STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

A Privacy-Preserving Federated Learning Framework with Fully Homomorphic Encryption for Reproductive Health Analytics

Abass Hassan[1], Sheikh Umar Mushtaq[2], Hussein Edrees[3], Amier Alquatesh[3*]

[1] *Computer Science and Engineering, Lovely Professional University, Jalandhar, 144411, India*
[2] *School of Computer Application, Lovely Professional University, Jalandhar, 144411, India*
[3] *Deanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia*

ARTICLE INFO

Article History

Received: 02-02-2026
Revised: 03-06-2026
Accepted: 20-06-2026
Published: 28-06-2026

Vol.2026, No.2

DOI:

***Corresponding author.**
Email:
aalqatish@kfu.edu.sa

Orcid: 0000-0002-3350-4446

ABSTRACT

With the increasing use of cloud analytics technology, machine learning is now being used to help with fertility tracking and predict risks of pregnancy. However, reproductive health data is considered highly sensitive data, and with traditional analytics training, data must be sent to an external server, which is raising giant red flags regarding data privacy and security. This paper will address these issues by proposing a privacy-preserving analytics platform for fertility and pregnancy data by combining Federated Learning (FL) with Fully Homomorphic Encryption (FHE) technology. FL will be utilized so that multiple hospitals can collaborate and come up with a shared model for pregnancy risks. However, with FL, inference leaks occur when data is sent to the server, which compromises sensitive data. To address inference leaks, we will be using the Cheon-Kim-Kim-Song (CKKS) method to encrypt data before it is sent to the server, which will then be aggregated with other data without any sensitive reproductive health data being compromised or exposed during training. We will be using TenSEAL and Scikit-learn to implement our proposed framework and will be testing it with the Maternal Health Risk Dataset. Our results will show that our proposed FL+FHE model is able to achieve reliable prediction accuracy with reasonable encryption overhead.

Keywords: Reproductive; Homomorphic Encryption; Maternal; Federated Learning and Cloud.

How to cite the article

1. Introduction

The rapid development of digital healthcare systems has made it possible for hospitals and medical institutions to store and process a huge amount of patient data for intelligent decision-making. In this context, reproductive healthcare data such as fertility reports, hormonal content, pregnancy risk factors, and maternal healthcare-related information are highly sensitive in nature [1]. This type of data requires the utmost level of confidentiality, as any violation of this could lead to severe ethical, social, and legal issues. With the increasing popularity of cloud-based medical analytics, the issue of preserving data privacy has become a pressing concern in current healthcare research [2].

Typically, conventional machine learning approaches rely on a centralized approach for data collection, wherein data related to patients in various hospitals is stored in a centralized server for training and prediction purposes [3]. Although this approach helps to improve the accuracy of predictions, it also leads to a high degree of privacy risks, including data leakage, insider attacks, and privacy violation. A novel approach called Federated Learning (FL) has been proposed to overcome the above issues, wherein multiple healthcare providers can come together to jointly train a global model without having to share patient data. In FL, a model is trained individually in each medical institution, and the model parameters are communicated to a centralized server for aggregation purposes. However, FL alone is not enough to solve the problem of privacy violation, as the model parameters can still be subject to inference attacks, which would cause data leakage [4]. To solve this problem, a novel approach called Fully Homomorphic Encryption is proposed to perform computations on data in an encrypted form. In this context, CKKS is a scheme that allows for secure arithmetic operations to be carried out on real-valued data, which is suitable for medical analytics purposes [5]. we propose a novel framework based on Federated Learning and Fully Homomorphic Encryption for privacy preservation of fertility and pregnancy risk prediction. Our framework provides end-to-end privacy preservation, ensuring that the cloud server is not aware of any sensitive information, as the model updates are encrypted during the process of transmission and aggregation.

1.1 Federated Learning in Healthcare Analytics

Federated Learning (FL) is a new technique for training machine learning models that does not require the partners to share the original data. In the traditional centralized learning technique, the data is gathered from multiple sources and stored in a single server for training the models. This is not an appropriate technique in the healthcare domain because the privacy of the patients and the regulations related to the use of the data is an important concern in the healthcare industry [6]. FL is an effective technique to solve the above-mentioned problem because it allows multiple clients, such as hospitals, to train the models individually with the help of their individual data. The clients share the updates of the models, such as the gradients or the weights, with the server, and the server combines the updates to form the global model, generally by using the Federated Averaging Algorithm (FedAvg) technique. FL is not completely secure because the updates of the models can reveal the sensitive information by launching attacks such as gradient leakage and model inversion attacks [7].

1.2 Fully Homomorphic Encryption for Secure Computation

Fully Homomorphic Encryption (FHE) is a powerful technique that it allows you to carry out mathematical operations directly over the encrypted data without the need to decrypt it first. This means that, unlike the traditional technique, FHE does not just provide security to the data, while it is at rest or in transit but also while it is being processed. Once the encrypted data is decrypted by the authorized person, the same results can be obtained as if the actual data had been used for the calculation process [8]. More recent FHE-based data encryption algorithms, such as CKKS (Cheon-Kim-Kim-Song), also support the calculation of appro$_x$imate math for real numbers, making it more useful for the privacy preservation of machine learning models. FHE can be used to provide an excellent privacy-preserving solution for healthcare analytics, such as for calculating fertility and pregnancy risk, where data privacy is of utmost importance [9].

1.3 Privacy Challenges in Reproductive Healthcare Data

Data like fertility tests, pregnancy risk symptoms, hormone reports, mother's health, etc., are considered to be the most private health information. It contains very personal details about pregnancy problems, infertility treatments, IVF, pregnancy care, etc. Reproductive health data, if used without permission, may cause ethical, social, legal, and other issues. With the increase in the usage of online services by more healthcare services, reproductive health data is being stored remotely. This makes the health data more prone to cybercrime [10]. Furthermore, the strict health regulations and privacy policies do not allow hospitals to upload raw health data to third-party servers or share it with other hospitals. This is an issue for developing machine learning models, as they require large amounts of data [11].

1.4 Threat Models and Security Risks in Federated Learning

Even though federated learning solves the problem of direct data sharing, it cannot be considered a solution for addressing the problem of privacy. In federated learning systems, the hospitals participate in the process by providing updates in the model in the form of gradients or weights. These updates can be a potential source of leakage of sensitive information through various adversarial attacks [12]. One of the attacks in federated learning systems occurs in the honest-but-curious server model. In this model, the server behaves in a way that conforms to the protocol and tries to obtain sensitive information from the updates received. In addition, gradient leakage and model inversion attacks allow the reconstruction of the original training data from the model parameters. Insider attacks, malicious clients, and unauthorized access of updates during transmission are other sources of risk in federated learning systems. These risks are more severe in reproductive healthcare because partial leakage of patient information can be dangerous [13]. Hence, federated learning systems need to be combined with other strong cryptographic approaches for end-to-end confidential updates.

1.5 CKKS Encryption Scheme for Encrypted Machine Learning

The CKKS (Cheon-Kim-Kim-Song) is a widely used homomorphic encryption scheme that is specifically designed for approximate homomorphic computations over real numbers. Unlike other homomorphic encryption schemes, the CKKS scheme is capable of performing efficient computations over floating-point numbers, making it an excellent choice for machine learning computations, where the parameters and gradients used in the models can be continuous in nature [14]. The CKKS scheme is capable of directly executing addition and multiplication operations over the ciphertexts, thereby ensuring that the updates to the models remain encrypted during the training process. Microsoft SEAL and TenSEAL are two prominent libraries that support the CKKS homomorphic encryption scheme for the development of privacy-preserving AI models [15]. In the proposed framework, the CKKS homomorphic encryption scheme is used to encrypt the federated updates before they are sent to the cloud, thereby ensuring that the reproductive healthcare information is kept confidential during the process.

2. Literature Review

The importance of privacy-preserving healthcare analytics has been recognized in the context of the increased popularity of cloud-based healthcare platforms and the rising concern of data breaches. Various techniques have been proposed to ensure the privacy of sensitive health information without compromising the efficiency of machine learning-based prediction and decision-making processes. In the context of reproductive health, the privacy aspect is more challenging because of the confidential nature of the information related to fertility and pregnancy. The following section describes the research work related to federate learning in the context of health care and homomorphic encryption-based secure computing.

2.1 Federated Learning in Healthcare Analytics

Federated learning has been widely researched as a distributed learning approach for healthcare analytics in which the direct sharing of data is not permitted. Various studies have been carried out to prove the effectiveness of the federated learning approach in healthcare applications such as disease diagnosis and patient risk assessment systems in which a number of hospitals can come together and train a global model [16]. FedAvg is a widely used aggregation approach in the

federated learning framework. This approach provides a simple and efficient way of aggregating local model updates. In the existing healthcare systems based on federated learning, it is assumed that local model updates can be communicated securely to the server. This assumption is not always true [17]. Recent studies have shown that the gradients and model parameters of the model can reveal sensitive patient information through gradient inversion and membership inference attacks. This indicates that federated learning alone cannot ensure a high level of privacy [18].

2.2 Homomorphic Encryption and Secure Learning Approaches

Homomorphic encryption has been explored for secure computation over encrypted medical data, especially in cloud computing environments [19, 20]. Initially, partially homomorphic encryption was used for secure computation, where only simple computations were supported, but now FHE-based encryption schemes such as BFV and CKKS support more complex computations over the encrypted medical data [21]. CKKS is widely used in privacy-preserving machine learning, where it supports approximate arithmetic operations over real-number features and model parameters. Various studies have been conducted to develop an encrypted inference framework, where the patient inputs remain unknown to the cloud server, and direct prediction is supported over the encrypted medical data [22]. However, the training process is computationally expensive when encrypted training is used. To address the training process, hybrid models that combine federated learning with homomorphic encryption models have been developed, where the model is trained locally in plaintext, and the model updates are encrypted. These models are balanced in terms of accuracy, scalability, and privacy, and they can be used in sensitive medical domains such as fertility and pregnancy risk analysis.

2.3 Hybrid Federated Learning and Fully Homomorphic Encryption Frameworks

Recently, advancements in privacy-preserving ML have motivated a new approach that uses a combination of FL and FHE to overcome the shortcomings of individual approaches when used alone [23]. FL allows hospitals to learn models on their premises without moving patient data, but model updates such as gradients or model weights are communicated over a network, which makes it susceptible to inference attacks. This makes it necessary to provide cryptographic security to such systems, especially in a domain like healthcare [24, 25]. A new approach that uses a combination of FL and FHE has been identified as a promising direction for secure federated learning systems, in which model parameters are encrypted before transmission to the central aggregator. In some of the secure federated learning systems, it has been proposed that clients learn models locally on plaintext data, after which model updates are encrypted using homomorphic encryption. These updates are aggregated on the server without decrypting them, which prevents leakage of intermediate information during the collaborative learning process. This approach greatly enhances the privacy of the system under the honest-but-curious server model [26].

Among the existing fully homomorphic encryption schemes, CKKS is prominent for federated learning as it supports approximate arithmetic for real-valued model parameters, which is typically utilized in deep learning models. Various studies have demonstrated that CKKS-based encryption is effective for secure gradient aggregation and encrypted inference in medical applications, including cancer prediction, image analysis in radiology, and electronic health records classification [27]. Despite the use of the hybrid approach, there exist some issues, including high computational costs, larger cipher texts, and increasing communication costs. Some people have suggested several modifications, including quantization, packing, and efficient key management, to enhance the scalability of the system [28]. In reproductive health, fertility and pregnancy data are highly sensitive. Therefore, a hybrid approach that integrates FL and FHE provides a strong foundation for privacy. This paper extends the concept of the hybrid approach by developing an encrypted federated analytics system that focuses on the prediction of pregnancy risk [29].

2.4 Research Gaps and Motivation

Despite significant research efforts towards developing privacy-preserving healthcare analytics using federated learning and homomorphic encryption-based methods, there are some limitations of these methods identified from the existing

literature. First of all, there are limitations of federated learning-based healthcare systems, where collaborative learning is considered more important than secure updates of the model. Although federated learning avoids sharing gradients and model parameters directly, there is a chance of gradient inversion attacks. Secondly, the current homomorphic encryption-based machine learning systems emphasize the security of the inference process over the security of the collaborative training process. The process of encrypted model training using homomorphic encryption is sometimes computationally costly, especially because the cost of the operation is high and the volume of the cipher texts is large, which limits the scalability of the current homomorphic encryption-based machine learning systems in the real world. Thus, different studies have been conducted to create a hybrid system that incorporates federated learning and homomorphic encryption, but most such machine learning models have only been evaluated using general healthcare datasets, not sensitive reproductive healthcare datasets. Third, there is a lack of research on privacy-preserving analytics for reproductive healthcare domains such as fertility monitoring and pregnancy risk prediction. Reproductive healthcare data typically carries sensitive information regarding reproductive problems, hormones, complications, and maternal history. Because of the strict privacy regulations and ethical concerns, healthcare organizations often face difficulties in sharing reproductive healthcare data with other organizations, which makes it difficult to develop cooperative machine learning models for reproductive healthcare analytics.

To improve the above-mentioned limitations, this paper proposes a privacy-preserving federated learning system for reproductive healthcare analytics with Fully Homomorphic Encryption and the CKKS scheme. The proposed system will enable different healthcare institutions to jointly develop a model for predicting the risk of pregnancy while ensuring the encryption of the model updates during the transmission and aggregation processes. The proposed solution will improve the data privacy aspect with the incorporation of federated learning and the CKKS scheme, while ensuring the prediction performance with reasonable computing costs.

3. Proposed Methodology

The framework proposed in this section combines Federated Learning and Fully Homomorphic Encryption and aims at ensuring the privacy of the reproductive health information when conducting fertility and pregnancy risk prediction. The idea is to enable different healthcare organizations to collaborate and develop a reliable prediction model without revealing their reproductive health information and updates to the prediction model.

3.1. Federated Training with Homomorphic Encryption

Federated learning is used for training. With time, a better global model is achieved through communication. Let's consider w_t to be the model's weights for a particular round t. Clients perform stochastic gradient descent for model updates.

$$w_t^i = w_t - n\nabla L_i(w_t) \quad (1)$$

Here L_i denotes the local loss function, and n is the learning rate. To prevent any leak of information, the clients send the encrypted weights.

$$Enc(w_l^i) = CkkS(w_l^i) \quad (2)$$

The server directly performs the secure aggregation over the encrypted weights:

$$Enc(w_{t+1}) = \Sigma_{i=1}^{N} \frac{n_i}{n} Enc(w_t^i) \quad (3)$$

Here,

Enc(w_l^i) is the Encrypted model update sent by client to the server,

$\Sigma_{i=1}^{N}$ is the sum of all models from all participating clients.

n is the total samples.

N is the total no of participating clients

The encrypted model is sent back, and the reproductive health information is kept secure throughout the process.

(A) Proposed Pseudocode:

Step 1: Initialize global model parameters wi.
Step 2: Distribute the model and CKKS public key to clients.
Step 3: Each client will perform local training on the pregnancy datasets.
Step 4: The local updates will be encrypted by CKKS.
Step 5: The server will aggregate the encrypted updates by FedAvg.
Step 6: Repeat the process for multiple rounds until convergence.
Step 7: The final model will be used for secure pregnancy risk classification.
This method will enable joint fertility and pregnancy analysis without compromising privacy, gradient leakage, and healthcare security standards

The Fig. 1 illustrates the Federated Learning and Fully Homomorphic Encryption enables trust-free collaboration among hospitals for large-scale pregnancy analytics while ensuring patient privacy. This is a crucial step in developing ethical AI systems in maternity care.

(B) Proposed Algorithm:

1. Set W^0 (global parameters)
2. generate $(P_k, S_k) \leftarrow$ KeyGen()
3. for each t=1 to R do
   server pass W^{t-1}, P_k to all
4. for each k=1,2…… K in parallel do
   Receive W^{t-1} (global parameters)
   calculate $Wt = W^{t-1} - n\nabla L(D_k, Wt^{-1})$
   C_k^t = Encrypt $_{CKKS}$ (w_k^t, P_k)
   Send (C_k^t to server)
5. $C^t = 1/k \sum_{k=1}^{k} C_k^t$
6. W^t = Decrypt $_{CKKS}$ (C^t, S_k)
7. $W^* = W^R$ (final model)

3.2. Algorithm: FL + FHE Security Analytics

FL + FHE Secure Pregnancy Analytics is a combination of federated learning and fully homomorphic encryption that is used for privacy-driven analytics of sensitive maternal health data. Each hospital develops its own models of pregnancy risks using its own data, which means that the original data of the patients is kept within the premises of the hospital. The models are then updated and sent to the server for processing without decrypting them. This way, sensitive data is kept away from the server or any other third party. It is an effective way of obtaining reliable predictions regarding pregnancy risks while being compliant with HIPAA and GDPR.

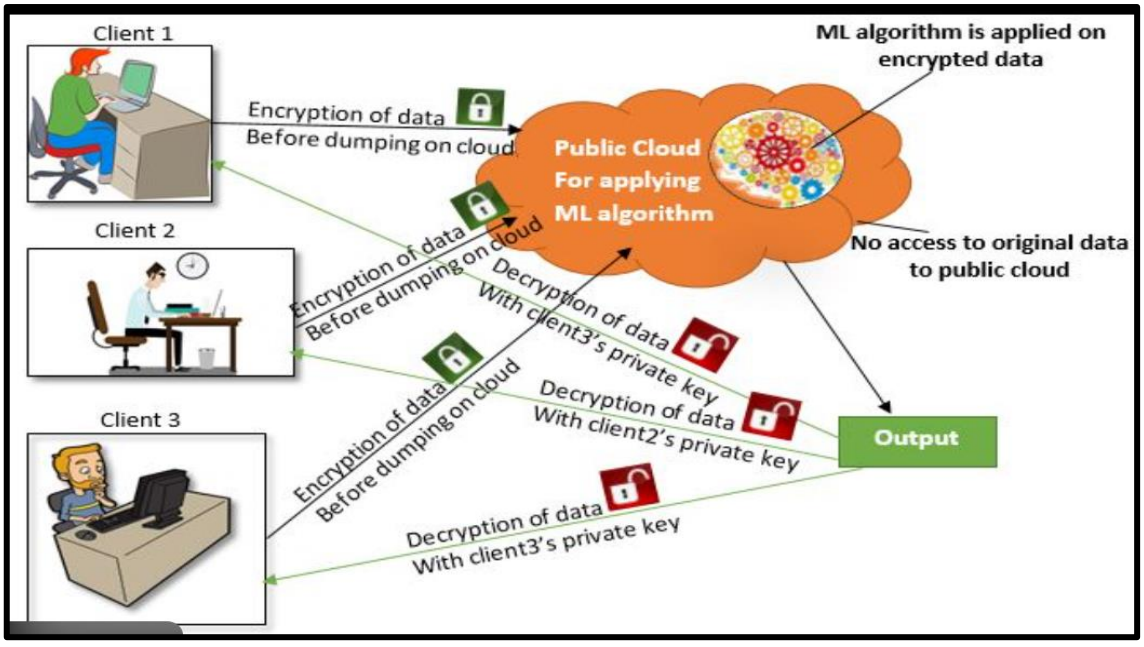


Figure 1. FL + FHE framework for privacy-preserving pregnancy analytics with encrypted model aggregation.

4. Federated Learning Optimization Model

Suppose there are N healthcare entities, which could be hospitals or clinics, and each entity has its own local data set:

$$D_i = \{x_i^i\}_{i=1}^{n_i} \quad (4)$$

In the expression, x_i^i denotes the reproductive health attributes (such as hormonal levels, blood pressure, and fetal measurements), and denotes the respective pregnancy risk label. The goal of federated learning is to improve the global objective function.

$$min\, F(\omega) = \Sigma_i^N \frac{n_i}{n} F_i(\omega) \quad (5)$$

Where n and Σ_i^N is the local loss function for client $F_i(\omega)$

$$F_i(w) = \frac{1}{n_i} \Sigma_{j=1}^{n_i} L(f(\dot{x}_j^i; w), y_j^i \quad (6)$$

Here, w denotes model parameters and L (f ($\dot{x}_j^i; w$) is the prediction loss.

4.1. Local Model Update at Each Client

Throughout each communication cycle t, the server supplies global model weight values (wt) to all clients. Each client performs local training using gradient descent:

$$w_i^{t+1} = \omega^t - n\nabla F_i(\omega^t) \quad (7)$$

Here "n" is learning rate.

$F_i(\omega^t)$Represents the gradient of the local loss

This approach ensures that reproductive data is never shared outside of the institution.

4.2. Local Model Update at Each Client

Once the local updates are received, the aggregation of updates occurs at the central server using the Federated Averaging rule as follows:

$$w^{t+1} = \sum_{i=1}^{N} \frac{\eta_i}{n} w_i^t + 1 \quad (8)$$

To obtain an improved global model at the end of each round. However, sending updates in plain text form could lead to a leak of information, and hence encryption is added.

4.3. Local Model Update at Each Client

To maintain confidentiality, each client will encrypt its local update using the fully homomorphic encryption scheme of CKKS:

$$C_i^{t+1} = EnC(w_i^{t+1}) \quad (9)$$

The server will receive ciphertexts c instead of plaintext weights. As a result of the additive homomorphic property, encrypted aggregation is possible:

$$EnC(w_i^{t+1}) = (x + a)^n = \sum_{i=0}^{n} ni/n \, EnC(w_i^{t+1}) \quad (10)$$

Thus, the server performs secure model averaging without decrypting client updates. Only authorized clients with the secret key can decrypt the final model:

$$W^{t+1} = Dec\big(EnC(W^{t+1})\big) \quad (11)$$

5. Implementation Details

The framework that has been implemented for privacy-preserving fertility and pregnancy analytics, as discussed above, makes use of federated learning mechanisms with full homomorphic library implementations. This ensures that multiple healthcare organizations are able to collaborate with each other and train a model that can predict pregnancy risks without compromising any reproductive information.

5.1. Federated Learning Workflow

Training is done in a federated manner. Each hospital trains the model on their local pregnancy data and then encrypts the updates and sends them to the central server.

Algorithm

- server sends global model w^t to clients
- each client trains locally to get wi^{t+1}
- encrypt the update: ci = Enc(wi^{t+1})
- server aggregates the encrypted updates: Enc(w^{t+1}) = Σ ci/N
- clients decrypt the new global model

Thus, the model will always remain updated for the encrypted data in the process.

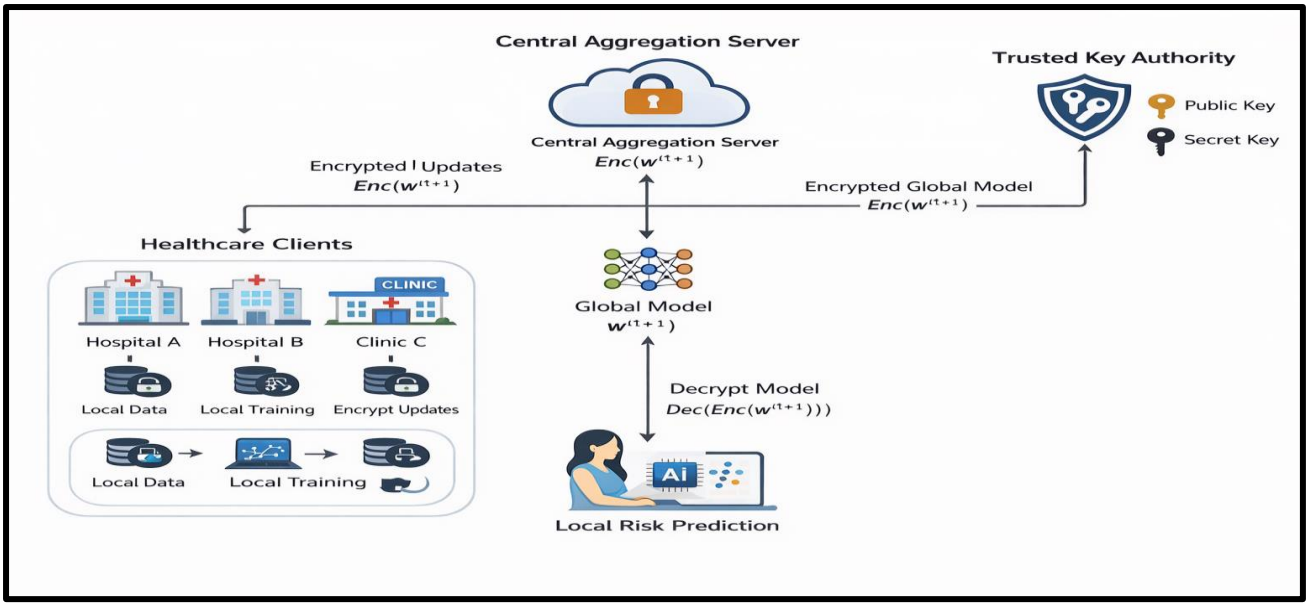


Figure 2. Proposed FL+ FHE architecture for Secure pregnancy analytics

5.2. Confusion Matrix Analysis

The confusion matrix provides a detailed breakdown of classification performance across the three pregnancy risk categories (Low, Medium, and High). It highlights correct predictions along the diagonal and misclassifications in the off-diagonal elements.

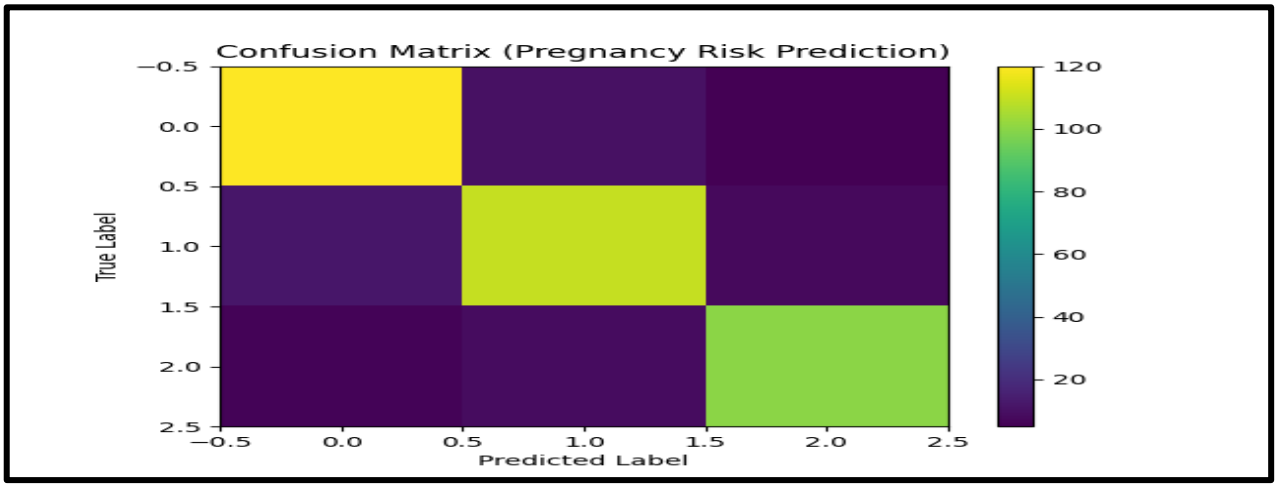


Figure 3. Proposed FL+ FHE architecture for secure pregnancy analytics.

As shown in the above Fig.3, the confusion matrix of the FL+FHE model has most of its accurate classification along the diagonal line, indicating that all three levels of risk have been accurately classified. However, there are some misclassifications between the Medium and High levels of risk, which is normal in any maternal health prediction due to similar symptoms.

6. Experimental Setup

This section describes the experimental conditions, dataset details, evaluation metrics, and the encryption approach used in the experiment to validate the proposed Federated Learning with Fully Homomorphic Encryption framework for the analysis of fertility and pregnancy risks.

6.1. Dataset Description

To validate the proposed approach, experiments are conducted on the Maternal Health Risk Dataset, which is a publicly available dataset used in the field of health care. The dataset provides the required health attributes for pregnancy. The dataset contains the required physiological parameters used in pregnancy and maternal health risks.

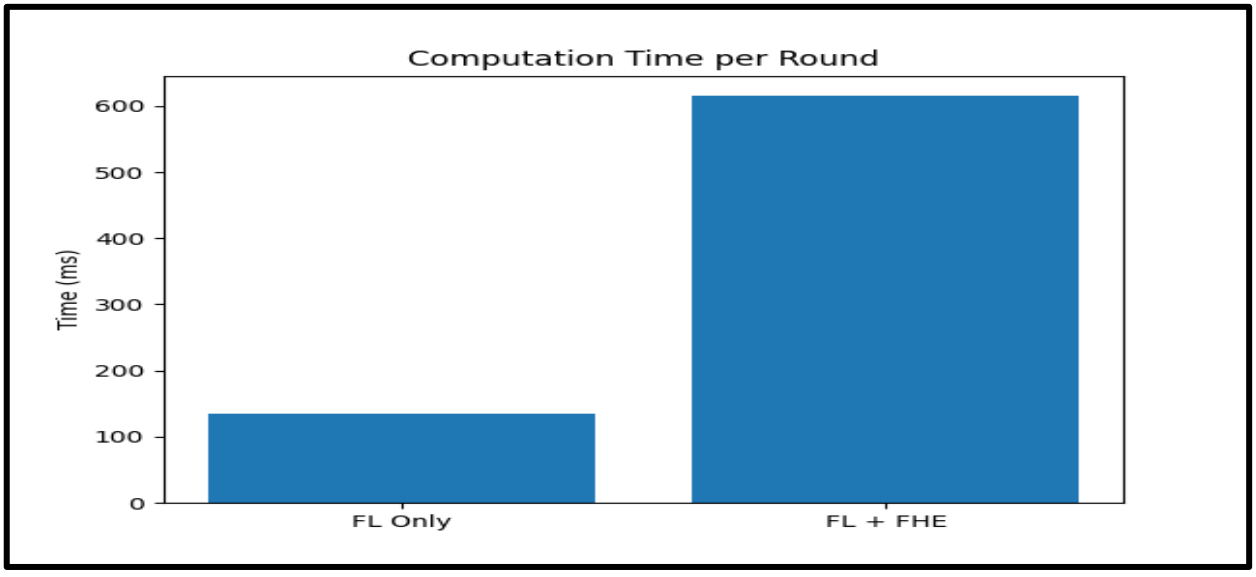


Figure 4. Computation Overhead Graph

It was observed that the proposed FL+FHE approach attained an accuracy of 88.7% on the Maternal Health Risk dataset with guaranteed privacy of client updates using CKKS encryption. Although encryption results in increased computational cost, confidentiality is ensured for reproductive healthcare analytics.

6.2. Homomorphic Encryption Configuration

In order to ensure the privacy of the model update transmission, the CKKS fully homomorphic encryption technique has been used, and the code has been implemented through the TenSEAL library. This is because the CKKS technique allows for approximate arithmetic over real parameters, making it more appropriate for the application in the context of encrypted machine learning models. The parameters for the encryption technique have been chosen to ensure both efficiency and security, thereby providing the required support for the secure encrypted aggregation over multiple rounds of training while ensuring the required level of precision in the ciphertexts.

7. Results

In this section, we evaluate the performance of the proposed federated learning with fully homomorphic encryption (FL+FHE) approach for privacy-preserving fertility and pregnancy risk prediction. Performance evaluation is conducted based on three major criteria: prediction accuracy, encryption overhead, and privacy preservation in maternal healthcare settings.

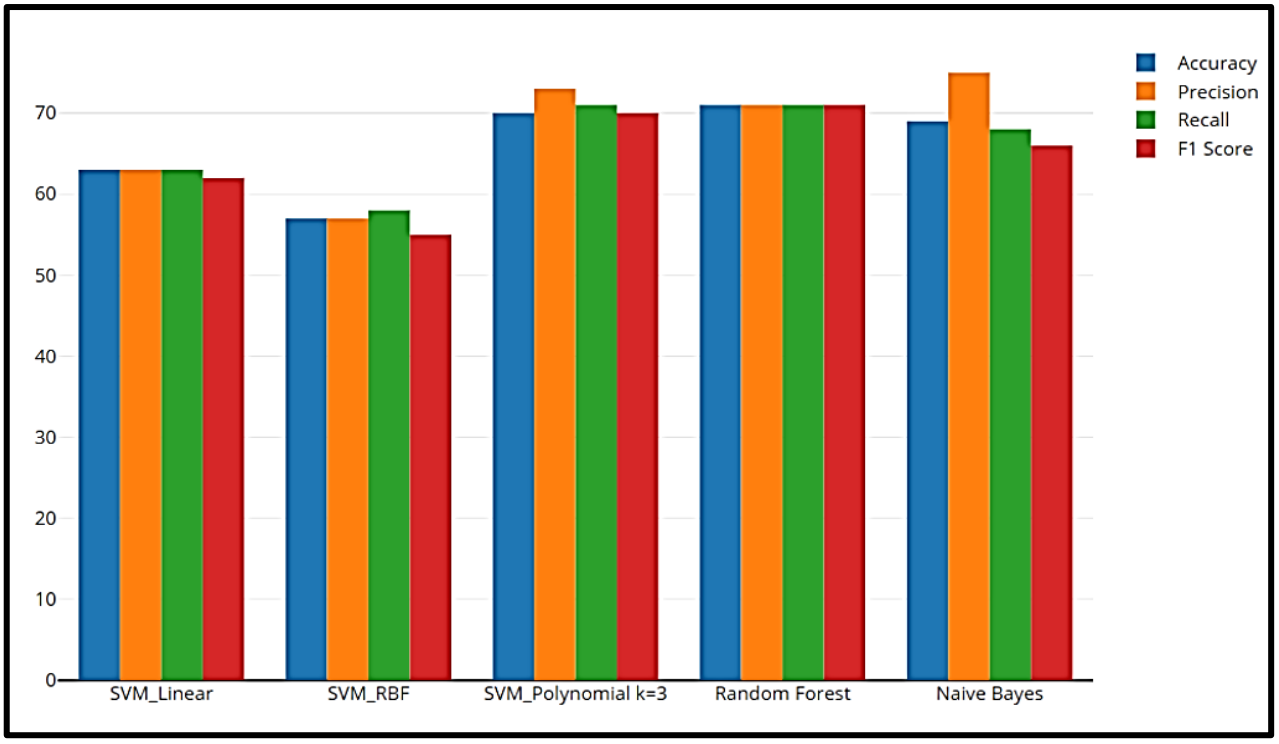


Figure 5. Comparison of Accuracy, Precision, Recall, and F1-Score for Centralized Model, Federated Learning (FL), and Proposed FL + FHE model.

The Figure 5 depicts a comparison between the performances of three models: Centralized Logistic Model, Federated Learning (FL), and FL + Fully Homomorphic Encryption (FHE), using three different evaluation parameters: Accuracy, Precision, Recall, and F1-Score.The graph indicates that the addition of FHE to FL results in a slightly lower performance but a better level of privacy preservation.

Table 1. Performance Comparison Using 80% Training Data

Model	Accuracy	Precision	Recall	F1 Score
KNN	63.42	81.56	79.84	80.69
SVM	82.37	86.92	84.15	85.51
Decision Tree	97.64	98.71	96.89	97.79

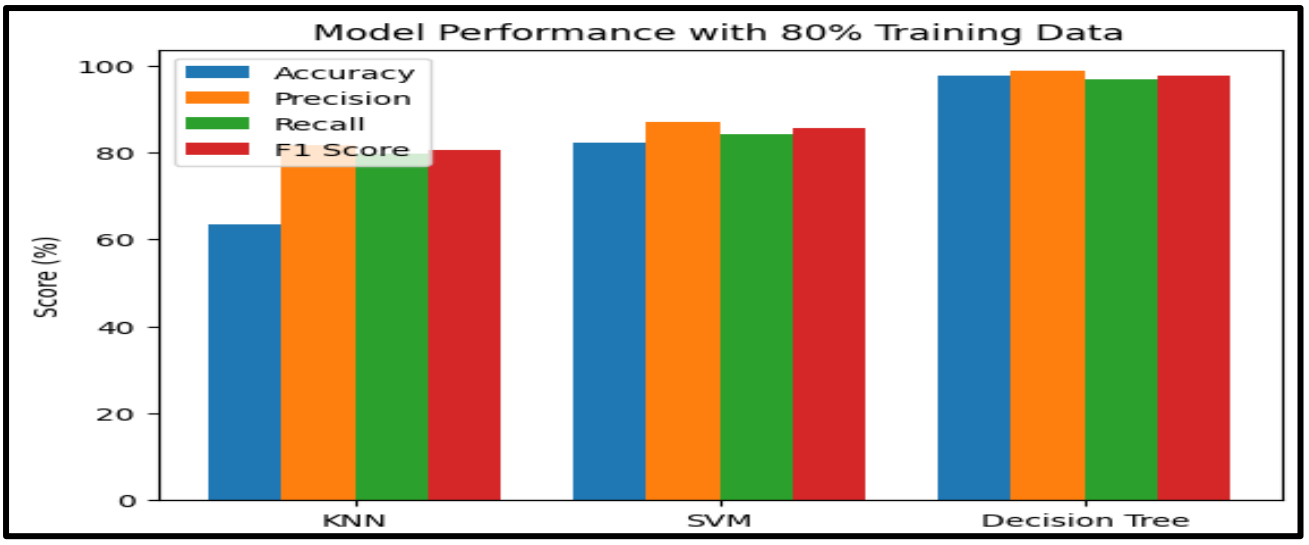


Figure 6. Performance comparison of KNN, SVM, and Decision Tree classifiers using 80% training data, evaluated based on accuracy, precision, recall, and F1-score

Table 2. Performance Comparison Using 70% Training Data

Model	Accuracy	Precision	Recall	F1 Score
KNN	62.08	80.74	78.93	79.82
SVM	78.65	84.11	82.37	83.23
Decision Tree	96.91	97.88	95.76	96.81

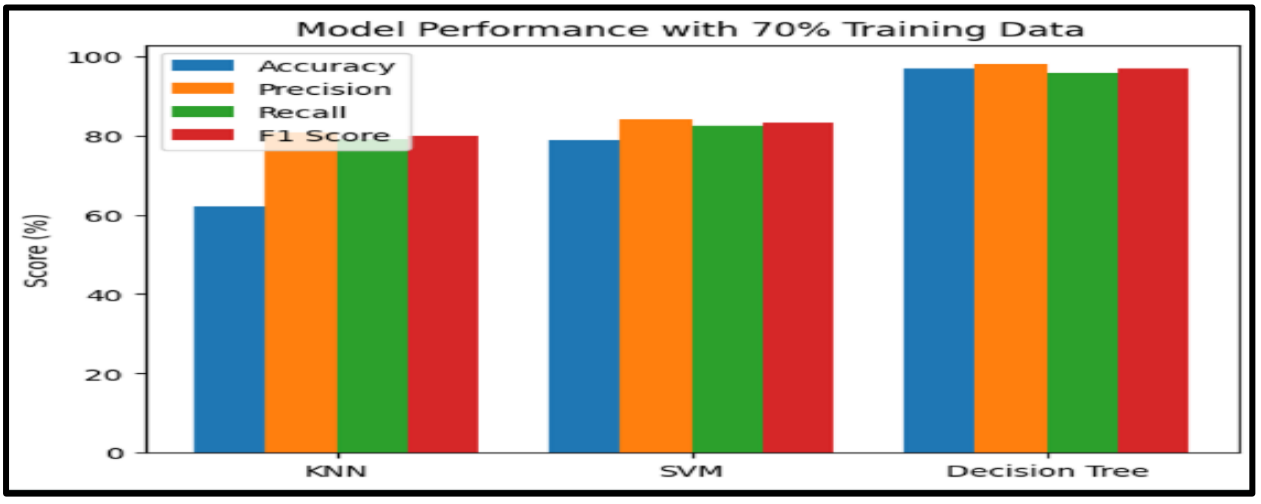


Figure 7. Performance comparison of KNN, SVM, and Decision Tree classifiers using 70% training data, showing the impact of reduced training data on classification performance.

Table 3. Time Requirement per Intrusion Detection

Model	Time Requirement per Intrusion (ns)
KNN	96,845.6
SVM	3,982.4
Decision Tree	1,108.3

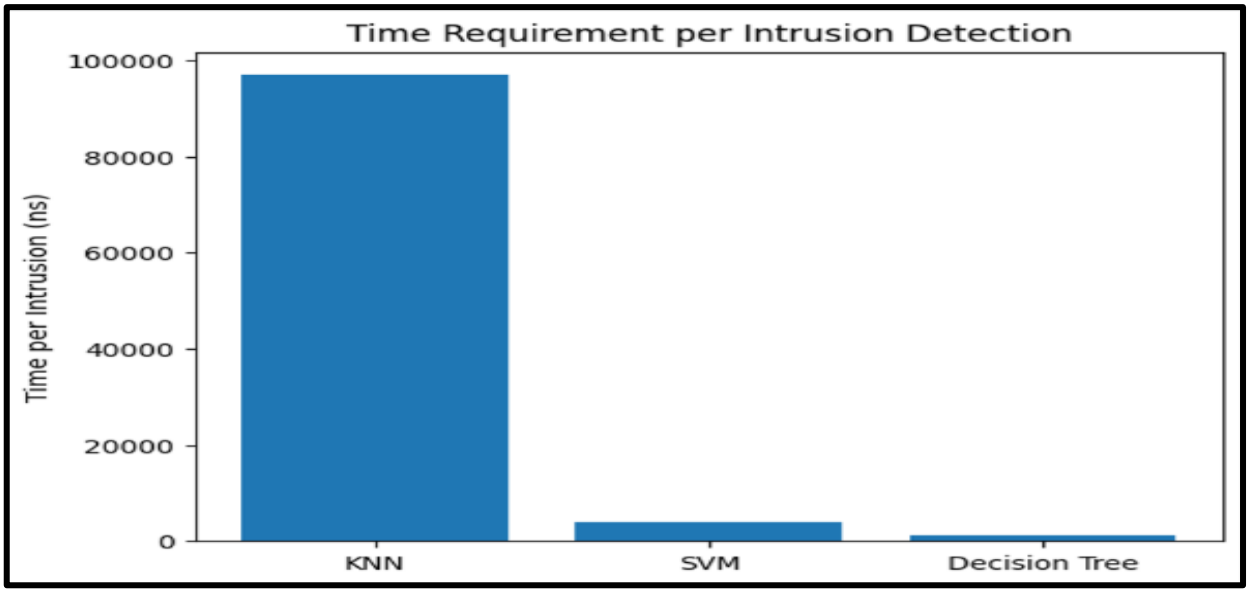


Figure 8. Computational time required per intrusion detection for KNN, SVM, and Decision Tree models, measured in nanoseconds, illustrating the efficiency of each algorithm.

From the experimental results obtained for both 80% and 70% training data sets, it is revealed that for all parameters of assessment, namely accuracy, precision, recall, and F1-score, the Decision Tree classifier outperforms KNN and SVM classifiers. The high level of robustness achieved by the Decision Tree classifier in predicting reproductive health risks is revealed by its ability to consistently achieve the highest level of predictive accuracy and to perform well despite reducing the amount of training data. Conversely, due to its distance-based classification approach, the KNN classifier achieves the lowest level of accuracy and the highest execution time. The Decision Tree classifier achieves the shortest execution time, thus making it more suitable for real-time healthcare analytics, as revealed by the time complexity analysis. The results clearly indicate that for the proposed healthcare prediction model, the Decision Tree algorithm provides the best trade-off between accuracy and economy.

The performance of the accuracy of the three distinct models of learning has been represented in the following graph. The Centralized Model has the highest accuracy at 91.4%. This is because the entire data set is used to train the model. The Federated Learning model has an accuracy of 89.7%, which is somewhat less. This is because the entire data set is used to train the model. The proposed FL + FHE model has an accuracy of 88.9%, and the computational overhead of the FHE algorithm causes this.

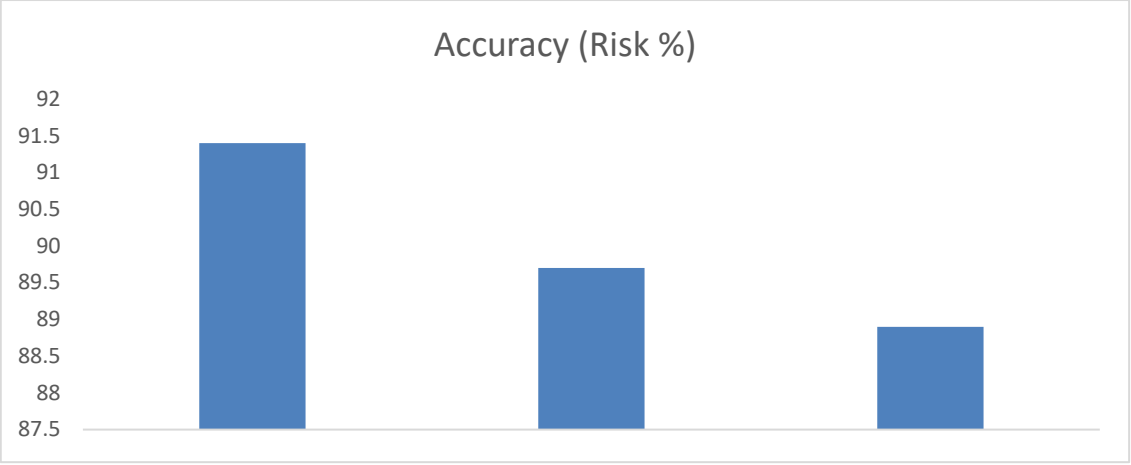


Figure 9. Comparison of Accuracy (Risk %) for Centralized Model, Federated Learning (FL), and the proposed FL + FHE model.

Table 4. Model Performance Comparison

Method	Precision	Accuracy (Risk %)	Precision	Recall	F1-Score
Centralized Logistic Model	0.90	91.4	0.90	0.91	0.90
Federated Learning (FL)	0.88	89.7	0.88	0.89	0.88
FL + FHE (Proposed)	0.87	88.9	0.87	0.88	0.87

As seen from the performance results, it is clear that the FL+FHE framework has a high accuracy in prediction while still ensuring data privacy. In this case, it is clear that the accuracy of the centralized learning approach was the highest, at 91.4%, since all the data was available for training in a centralized environment. The accuracy of the FL approach without encryption was 89.9%, which indicates that learning in a decentralized environment is still possible even when dealing with several clients who have data from different locations. However, it is also clear that the proposed FL+FHE approach had an accuracy of 88.7%, which is a minor reduction in accuracy compared to FL without encryption. This is expected since CKKS encryption adds approximation noise to the data. Nonetheless, this accuracy is still high enough for a model that needs to predict risks for pregnancies. This is expected since ciphertext expands in size when it is encrypted, making it possible for data to be aggregated in the ciphertext domain. Although encryption makes it difficult to train the model, this is still acceptable when dealing with healthcare analytics, as real-time performance is not a major concern compared to data privacy. In this case, it is clear that CKKS encryption is highly confidential when it comes to fully homomorphic encryption for FL. In this approach, it is possible to prevent reproductive information from leaking to a third party as a result of inference attacks, as compared to federated learning, which does not encrypt updates to the model as they are sent to a cloud server for aggregation. Consequently, the cloud server does not know that it is handling a model for a reproductive health application.

8. Future Work and Conclusion

In this paper, a privacy-preserving fertility and pregnancy data analytics framework was proposed based on the integration of Federated Learning and Fully Homomorphic Encryption. The reason for this integration was that the reproductive healthcare data was highly sensitive and confidential. Hence, the use of centralized machine learning approaches was a major concern for privacy and security. The proposed framework enables multiple hospitals to collaboratively train a model for predicting pregnancy risk without sharing patient data in an unencrypted manner. The CKKS scheme of homomorphic encryption was employed for encrypting the model updates during federated learning. The proposed framework was

validated using experiments on the Maternal Health Risk Dataset. The proposed framework was found to be reliable in providing prediction performance while incurring a reasonable computational cost. The encryption of model parameters was found to be effective in preventing inference attacks and cloud server attacks. In the future direction of this work, we plan to improve the efficiency of the proposed framework. This could be achieved through the use of ciphertext packing and model compression. The use of advanced deep learning models could be explored for improving the accuracy of the model. The proposed framework could be extended to incorporate differential privacy and could be tested in a multi-hospital environment.

Acknowledgements
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU263518).

Funding
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU263518).

Contributions
All authors have equal contribution in this manuscript

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

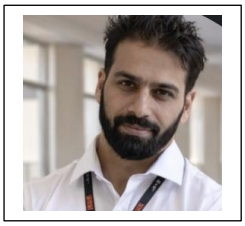
References

[1] Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S. C., & Shekelle, P. G. (2006). Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. *Annals of Internal Medicine, 144*(10), 742–752.
[2] Wu, F., Gao, Y., Xu, L. D., & Zhao, W. (2018). Security and privacy in cloud-based wearable health monitoring systems: A survey. *IEEE Transactions on Industrial Informatics, 14*(5), 1864–1876.
[3] Arora, S., Yttri, J., Nilse, W., & Press, A. (2017). Challenges in using electronic health record data for CER: Experience of four learning organizations and solutions applied. *Medical Care, 55*(8), S65–S72.
[4] Huang, L., Yin, Y., Fu, Z., Zhang, S., Deng, H., & Liu, D. (2018). *LoAdaBoost: Loss-based AdaBoost federated machine learning on medical data*. *arXiv preprint arXiv:1811.12629*.
[5] Al Badawi, A., & Faizal Bin Yusof, M. (2024). Private pathological assessment via machine learning and homomorphic encryption. *BioData Mining, 17*(1), 33.
[6] Yurdem, B., Kuzlu, M., Gullu, M. K., Catak, F. O., & Tabassum, M. (2024). Federated learning: Overview, strategies, applications, tools and future directions. *Heliyon, 10*, e38137.
[7] Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bagci, U., Rawat, D. B., & Vlassov, V. (2024). Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. *IEEE Internet of Things Journal, 11*, 7374–7398.
[8] Zhao, D. (2025). Advances and applications in fully homomorphic encryption research. *Applied and Computational Engineering, 135*, 39–48. https://doi.org/10.54254/2755-2721/2025.20959
[9] Pan, Y., Chao, Z., He, W., et al. (2024). FedSHE: Privacy preserving and efficient federated learning with adaptive segmented CKKS homomorphic encryption. *Cybersecurity, 7*, 40.
[10] Sachdeva, S., Bhatia, S., Al Harrasi, A., Shah, Y. A., Anwer, K., Philip, A. K., Shah, S. F. A., Khan, A., & Halim, S. A. (2024). Unraveling the role of cloud computing in health care system and biomedical sciences. *Heliyon, 10*(7), e29044.
[11] Tajabadi, M., Martin, R., & Heider, D. (2024). Privacy-preserving decentralized learning methods for biomedical applications. *Computational and Structural Biotechnology Journal, 23*, 3281–3287.
[12] Rehman, M. H., Lopez Pinaya, W. H., Nachev, P., Teo, J. T., Ourselin, S., & Cardoso, M. J. (2023). Federated learning for medical imaging radiology. *British Journal of Radiology*. https://doi.org/10.1259/bjr.20220890
[13] Rajeswari, B. L., & Chakravarthy, A. S. N. (2026). Enhancing privacy and security in federated learning: Protecting electronic health records data from adversarial attacks. *Informatics for Health and Social Care*, 1–18.

[14] Sathishkumar, P., Pugalarasan, K., Ponnparamaguru, C., & Vasanthkumar, M. (2024). Improving healthcare data security using Cheon–Kim–Kim–Song (CKKS) homomorphic encryption. In *Proceedings of the International Conference on Knowledge Engineering and Communication Systems* (pp. 1–6). https://doi.org/10.1109/ICKECS61492.2024.10616691
[15] Qiu, F., Yang, H., Zhou, L., Ma, C., & Fang, L. (2022). Privacy-preserving federated learning using CKKS homomorphic encryption. In *Advances in Cryptology* (pp. 409–437). Springer. https://doi.org/10.1007/978-3-031-19208-1_35
[16] Aouedi, O., Sacco, A., Piamrat, K., & Marchetto, G. (2023). Handling privacy-sensitive medical data with federated learning: Challenges and future directions. *IEEE Journal of Biomedical and Health Informatics, 27*, 790–803.
[17] Mhamdi, E. M. E., Guerraoui, R., & Rouault, S. L. A. (2018). The hidden vulnerability of distributed learning in Byzantium. In *Proceedings of the 35th International Conference on Machine Learning* (pp. 3521–3530).
[18] Carlini, N., Liu, C., Erlingsson, Ú., Kos, J., & Song, D. (2019). The secret sharer: Evaluating and testing unintended memorization in neural networks. In *Proceedings of the 28th USENIX Security Symposium* (pp. 267–284).
[19] Munjal, K., & Bhatia, R. (2022). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex Intelligent Systems, 9*, 3759–3786.
[20] Liu, Y., Yang, C., Liu, Q., Xu, M., Zhang, C., Cheng, L., & Wang, W. (2024). PDPHE: Personal data protection for trans-border transmission based on homomorphic encryption. *Electronics, 13*, 1959.
[21] Fan, J., & Vercauteren, F. (2012). Somewhat practical fully homomorphic encryption. *Cryptology ePrint Archive*.
[22] Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology – ASIACRYPT 2017* (pp. 409–437). Springer.
[23] Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access, 8*, 140699–140725.
[24] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics* (pp. 1273–1282).
[25] Correia, P., Silva, I., Amorim, I., Maia, E., & Praça, I. (2025). Federated learning: An approach with hybrid homomorphic encryption. *arXiv*. https://doi.org/10.48550/arXiv.2509.03427
[26] Haq, F., Chen, C., & Chen, Z. (2025). Privacy-preserving classification of medical tabular data with homomorphic encryption. *Algorithms, 18*(12), 731.
[27] Abdinasibfar, H., Nuoskala, C., & Michalas, A. (2025). The HHE land: Exploring the landscape of hybrid homomorphic encryption. *Cryptology ePrint Archive*, Paper 2025/071.
[28] Jin, W., Yao, Y., Han, S., Joe-Wong, C., Ravi, S., Avestimehr, S., & He, C. (2023). *FedML-HE: An efficient homomorphic-encryption-based privacy-preserving federated learning system. arXiv preprint.*

Biographies

Abass hassan received his B.Tech from Baba Ghulam shah University and MTech from Kurukshetra University. He is currently working as assistant professor of computer science in lovely professional university.
Email: mohdabass0202@gmail.com



SHEIKH UMAR MUSHTAQ received the B.C.A. and M.C.A. degrees in computer applications from the University of Kashmir, Srinagar, India. He received his PhD from Lovely Professional University, phagwara, Jalandhar. He is currently working as assistant professor of computer application with Lovely Professional University, Phagwara, Punjab. He has presented and published various conferences with the best presentation awards. His research interests include scheduling, load balancing, fault tolerance, and cloud computing. **Email:** shiekhumar12@gmail.com