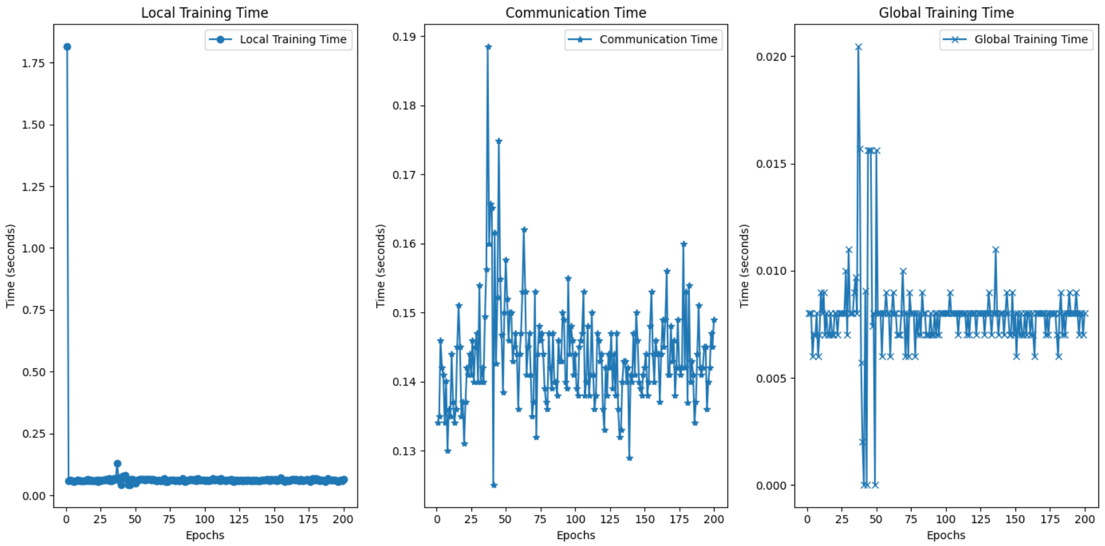


Figure 4. Computational time on Client model and global model

Performance Comparison:

Model 1 - Dimensionality reduction using Auto encoder with Logistic regression

Logistic regression is one of the most often used classification methods in machine learning. The logistic regression model explains relationships between continuous, binary, and categorical factors. Binary is one kind of dependent variable. Based on a few variables, we predict whether or not something will happen. We compute the probability of belonging to each category for a given set of predictors.

Classification reports display several metrics, such as F1 score, precision, and recall, for each class in the classification problem. The ratio of actual positive results to all projected positive results can be used to determine accuracy. It evaluates how effectively the model forecasts the advantageous results. The percentage of true positives to all actual positives is known as the recall. It evaluates the model's capacity to identify positive samples. The harmonic mean of precision and recall is used to get the F1 score, which provides a fair evaluation of the model's performance. The true labels of the test data and the predicted labels generated by the model are the two arguments that can be used by the function to build the classification report. The categorization report can be a useful tool for identifying possible areas of weakness in your model and putting modifications in place to improve accuracy. By using the report's data to enhance the model, one can increase the model's precision and efficacy in categorizing new samples.

Table 2. Classification report LR

	Precision	Recall	F1_score	Support
0	0.61	0.59	0.60	192
1	0.68	0.70	0.69	209
2	0.71	0.61	0.66	219
3	0.75	0.79	0.77	210
4	0.86	0.93	0.90	207
5	0.66	0.69	0.67	214
Accuracy			0.72	1251
Macro avg	0.71	0.72	0.71	1251
Weighted avg	0.72	0.72	0.72	1251

The framework for ML group execution provides support for this system. We may have a better understanding of the average illustration's correctness and the types of obligations it creates by computing the chaotic grid. The representation's accuracy is evaluated in a way that is comparable to the way true and prophetic markers are arranged. They represent the classifier and its representation graphically. In the LR's confusion matrix, Figure 5 . The graphic that is attached displays the measure for our model. The confusion matrix shows the number of projected and distinct brands for a given procedure. The disorderly dot matrix addresses the total number of real marks as well as the names meant for organization. A variety of false positives, true negatives, false negatives, and expected names are among these realistic and anticipated names.

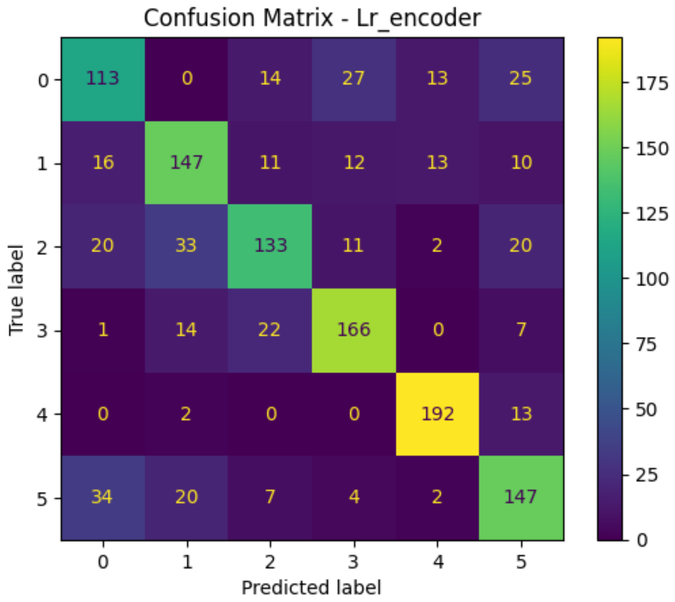


Figure 5. LR's confusion matrix

Model 2 - Dimensionality reduction using auto encoder with K-nearest neighbor

Even if the outcomes are not perfect, it is evident by looking at the collected data that accuracy is extremely high. Although 92% accuracy is ideal, it should be interpreted in light of other factors. The results show that a simple K nearest neighbor can yield results that are similar to those of a more conventional approach like KNN. We plot the differences in measures, including accuracy and loss, between training and validation in this section.

Table 3 Classification report KNN

	Precision	**Recall**	**F1_score**	**Support**
0	0.92	1.00	0.96	192
1	0.94	0.70	0.80	209
2	0.96	0.95	0.96	219
3	0.95	0.91	0.93	210
4	0.97	0.94	0.95	207
5	0.80	1.00	0.89	214
Accuracy			0.92	1251
Macro avg	0.92	0.92	0.91	1251
Weighted avg	0.92	0.92	0.91	1251

This approach is employed in the ML group implementation plan. By computing the chaotic grid, we can have a deeper understanding of the illustration approaches accuracy and the kinds of flaws it generates. It is used to assess how accurate the depiction is, much like true and prophetic markers are set up. They use images to depict the classifier and its illustration graphically. KNN confusion matrix in Figure 6.

The measure in our model is displayed in the provided figure. The confusion matrix for a given algorithm displays the total number of actual and anticipated labels. False positives, genuine positives, false negatives, and false positives come in various varieties.

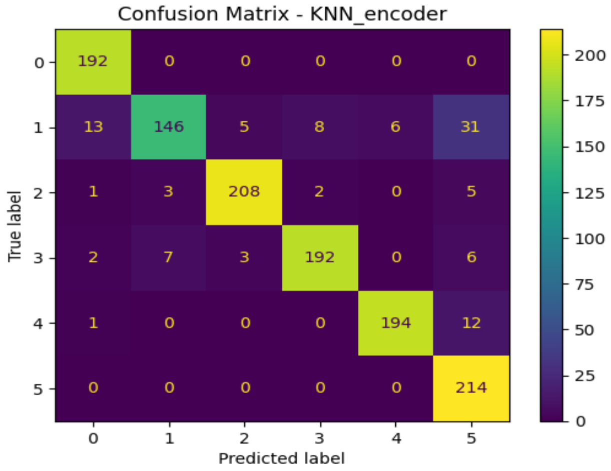


Figure 6. KNN confusion matrix

Model 3 - Dimensionality reduction using auto encoder with SVM

Examining the collected data makes it evident that accuracy is extremely high even though the findings are not perfect. While 84% accuracy is a desired goal, it should be interpreted in light of additional factors. The results show that even a simple SVM may yield results that are on par with those of more conventional methods like SVM. This section presents a chart that illustrates how measures like accuracy and loss change between the two processes.

Table 4. Classification report SVM

	Precision	**Recall**	**F1_score**	**Support**
0	0.83	0.85	0.84	192
1	0.72	0.72	0.72	209
2	0.87	0.77	0.81	219
3	0.88	0.93	0.90	210
4	0.99	0.94	0.97	207
5	0.78	0.85	0.81	214
Accuracy			0.84	1251
Macro avg	0.84	0.84	0.84	1251
Weighted avg	0.84	0.84	0.84	1251

This secondary strategy is part of the ML group's implementation plan. By computing the chaotic grid, we can gain a deeper insight of the illustration approach accuracy and the kinds of faults it generates. It is employed, like the placement of true and prescient markers, to assess how accurately the picture is represented. They give a direct description of the classifier and its representation. The diagram that follows displays our model's metric. The confusion matrix shows how many real and forecast components there are in a certain approach. The names that will be utilized for arrangement and the overall amount of marks are taken into account by the disordered dot matrix. False positives, false negatives, real positives, and false negatives come in different varieties.

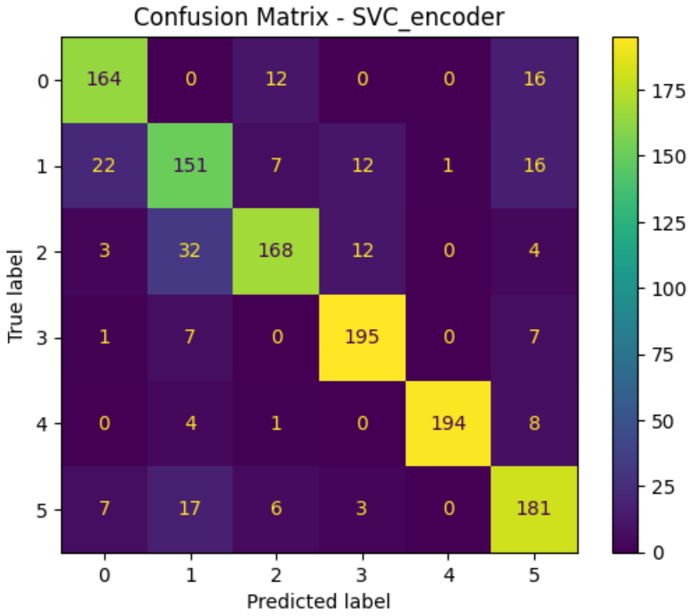


Figure .8. SVM confusion matrix

Model 4 - SPDZ Homomorphic Encryption using Federated Learning

The way distributed machine learning relies on a central hub assigning tasks to external parties, data privacy cannot be adequately safeguarded because the data are visible to the system. In general, multi-party computing which frequently assigns the difficult or unfamiliar computing activity to a third party is involved in distributed learning.

We examine the connection between the quantity of MPC servers and the time spent on multiplications within the SPDZ architecture. The first author's Python crypto package, python is used to test the effectiveness of four parts that make up the architecture data splitting, multiplication, and the link between the number of cryptosystem-based multi-party computations is used to develop the Leave multiple power source, MPC servers, and time charges on multiplications.

Table 5. Classification report SPDZ Homomorphic Encryption using Federated Learning

	Precision	**Recall**	**F1_score**	**Support**
0	0.93	1.00	0.96	192
1	0.90	0.79	0.84	209
2	0.94	0.95	0.94	219
3	0.94	0.92	0.93	210
4	0.97	0.94	0.95	207
5	0.87	0.94	0.90	214
Accuracy			0.92	1251
Macro avg	0.96	0.92	0.92	1251
Weighted avg	0.96	0.92	0.92	1251

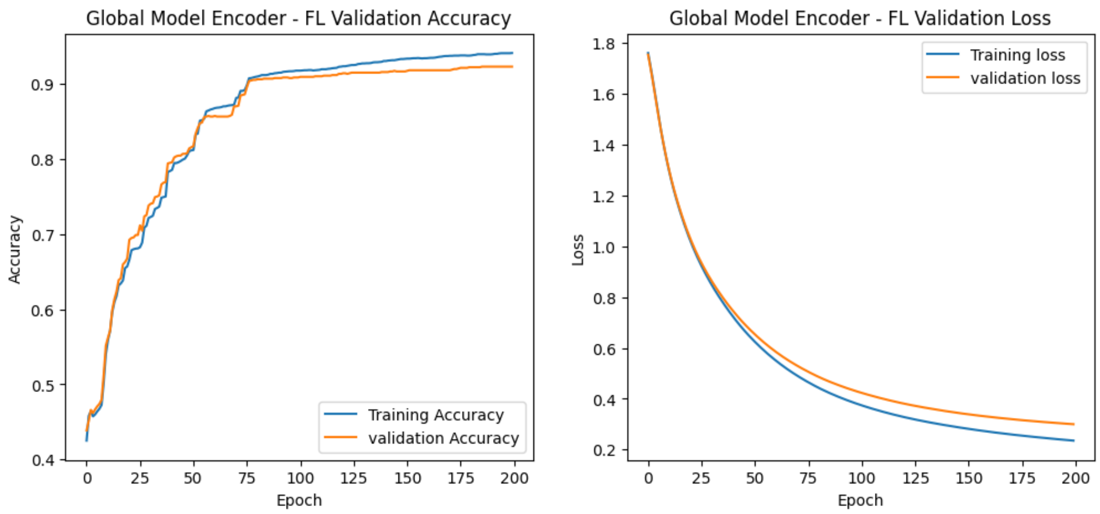


Figure 9. Global encoder validation accuracy and loss

This indirect approach is part of the ML group's execution plan. Computing the chaotic grid allows us to have a better idea of the accuracy of the illustration approach and the kinds of errors it produces. Like the arrangement of true and prescient marks, it is used to assess the depiction's accuracy. They give a direct description of the representation of the classifier. SPDZ Homomorphic Encryption using Federated Learning are displayed in Figure 6. The following diagram displays our model's metric. The confusion matrix shows the total number of real and forecast components for a certain approach. Both the overall number of marks and the names that will be utilized for arrangement are taken into account by the disordered dot matrix.

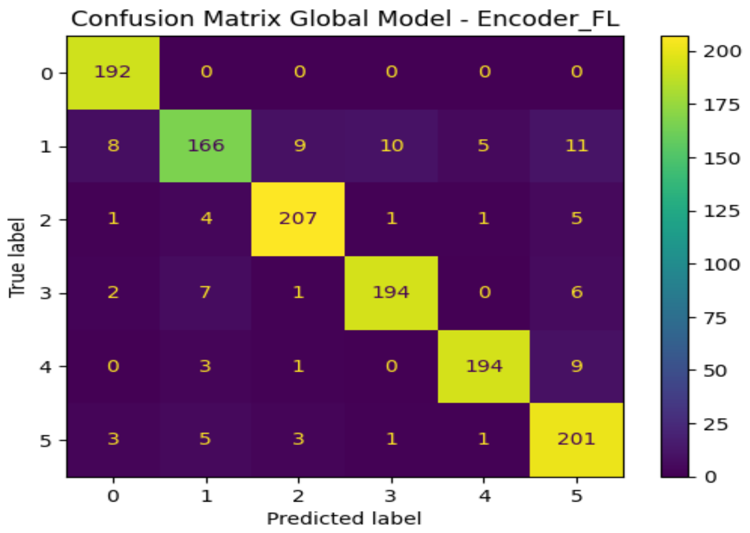
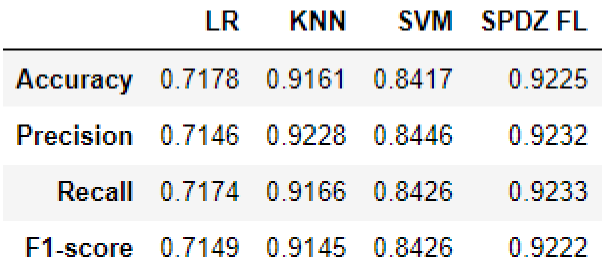


Figure 10. global model encoder FL

Comparison and Evaluation:

The section comparing the current and indicated models indicates that the accuracy increase rate of the proposed framework is approximately 8% higher than that of the current model. This was discovered in all four algorithms: SPDZ Homomorphic Encryption via Federated Learning, KNN, Logistic Regression, and SVM. Subsequent investigation revealed that, among the three algorithms in the proposed model, DT had the highest enhanced accuracy rate, approximately 92%. The analysis of the trade-off between privacy and utility offers a numerical evaluation of the privacy preservation capabilities and performance of the proposed FL models. We tested the recommended framework on an alternative dataset to make sure it was reliable. The data we found supported our assessment that the DT model's implementation algorithm was clear and produced an accurate outcome; table 5 presents the comparison study.



	LR	KNN	SVM	SPDZ FL
Accuracy	0.7178	0.9161	0.8417	0.9225
Precision	0.7146	0.9228	0.8446	0.9232
Recall	0.7174	0.9166	0.8426	0.9233
F1-score	0.7149	0.9145	0.8426	0.9222

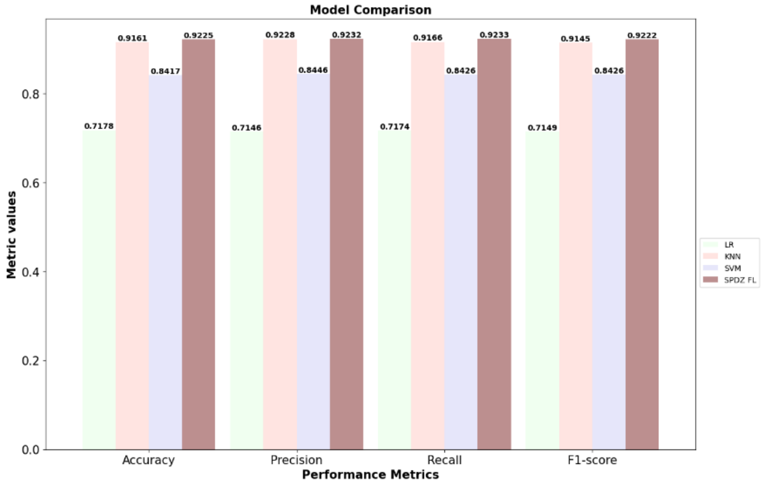
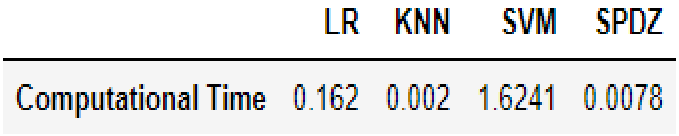


Figure 11. model comparison

Performance evaluation on Communication time

Additionally, efficient communication protocols are used in the FL models we have developed, which lowers latency and data transfer overhead. As a result, the system performs better and can react more quickly two essential qualities in the healthcare industry where swift decision-making is required. When compared to various other models, the numerical analysis demonstrates that our proposed FL models increase computing efficiency. These findings highlight the applicability and relevance of our approach in practical healthcare applications, which are among the key fields in which computing efficiency has a vital function. Our proposed FL models outperform SPDZ Homomorphic Encryption via Federated Learning, KNN, Logistic Regression, and SVM in terms of computing efficiency, according to the findings of the comparison study.



	LR	KNN	SVM	SPDZ
Computational Time	0.162	0.002	1.6241	0.0078

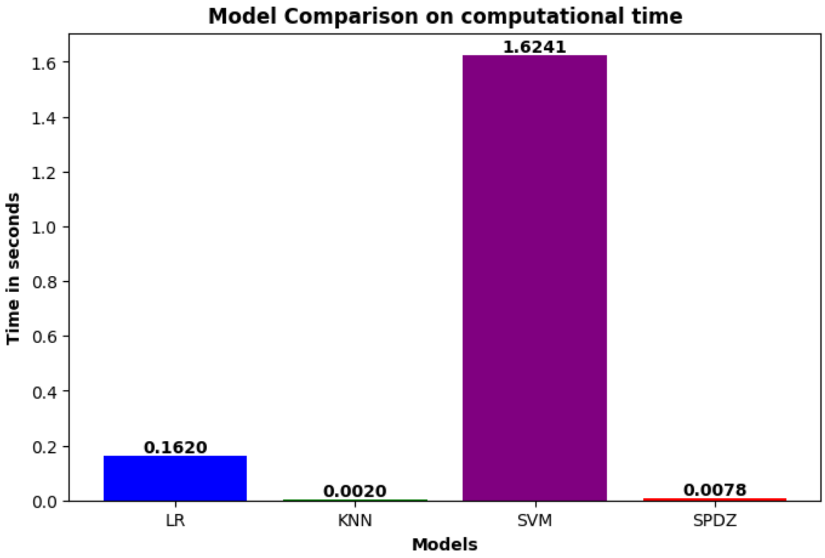


Figure 12. Model comparison on computational time

DISCUSSION

The research included in this study emphasizes how federated learning has the potential to revolutionize the healthcare industry. Our proposed methodology integrates cutting-edge technologies with creative thinking to create a model that protects patient privacy and maximizes the benefits of collaborative learning. A few areas require more research: vertical FL, privacy-preserving FL, and decentralized topology in FL. In this work, we present a unique method for privacy-preserving Federated Learning (FL) models that are intended for use in healthcare settings. Comprehensive analysis and accurate numerical calculation yielded tangible evidence of the efficiency and superiority of the models we offered over existing methods. This effectively safeguarded confidential health information during the federated learning process. Additionally, our models effectively achieved a reasonable trade-off between privacy and utility, safeguarding users' privacy without compromising their usefulness in healthcare applications. When statistically assessing this balance, consideration was given to the models' accuracy and level of privacy protection. Although our research shows a potential direction for privacy-preserving federated learning in the medical field.

CONCLUSION

In the decades to come, federated learning in the healthcare industry will increase significantly. Further research is needed in a few areas, including privacy-preserving FL, decentralized topology in FL, and vertical FL. In the current study, we describe a novel approach to privacy-preserving Federated Learning (FL) models designed with healthcare applications in mind. A thorough assessment and precise numerical computation provided concrete proof of the effectiveness and superiority of the models we provided in comparison to current approaches**.**

This successfully protected private medical information throughout the federated learning procedure. Furthermore, our models successfully struck a respectable utility-privacy balance, tactfully protecting privacy without sacrificing usefulness in healthcare applications. The degree of privacy preservation and the accuracy attained by the models were taken into account when statistically evaluating this balance. Our models showed a strong utility-privacy balance that ensured high accuracy and successfully protected privacy. Future research and development could focus on improving privacy preservation mechanisms through the investigation of cutting-edge methods like homomorphic encryption and secure enclaves. analyzing the federated learning trade-offs between stability, privacy, and usefulness. This may include investigating how different privacy strategies affect the accuracy and wide application of federated models in addition to testing how susceptible they are to corrupt attacks.

References:

1. Thummisetti, B. S. P., & Atluri, H. (2024). Advancing Healthcare Informatics for Empowering Privacy and Security through Federated Learning Paradigms. International Journal of Sustainable Development in Computing Science, 6(1), 1-16.
2. Myrzashova, R., Alsamhi, S. H., Hawbani, A., Curry, E., Guizani, M., & Wei, X. (2024). Safeguarding Patient Data-Sharing: Blockchain-Enabled Federated Learning in Medical Diagnostics. IEEE Transactions on Sustainable Computing, Early Access, 1-15.
3. Soltan, A. A. S., Thakur, A., Yang, J., Chauhan, A., D'Cruz, L. G., & Dickson, P. (2024). A scalable federated learning solution for secondary care using low-cost microcomputing: privacy-preserving development and evaluation of a COVID-19 screening test in UK hospitals, 6, (2), 93-104.
4. Truhn, D., Tayebi Arasteh, S., Lester Saldanha, O., Müller-Franzes, G., Khader, F., Quirke, P., West, N. P., Gray, R., Hutchins, G. G. A., James, J. A., Loughrey, M. B., Salto-Tellez, M., Brenner, H., Brobeil, A., Yuan, T., Chang-Claude, J., Hoffmeister, M., Foersch, S., Han, T., Keil, S., & Kather, J. N. (2024). Encrypted federated learning for secure decentralized collaboration in cancer image analysis. Medical Image Analysis, 92, 103059.
5. Sinaci, A. A., Gencturk, M., Alvarez-Romero, C., Laleci Erturkmen, G. B., Martinez-Garcia, A., Escalona-Cuaresma, M. J., & Parra-Calderon, C. L. (2024). Privacy-preserving federated machine learning on FAIR health data: A real-world application. Computational and Structural Biotechnology Journal, 24, 136-145.
6. Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine, 158, 106848.
7. Hiwale, M., Walambe, R., Potdar, V., & Kotecha, K. (2023). A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. Healthcare Analytics, 3, 100192.

8. Abaoud, M., Almuqrin, M. A., & Khan, M. F. (2023). Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications. IEEE Access, 11, 83562-83579.
9. Butt, M., Tariq, N., Ashraf, M., Alsagri, H. S., Moqurrab, S. A., Alhakbani, H. A. A., & Alduraywish, Y. A. (2023). A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications. Electronics, 12(19), 4074.
10. Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. Knowledge-Based Systems, 274, 110658.
11. Andriole, K. P. (2014). Security of electronic medical information and patient privacy: what you need to know. *Journal of the American College of Radiology*, *11*(12), 1212-1216.
12. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity*, *4*(1), tyy001.
13. Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2018). Health insurance portability and accountability act.
14. Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*, *21*, 106.
15. Elish, M. C., & Boyd, D. (2018). Situating methods in the magic of Big Data and AI. *Communication monographs*, *85*(1), 57-80.
16. Shabunina, E., & Pasi, G. (2018). A graph-based approach to ememes identification and tracking in social media streams. *Knowledge-Based Systems*, *139*, 108-118.
17. Zeng, J., Yu, H., & Kjellberg, F. (2018). Transcriptome analysis of genes involved in the response of a pollinator fig wasp to volatile organic compounds from its host figs. *Acta Oecologica*, *90*, 91-98.
18. Christodoulou, E., Ma, J., Collins, G. S., Steyerberg, E. W., Verbakel, J. Y., & Van Calster, B. (2019). A systematic review shows no performance benefit of machine learning over logistic regression for clinical prediction models. *Journal of clinical epidemiology*, *110*, 12-22.
19. Maxeiner, J. R. (1995). Freedom of information and the EU data protection directive. *Fed. Comm. LJ*, *48*, 93.
20. Bennett, S. M., Ehrenreich-May, J., Litz, B. T., Boisseau, C. L., & Barlow, D. H. (2012). Development and preliminary evaluation of a cognitive-behavioral intervention for perinatal grief. *Cognitive and Behavioral Practice*, *19*(1), 161-173.