**Federated Learning-Based Privacy-Preserving Diabetes Detection with Encrypted Computation**

,, , , ,

1, \* Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudeam-534101, Andhra Pradesh, India.

\*Email: vsnaresh111@gmail.com (Corresponding author)

**ABSTRACT**

The adoption of machine learning in healthcare holds immense potential for improving diagnosis and treatment, but the sensitivity of medical data demands rigorous privacy protections. While Federated Learning (FL) allows collaborative model training without sharing raw data, it still faces challenges in protecting model updates from potential inference attacks. To address this, we propose a robust privacy-preserving FL framework that integrates Homomorphic Encryption (HE). In this design, HE ensures that model updates remain encrypted during training and aggregation, preventing exposure to the central server. This approach guarantees that neither the raw data nor the intermediate updates are accessible to adversaries, offering stronger privacy guarantees. Experimental evaluation on real world medical datasets shows that our system preserves model performance while significantly enhancing data confidentiality, making it well-suited for secure and scalable machine learning in healthcare environments.

Keywords: Diabetes Detection, Federated Learning(FL), Homomorphic Encryption (HE), Logistic Regression, Data Privacy.

**1.INTRODUCTION**

In the healthcare industry, machine learning (ML) has become a game-changing technology that makes it possible for early disease detection, better diagnosis, and tailored treatment recommendations. ML systems are being used more and more to support clinical decision-making and improve patient outcomes as a result of the expanding availability of medical records, diagnostic images, and wearable sensor data. However, one crucial factor—the sensitivity of medical data—restricts the successful application of machine learning in healthcare, despite its potential. Clinical histories, test results, and imaging data are examples of extremely private patient information. Misuse or disclosure of this information can have serious ethical, legal, and security repercussions. Because of these worries, healthcare organizations are hesitant to centralize their data, which limits the potential of conventional machine learning techniques that depend on extensive, aggregated datasets.

Federated Learning (FL), a paradigm that facilitates cooperative model training without direct data sharing, has drawn attention lately as a solution to these issues. Hospitals and clinics are examples of client institutions in Florida that train local models using data that is kept locally. A central server receives only the learned model parameters, which are then combined to create a global model. Although this method greatly lowers privacy risks in comparison to centralized learning, inference attacks can still occur. According to recent research, adversaries may still be able to compromise patient confidentiality by extracting private data from gradients or parameter updates. This restriction emphasizes the necessity of more robust privacy-preserving features in federated learning systems, particularly in crucial fields like medicine.

This study presents a privacy-preserving federated learning framework that incorporates Homomorphic Encryption (HE) to address these vulnerabilities. Computations can be carried out directly on encrypted data using homomorphic encryption, negating the need for decryption. We remove the possibility of parameter leakage to the central server by implementing HE in federated learning, which guarantees that local model updates stay encrypted during training and aggregation. Compared to traditional FL, this design offers stronger privacy guarantees by ensuring that neither the intermediate updates nor the raw medical data are exposed to adversaries.

This work's main contributions are threefold: (i) we present a strong FL framework that has been improved with homomorphic encryption to protect model updates from inference attacks; (ii) we test the framework on actual healthcare datasets to determine how well it preserves model performance while maintaining privacy; and (iii) we show how scalable and useful our method is in healthcare settings where accuracy and security are crucial. Through the integration of federated learning and sophisticated cryptographic techniques, this work seeks to close the gap between patient data confidentiality and data-driven innovation, opening the door for reliable and secure machine learning applications in healthcare.

* 1. Contributions

**2.LITERATURE SURVEY**

The suggested framework combines Homomorphic Encryption (HE) and Federated Learning (FL) to allow for safe, cooperative model training without disclosing private information. Each client in this system uses its own private dataset to train a local Logistic Regression model; raw data is not shared; only the model parameters are. Before being transmitted, these parameters are encrypted using the CKKS scheme to guarantee confidentiality. In order to maintain privacy throughout the process, the central server applies aggregation functions, like averaging, directly to the encrypted model updates without first decrypting them. Clients decrypt the encrypted global model locally and proceed with validation or training after obtaining it. While still utilizing the collaborative potential of distributed learning, this method guarantees that private data is safeguarded at both the data and model update levels.

Examines the application of Federated Learning (FL) to enhance diabetes prediction while protecting patient privacy. It was written by Tariq Sa'ad Jarrar, Dr. Amjad Hudaib, and Dr. Nadim Obeid. According to the size and caliber of each client's local dataset, the authors' weighted FL framework dynamically modifies each client's contribution to the global model. This method successfully tackles issues that are frequently present in medical records, such as data heterogeneity and class imbalance. The framework outperformed conventional centralized and federated approaches using a sizable CDC dataset in a simulated multi-client setting. The study highlights weighted FL's potential as a scalable and privacy-preserving solution for healthcare applications, facilitating safe inter-institution collaboration without leaking private patient information.

FedSHE, a privacy-preserving and effective federated learning framework that incorporates adaptive segmented CKKS homomorphic encryption, is presented by Pan, Chao, He, Jing, Hongjia, and Liming (2024). The intricacy of parameter selection and the encryption length restriction for large models are the two main issues that their work tackles with CKKS in FL. The authors make it possible to handle big neural networks effectively while preserving privacy by examining CKKS security parameters and suggesting a segmented encryption technique. Built on the FedAvg algorithm, FedSHE offers a workable solution that strikes a balance between privacy, utility, and efficiency in federated learning. It outperforms Paillier-based and previous CKKS-based schemes in terms of computational efficiency and communication cost.

In order to reduce the risk of data leakage, Yasmin Makki Mohialden, Nadia Mahmood Hussien, Saba Abdulbaqi Salman, and Mohammad Aljanabi (2023) suggest a safe federated learning framework that makes use of homomorphic encryption. Throughout the training process, their method encrypts local data and model updates. To allow secure aggregation on the server without decryption, a key pair is created. This improves model integrity, data privacy, and regulatory compliance (e.g., GDPR). The framework facilitates safe cooperation between industries, including enterprise systems, healthcare, finance, and the Internet of Things.

The authors Mazin Abed Mohammed, Abdullah Lakhan, Karrar Hameed Abdulkareem, Dilovan Asaad Zebari, Jan Nedoma, Radek Martinek, Seifedine Kadry, and Begonya Garcia-Zapirain present a privacy-preserving detection framework for intelligent transportation systems (ITS) in their paper "Homomorphic Federated Learning Schemes Enabled Pedestrian and Vehicle Detection System." To process encrypted data securely across fog and cloud nodes without disclosing sensitive information, the system, called HMFLS, combines federated learning and homomorphic encryption. It is deployed via an Android-based interface and uses VGG-19 and GANs to extract features from surveillance and vehicle images. The method provides a safe and effective way to detect cars and pedestrians in dispersed environments while also cutting down on processing time and resource leakage.

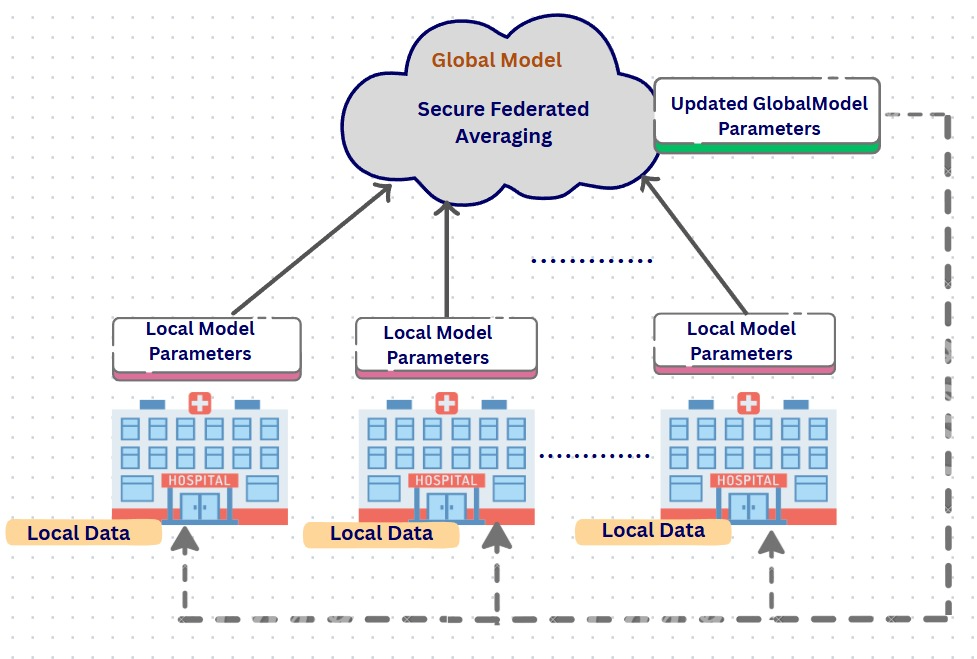
Using federated learning enhanced with homomorphic encryption, Mohandas, Veena, Kirubasri, Thusnavis Bella Mary, and Udayakumar (2024) present a privacy-preserving framework for safe medical data analysis. Without disclosing raw data, the suggested system, called SMHEA (Secured Medical Homomorphic Encryption Algorithm), enables encrypted local model updates to be combined at a central server. The data-quality-aware weighting mechanism is a significant innovation that takes into account the quantity and caliber of local datasets when aggregating models. SMHEA is a good fit for collaborative learning in delicate healthcare settings because it lowers communication overhead and error rates while preserving strong privacy, according to experimental evaluation on the HAM10000 medical image dataset.

**3.BACKGROUND WORK**

**3.1 Federated Learning(FL)**

Federated Learning (FL) is a decentralized machine learning paradigm that allows several clients, including IoT systems, financial institutions, mobile devices, and hospitals, to work together to train a global model without sharing their raw data. Each client trains a local model on its own private dataset independently, sending only the learned parameters or gradients to a central aggregator rather than aggregating sensitive data on a central server. These updates are then combined by the server to enhance the shared global model, which is then sent back to the clients for additional training. In addition to protecting data privacy and lowering the risks connected with centralized data storage, this architecture enables efficient knowledge sharing. FL reduces worries about data breaches, legal compliance, and illegal access by keeping data local.

Additionally, it facilitates collaborative intelligence across heterogeneous and geographically dispersed datasets, enabling organizations to gain from collective knowledge without jeopardizing confidentiality. The method is especially helpful in delicate fields like healthcare and finance, where data privacy is crucial, but high-quality models need large and varied datasets.

Fig.1. FL model overview

**3.2 Logistic Regression**

A popular statistical and machine learning technique for simulating the probability of a binary outcome—where the dependent variable can have one of two possible values, such as 0/1, yes/no, or success/failure—is logistic regression. Using the logistic (sigmoid) function, logistic regression forecasts probabilities that are limited between 0 and 1, in contrast to linear regression, which makes predictions for continuous values:

In this case, denotes a linear combination of input features. A threshold (usually 0.5) is used to categorize the result into one of the two classes, and the sigmoid function's output indicates the likelihood of the positive class.

**3.3 Homomorphic Encryption(HE)**

A cryptographic method called homomorphic encryption (HE) dispenses with the need for decryption by enabling computations to be done directly on encrypted data (ciphertext). This guarantees that private data is kept private even when handled by unreliable individuals. Formally, HE permits operations such that

where ∘ indicates an operation in the plaintext domain (such as addition or multiplication) and ⊕ indicates the corresponding operation in the encrypted domain, provided that E(m) represents the encryption of a message m.Because model parameters or gradients can be encrypted before being sent to a server, HE is frequently used in privacy-preserving machine learning to enable secure aggregation without disclosing raw data.

For calculations involving real (floating-point) numbers, the CKKS scheme is an approximate homomorphic encryption method. CKKS is appropriate for machine learning applications since it allows encrypted arithmetic for real-valued data, in contrast to standard HE, which mainly operates on integers.CKKS encrypts a plaintext vector , as , and operations on ciphertexts roughly correspond to operations on plaintexts:

By encrypting model weights or gradients in federated learning, CKKS allows for secure server aggregation while maintaining the privacy of client data. Because of this, CKKS is perfect for collaborative machine learning that protects privacy in industries like healthcare, finance, and the Internet of Things.

**4.PROPOSED SYSTEM**

The suggested model allows for privacy-preserving collaborative training across numerous clients by combining Homomorphic Encryption (HE) and Federated Learning (FL). Each client trains its private data locally and only contributes encrypted model updates for aggregation, rather than sending sensitive datasets to a centralized server. In distributed environments, this design guarantees both scalability and confidentiality.

Logistic Regression (LR), a popular method for binary classification problems, is used to model the learning task at the client side. The probability of a positive result is calculated as follows, given an input feature vector :

where w and b are the model parameters. Reducing the binary cross-entropy loss over client k's local dataset is how training is accomplished

where is the ground truth label, is the predicted probability, and is the size of the dataset . Stochastic gradient descent (SGD) is used for local optimization, producing updated model parameters for every client.

The CKKS homomorphic encryption scheme is used to encrypt the model parameters following local training. The server can securely aggregate ciphertexts directly thanks to CKKS's support for approximate arithmetic over encrypted vectors. The following homomorphic properties apply to two plaintexts, a and b, and their encrypted versions, ,

The server can aggregate encrypted model weights thanks to this feature without ever decrypting them. In particular, the server calculates the encrypted global model as follows if represents the encrypted parameters from client :

where t is the federated communication round and K is the total number of clients. The confidentiality of both model updates and underlying data is guaranteed because aggregation is carried out fully within the encrypted domain, preventing the server from ever accessing the plaintext weights. The clients are then given a new copy of the encrypted global model. Using its private key, each client decrypts the combined parameters and modifies its local model appropriately. Up until convergence, this iterative cycle of local training → encryption → secure aggregation → decryption is repeated, creating a reliable and broadly applicable global model.The suggested system strikes a balance between accuracy, efficiency, and privacy by integrating logistic regression with federated learning and homomorphic encryption. Decentralized knowledge sharing is made possible by federated learning, interpretable classification is ensured by logistic regression, and sensitive data is protected during the training process by CKKS-based encryption.

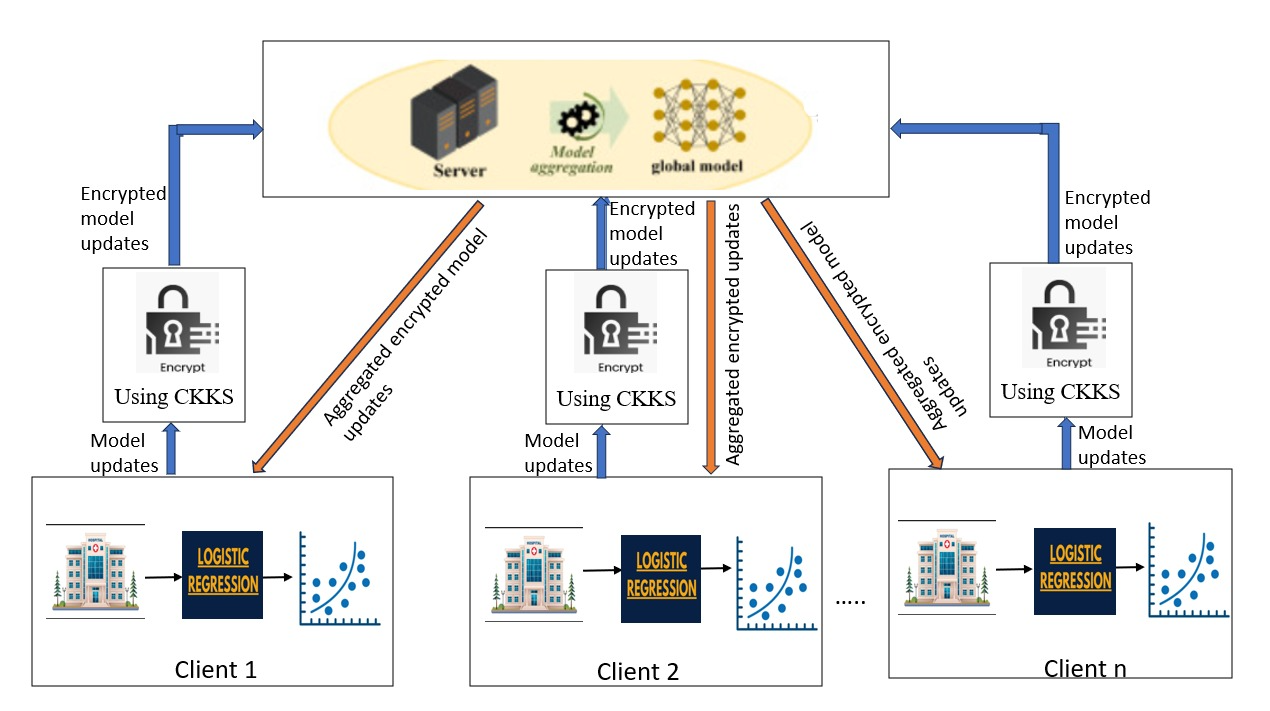


Fig.2.System Architecture of proposed model with FL and HE

**WorkFlow for Proposed Model**  
The following steps describe the workflow of the suggested federated learning framework with homomorphic encryption:   
**Step i: Training Local Models at Clients**

Due to privacy and regulatory restrictions, sensitive diabetes datasets held by each participating client (such as a hospital or medical facility) cannot be shared. Each client uses its own diabetes dataset to train a local Logistic Regression model rather than sending raw data. In order to capture the information gleaned from its local data, the client calculates model updates during training, such as weight parameters or gradients. This guarantees that private patient data stays within the client's immediate surroundings.

**Step ii: Model Update Encryption**

Each client uses CKKS homomorphic encryption prior to sending the local updates to the server. Arithmetic operations (addition, multiplication) can be carried out directly on encrypted values thanks to the CKKS scheme. This ensures that sensitive information cannot be deduced from the updates by the server or any other third party, protecting data confidentiality even in the event that communication channels are compromised.

**Step iii: Sending the Server Encrypted Updates**

The model updates are safely sent to the central server after being encrypted. Sensitive information about the local diabetes datasets cannot be reconstructed because the updates are encrypted. Each client simply sends ciphertext representations of the model parameters to the server.

**Step iv: Server-side secure aggregation**

The server carries out secure aggregation after receiving encrypted updates from several clients. The server can average or sum the encrypted parameters without decrypting them by utilizing the features of CKKS encryption. This guarantees the privacy of the entire aggregation process by preventing the server from accessing any individual client's update in plaintext.

**Step v: Update the Global Model**

The combined knowledge of all participating clients is represented by the aggregated encrypted result. The server then uses this combined data to update the global Logistic Regression model. The model update is protected during the entire process because the aggregation is done on ciphertexts.   
  
**Step vi: Delivering the Global Model to Customers**

After that, the participating clients receive a redistribution of the encrypted global model. Clients can use the received global model for local inference on diabetes prediction tasks or for additional training by decrypting it with their private decryption keys. This guarantees that each client gains from the cooperative training procedure while protecting its confidential information.

**Step vii: The Iterative Method**

Throughout several federated learning rounds, the aforementioned procedures are repeated. Clients continue training on their local diabetes data in each round, sending updates to the server encrypted. These updates are combined by the server, which then re-distributes the enhanced global model. Until the global model converges and reaches acceptable performance metrics, this iterative process keeps going.

**5.EXPERIMENTAION AND RESULTS**

The Pima Indians Diabetes Dataset is a widely used benchmark in medical research and machine learning applications for predicting the onset of diabetes. Originally collected by the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) and made publicly available through the UCI Machine Learning Repository, the dataset was introduced by Smith et al. (1988). It consists of 768 records, each representing a female patient of Pima Indian heritage aged 21 years or older. The dataset includes eight numerical features: number of pregnancies, plasma glucose concentration, diastolic blood pressure, triceps skin fold thickness, 2-hour serum insulin, body mass index (BMI), diabetes pedigree function (reflecting genetic predisposition), and age. The binary target variable, labeled as ‘Outcome’, indicates whether the patient was diagnosed with diabetes (1) or not (0). Among the 768 individuals, 268 were diagnosed with diabetes (Outcome = 1), while 500 were not (Outcome = 0), highlighting a class imbalance that must be considered during model training and evaluation. Additionally, several features contain biologically implausible zero values—such as in glucose, BMI, and blood pressure—which are typically treated as missing data and handled through imputation techniques. This dataset serves as a foundational resource for developing and evaluating classification algorithms such as logistic regression, decision trees, support vector machines, and neural networks in the healthcare domain.

The implemented framework shows how to use homomorphic encryption (HE) and logistic regression to predict diabetes in a federated learning environment while maintaining privacy. Four different clients independently train local models using their respective diabetes datasets in the system's simulation of a multi-client architecture. Every dataset goes through a standard preprocessing pipeline that consists of a stratified split into training and validation subsets, z-score normalization, and feature-label separation. Using stochastic gradient descent over several epochs, a logistic regression model is locally trained at the client level. Each client uses the TenSEAL library's implementation of the CKKS homomorphic encryption scheme to encrypt its learned model parameters in order to maintain data confidentiality during model aggregation.Without requiring decryption at all, the central server then computes an element-wise average of the encrypted model weights to carry out secure aggregation. This guarantees that the global model is created in a way that respects privacy and complies with secure federated learning guidelines.

In a Federated Learning setup with four clients, the Fig.3 depicts the loss progression over 20 communication rounds. It displays both the average loss for all clients as well as the unique loss trends for each client. Clients 1 and 2 show moderate variability during training, with loss values of approximately 0.4896 and 0.4833, respectively. While Client 4 exhibits the most stable performance with a consistent loss of roughly 0.4340, Client 3 maintains a comparatively low loss of roughly 0.4336 with only slight fluctuations. The fifth subplot illustrates the aggregated results, which show the average loss stabilizing at 0.4602 with minor oscillations to reflect the variety of client behaviours. The overall stability of the training process is emphasized in this visualization, which also shows how client-specific traits affect global model convergence.

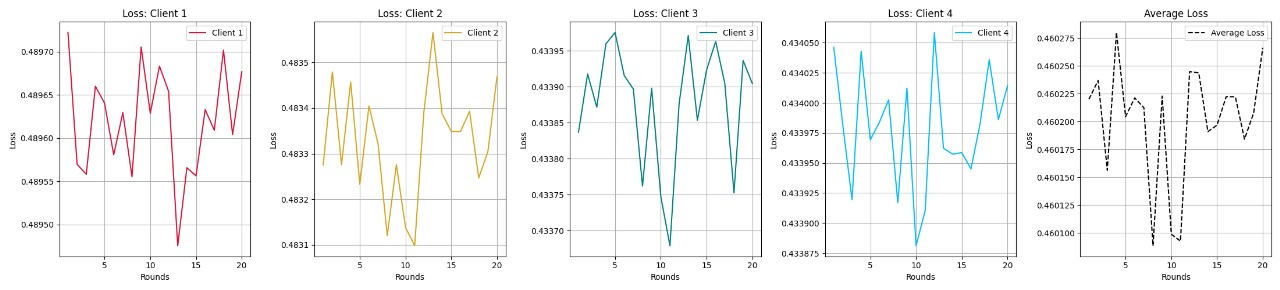


Fig.3.Loss graphs for each client along with average

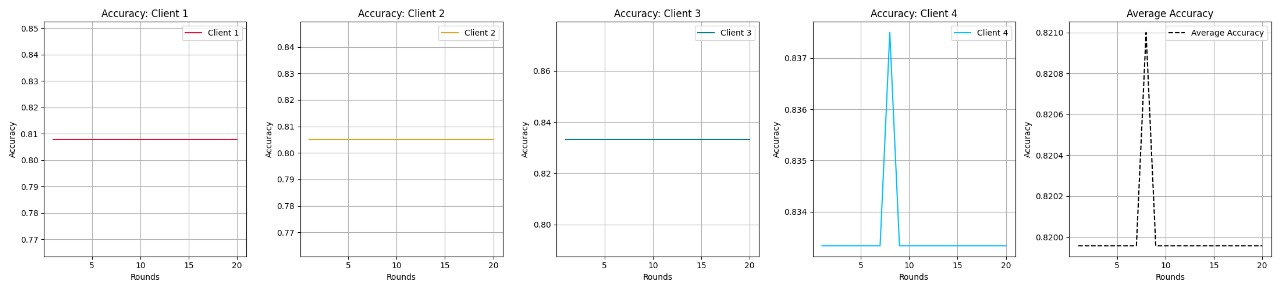
The Fig.4 demonstrate that there is very little variation in the accuracy of all four clients over the course of the 20 training rounds. Client 2 maintains the lowest accuracy of all the clients at about 0.805, while Client 1 maintains an accuracy of roughly 0.81. With a consistent accuracy of about 0.833, Client 3 is the best performer. Client 4's accuracy stays around 0.834, with the exception of a brief spike at round 8, when it reaches about 0.839 before falling back to the baseline. The average accuracy for all clients is roughly 0.82, with a slight peak around round 8 but otherwise staying steady. This suggests that either the model converged quickly or that additional performance gains were limited by factors like data distribution or model complexity. It also shows that the training process did not significantly improve accuracy over rounds.

Fig.4.Accuracy graphs for each client along with average

A federated learning model's performance stability over 20 training rounds across four clients is depicted by the precision plots as shown in Fig.5. The precision curves for clients 1, 2, and 3 are entirely flat, suggesting that their precision scores did not change during the training phase. Notably, Clients 1 and 2 maintained a marginally lower score of roughly 0.756, while Client 3 achieved the highest and most consistent precision at roughly 0.781. Around Round 8, Client 4's precision briefly increased to about 0.776 before falling back to its baseline of 0.766. The average precision curve, which was otherwise stable at about 0.7645, also slightly increased as a result of this fluctuation. All things considered, the model performs consistently and dependably for all clients, with little fluctuation over time. indicating steady precision throughout training and early convergence.

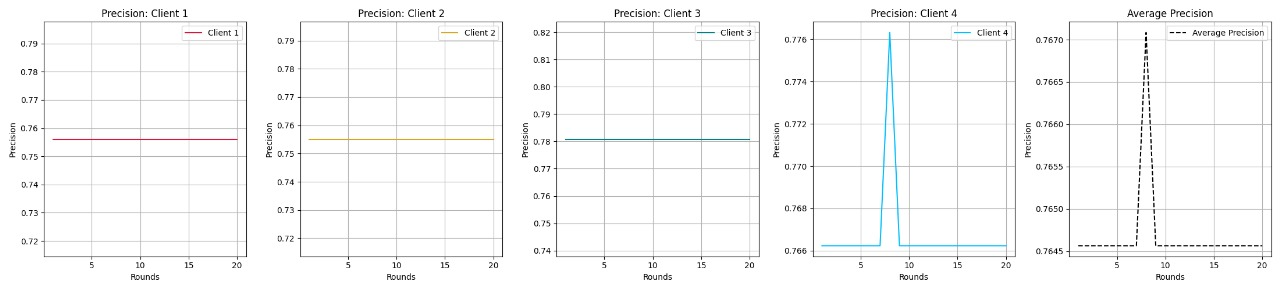


Fig.5.Precision graphs for each client along with average

The Fig.6 depicts the recall performance over 20 training rounds in a Federated Learning scenario with four clients, taking into account both the average recall for all clients and the recall for each individual client. Recall metrics for Clients 1 through 4 are displayed in the first four subplots, and the average recall for all clients is summarized in the fifth subplot. Throughout the training rounds, the recall values stay constant, indicating reliable performance throughout the federation. Client 1 consistently maintains a recall of roughly 0.65, Client 2 stays steady at roughly 0.67, Client 3 stays at roughly 0.70, and Client 4 consistently reaches the highest recall of roughly 0.73. The final subplot shows the average recall, which stays fixed at roughly 0.69.This consistent behaviour indicates that clients contribute fairly, guaranteeing consistent model performance and highlighting the stability of the federated training process.

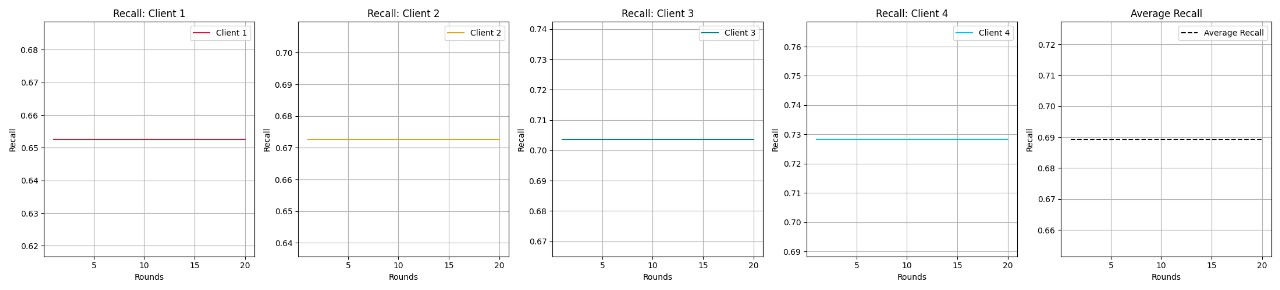


Fig.6.Recall graphs for each client along with average

Four clients F1-scores and their average F1-score over 20 training rounds are shown in the Fig.7. The outcomes are fairly consistent, exhibiting little variation over time. While Client 2 remains stable at 0.71 , Client 1 maintains an F1-score of roughly 0.70. Client 4 performs similarly at 0.747, with the exception of a brief spike around round 8, when its score slightly exceeds 0.752 before falling back to baseline. Client 3 consistently achieves a higher F1-score of around 0.74. The average F1-score for all clients is roughly 0.725, with a slight increase at round 8 but no other changes. The model either rapidly stabilized or had little room for improvement because of things like data distribution or convergence, as indicated by the flat trend across rounds, which generally shows that training had no discernible effect on F1-scores.

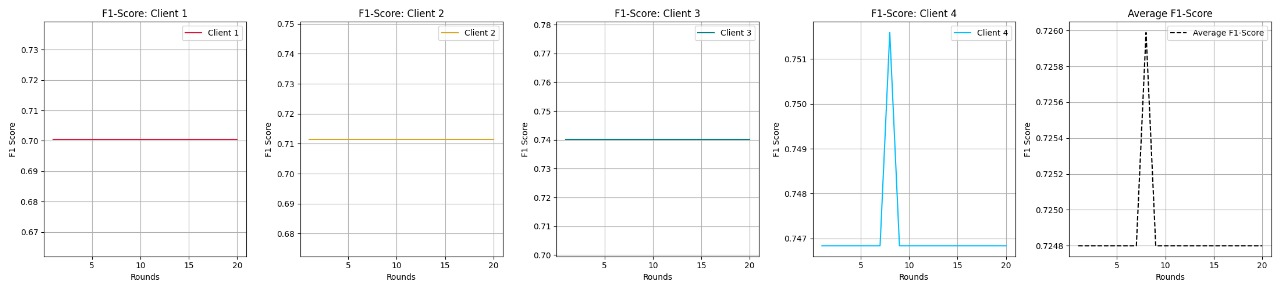


Fig.7.F1-score graphs for each client along with average

The performance of a federated learning model assessed across four clients is depicted in Fig.8. The model's ability to differentiate between classes on each client's local dataset is shown by the ROC curve. An Area Under the Curve (AUC) score of 0.86 was attained by all four clients, indicating a consistently high level of performance across the distributed nodes. The model's ability to produce accurate predictions is confirmed by the fact that all of the ROC curves are significantly above the diagonal reference line, which stands for random guessing. This consistency in AUC values indicates that a well-generalized model that functions similarly across various data distributions has been produced by the federated training process.

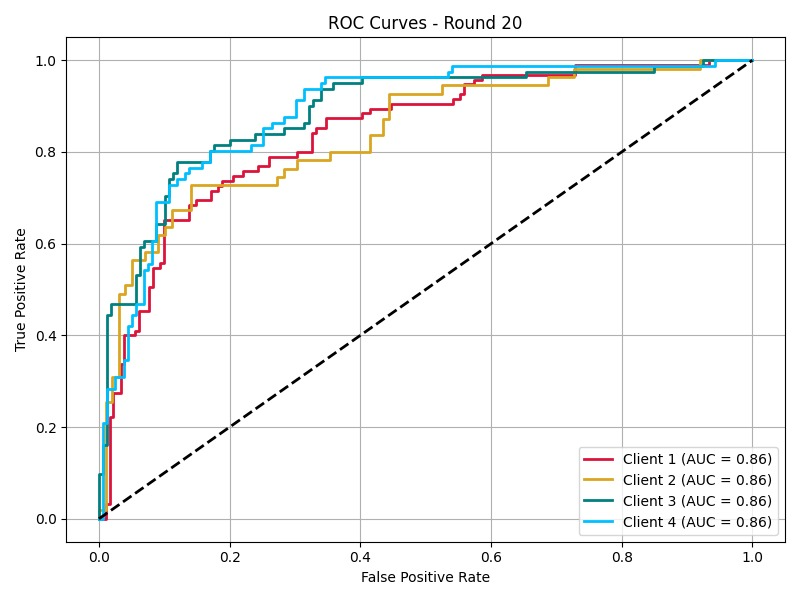


Fig.8.ROC curve graph for all clients

**6.Discussion on Results:**

The proposed privacy-preserving federated learning framework successfully demonstrated consistent and dependable performance for diabetes prediction while closely protecting patient data. Using a federated configuration with four scattered clients, the model consistently produced accurate predictions across all nodes. By the final communication rounds, the framework had stabilized at an average validation accuracy of roughly 82%, with individual client accuracies ranging from 80.5% to 83.4%. The average recall was 69%, with precision staying steady at roughly 76.45% and recall values ranging from 65% to 73%. Furthermore, a balanced ability to reduce false positives and false negatives is indicated by the model's average F1-score of 72.5%.

The framework's ability to successfully differentiate between diabetic and non-diabetic cases across a variety of datasets was further confirmed by the ROC curve analysis, which showed strong discriminative power with all clients reaching an AUC score of 86% by round 20. The stability of these results over 20 federated training rounds highlights the system's resilience, as client-specific variations had minimal impact on the global model's convergence.

**7.Conclusion:**

Homomorphic encryption and federated learning together create a safe and efficient framework for diabetes prediction in dispersed healthcare settings. The framework guarantees robust privacy preservation while maintaining high predictive performance by permitting collaborative model training without disclosing private patient data. Utilizing HE, especially schemes like CKKS, helps ensure compliance with data protection laws and further protects intermediate computations during aggregation. The significant advantages in terms of privacy and trust outweigh the small approximation error and computational overhead that encryption brings. The combination of FL and HE is a viable and scalable approach to creating precise, privacy-preserving models, as this study shows, opening the door for a wider use of secure AI in healthcare.

**References:**

1. Zhu, B., & Niu, L. “A privacy-preserving federated learning scheme with homomorphic encryption and edge computing.” Alexandria Engineering Journal, 2025.
2. X. Wu, F. Huang, Z. Hu, and H. Huang, “Faster Adaptive Federated Learning,” Proceedings of the AAAI Conference on Artificial Intelligence, vol. 37, no. 9, pp. 10379–10387, Jun. 2023, doi: 10.1609/aaai.v37i9.26235.
3. T. Deng, H. Hamdan, R. Yaakob, and K. A. Kasmiran, “Personalized Federated Learning for In-Hospital Mortality Prediction of Multi-Center ICU,” IEEE Access, vol. 11, pp. 11652–11663, 2023, doi: 10.1109/ACCESS.2023.3241488.
4. A. Senapati, H. K. Tripathy, V. Sharma, and A. H. Gandomi, “Artificial intelligence for diabetic retinopathy detection: A systematic review,” Inform Med Unlocked, vol. 45, p. 101445, 2024, doi: 10.1016/j.imu.2024.101445.
5. V. R. S. Sushma, K. Nikhil, K. A. Reddy, and L. Sunitha, “Diagnosis of Cardiovascular Disease using Deep Learning,” Int J Res Appl Sci Eng Technol, vol. 11, no. 4, pp. 371–378, Apr. 2023, doi: 10.22214/ijraset.2023.49209.
6. M. M. Yaqoob, M. Nazir, M. A. Khan, S. Qureshi, and A. Al Rasheed, “Hybrid Classifier-Based Federated Learning in Health Service Providers for Cardiovascular Disease Prediction,” Applied Sciences, vol. 13, no. 3, p. 1911, Feb. 2023, doi: 10.3390/app13031911.
7. M. Babar, B. Qureshi, and A. Koubaa, “Investigating the impact of data heterogeneity on the performance of federated learning algorithm using medical imaging,” PLoS One, vol. 19, no. 5, p. e0302539, May 2024, doi: 10.1371/journal.pone.0302539.
8. K. Cheng et al., “SecureBoost: A Lossless Federated Learning Framework,” IEEE Intell Syst, vol. 36, no. 6, pp. 87–98, Nov. 2021, doi: 10.1109/MIS.2021.3082561.
9. Lin, J.C.W.; Srivastava, G.; Zhang, Y.; Djenouri, Y.; Aloqaily, M. Privacy-preserving multiobjective sanitization model in 6G IoT environments. IEEE Internet Things J. 2020, 8, 5340–5349.
10. Li, T.; Hu, S.; Beirami, A.; Smith, V. Ditto: Fair and robust federated learning through personalization. In Proceedings of the International Conference on Machine Learning, Virtual, 18–24 July 2021; pp. 6357–6368.
11. Ou,W.;Zeng, J.; Guo, Z.; Yan, W.; Liu, D.; Fuentes, S. A homomorphic-encryption-based vertical federated learning scheme for rick management. Comput. Sci. Inf. Syst. 2020, 17, 819–834.
12. M. H. Qasem, A. Hudaib, and N. Obeid, “Multiagent System for Mutual Collaboration Classification for Cancer Detection,” Math Probl Eng, vol. 2019, pp. 1–17, Dec. 2019, doi: 10.1155/2019/2127316.
13. Xu,G.; Li, H.; Liu, S.; Yang, K.; Lin, X. Verifynet: Secure and verifiable federated learning. IEEE Trans. Inf. Forensics Secur. 2019, 15, 911–926.
14. Liu, X.; Deng, R.H.; Choo, K.K.R.; Weng, J. An efficient privacy-preserving outsourced calculation toolkit with multiple keys. IEEE Trans. Inf. Forensics Secur. 2016, 11, 2401–2414.
15. Zahrani, and A. Al-Khasawneh, “Multi-Agent System Combined With Distributed Data Mining for Mutual Collaboration Classification,” IEEE Access, vol. 9, pp. 70531–70547, 2021, doi: 10.1109/ACCESS.2021.3074125.
16. Acar A, Aksu H, Uluagac AS, Conti M (2018) A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (Csur) 51(4):1–35
17. Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, Patel S, Ramage D, Segal A, Seth K (2017) Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of the 2017 ACM SIGSAC confer ence on computer and communications security, pp 1175–1191
18. Aono Y, Hayashi T, Wang L, Moriai S et al (2017) Privacy-preserving deep learn ing via additively homomorphic encryption. IEEE Trans Inf Forensics Secur 13(5):1333–1345
19. Albrecht M, Chase M, Chen H, Ding J, Goldwasser S, Gorbunov S, Halevi S, Hoff stein J, Laine K, Lauter K et al (2021) Homomorphic encryption standard. Protect Privacy Through Homomorphic Encrypt. 31–62
20. D. Dave, K. Vyas, J. K. Jayagopal, A. Garcia, M. Erraguntla, and M. Lawley, “FedGlu: A personalized federated learning-based glucose forecasting algorithm for improved performance in glycemic excursion regions,” arXiv preprint arXiv:2408.13926, 2024.
21. NVIDIA Technical Blog. (2022, September 2). Federated Learning with Homomorphic Encryption.NVIDIA Technical Blog.https://developer.nvidia.com/blog/federatedlearning-with-homomorphic-encryption/.
22. Yackel, R. (2021, July 6). What Is Homomorphic Encryption, and Why Isn't It Mainstream?Keyfactor.<https://www.keyfactor.com/blog/what-is-homomorphic-encryption/>.
23. Wibawa, F., Catak, F. O., Sarp, S., Kuzlu, M., & Cali, U. (2022). Homomorphic Encryption and Federated Learning-based Privacy-Preserving CNN Training: COVID-19 Detection Use-Case. ArXiv. /abs/2204.07752.
24. Park, J., & Lim, H. (2022, January 12). Privacy-Preserving Federated Learning Using Homomorphic Encryption. Applied Sciences. <https://doi.org/10.3390/app12020734>.
25. I. Jannoud, M. Z. Masoud, Y. Jaradat, A. Manaserah, and D. Zaidan, “A Multi-Layered Hybrid Machine Learning Algorithm (MLHA) for Type II Diabetes Classification,” Procedia Comput Sci, vol. 237, pp. 445–452, 2024, doi: 10.1016/j.procs.2024.05.126.