Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Secure Privacy Preserving Banking Customer Churn Prediction using Federated Learning and Fully Homomorphic Encryption

Yasmin Gamal Fahmy[1,*], Mohamed Waleed Fakhr[1], Mohamed Kholief[1]

[1] College of Computing and Information Technology, Arab Academy for Science, Technology, and Maritime Transport, Cairo P.O. Box 2033, Egypt

ARTICLE INFO

Keywords:
Machine learning (ML); customer churn prediction (CCP); federated machine learning (FedML); artificial neural network (ANN); convolutional neural network (CNN); fully homomorphic encryption (FHE)

ABSTRACT

Banking domain is interested in customer churn prediction applications due to the rising competition with financial technologies (FinTech). This fierce competition is impacting banks market share, and it was found that it's much easier and less costly to keep existing customer rather than acquiring new customers to the bank. Secure privacy preserving Customer Churn Prediction is a challenging and interesting area for research. Federated Machine Learning (FedML) has been proposed to resolve privacy problem, by using federated learning (FL) to apply Machine Learning (ML) prediction at banks locally and was proven to be one of the most effective solutions for this challenge. However, some gaps are identified for using federated machine learning (FedML) like the security attacks targeting the aggregation server or communication with the clients. Accordingly, this research proposes securing FedML vulnerabilities using Fully Homomorphic Encryption (FHE) encryption through a secure privacy preserving framework for customer churn prediction. The proposed framework guarantees the privacy preserving of customer data using Federated Machine Learning (FedML) while securing the aggregation and communication against vulnerabilities by a (FHE) provably secure algorithm. The proposed solution is demonstrated using a public dataset to predict the customer churn of 3 bank clients in different locations. FedML is applied to ensure data privacy for each client by training the model locally while only sharing the updates. FHE is used to encrypt all the updates, model aggregation and model prediction. Prediction accuracy is compared for the global model, the FedML without encryption and the FedML with FHE encryption using neural network binary classifiers. The proposed framework achieved high prediction accuracy, very close to the baseline, in addition to providing privacy and security safeguards that are mandated in banking domain.

1. Introduction

1.1 Background

The rise of financial technologies (FinTech) has intensified competition within the banking sector, transforming the industry landscape. FinTech innovations, fuelled by vast amounts of data, have fundamentally altered customer interactions and expectations. In this dynamic environment,

* *Corresponding author.*
E-mail address: ygamal@outlook.com

https://doi.org/10.37934/araset.63.3.201215

customer retention has emerged as a strategic imperative for banks. Research demonstrates that even modest reductions in customer churn, such as a 5% improvement, can translate to substantial gains in customer-related profitability as shown by J. Brito *et al*., [1].

Consequently, banks must harness advanced analytical tools to gain understanding of the factors driving customer defection and implement proactive countermeasures. Beyond immediate revenue loss, customer churn has cascading effects on a bank's financial health, reputation, and competitive standing. Attrition erodes the lifetime value of customers, hindering long-term profitability. Moreover, high churn rates signal potential weaknesses in customer experience, product offerings, or operational efficiency factors that can damage a bank's brand perception and reputation as shown by P. Singh *et al.,* [2]. Therefore, churn analytics offer a window into the bank-customer relationship, empowering institutions to tailor strategies that foster loyalty and differentiation within an increasingly crowded marketplace.

Artificial Intelligence (AI), particularly machine learning (ML), has revolutionized numerous industries, including finance. Yet, the success of Deep Learning (DL) models and the sensitivity of banking data raise legitimate privacy concerns. Traditional centralized cloud models necessitate the aggregation of client information, increasing vulnerability to data breaches and potential misuse which is a significant risk in the financial sector. Furthermore, centralized architectures face bottlenecks in latency, bandwidth, and computational scalability, particularly as datasets and model complexity grow. Cross-device federated machine learning (FedML) offers an elegant solution, enabling collaborative model training without compromising data privacy. By training local models on-device and aggregating encrypted updates at a central server, FL preserves confidentiality while allowing for the development of robust global models avoiding disadvantages of the centralised model architecture such as high latency, long learning time, greater server load and expensive transmission time as explained further in several research [3-5].

While FedML offers compelling benefits, it's essential to acknowledge the unique security considerations it presents. The decentralized nature of federated learning (FL) introduces potential attack vectors through malicious clients, compromised aggregators, or external adversaries. A robust churn prediction solution within this framework necessitates a thorough analysis of these threat models and the development of appropriate countermeasures as shown by C. Zhang *et al.,* [6].

Encryption is one of the countermeasures that are proposed to further strengthen security. Within this paradigm, Fully Homomorphic Encryption (FHE) enables computations directly on encrypted data. This unlocks the potential for even greater privacy in FL systems, vital in the risk-sensitive financial domains.

1.2 Problem Statement & Research Objective

The primary objective of customer churn prediction is to minimize attrition by enhancing the accuracy, privacy, and security of prediction models. High-confidence, secure machine learning models allow banks to leverage these technologies to gain competitive advantages over FinTech companies by offering quicker and more personalized services, supported by secure decision-making processes due to the sensitive nature of customer data.

1.2.1 Research contribution

This research addresses securing customer sensitive data in prediction models by proposing a framework that resolves privacy concerns by applying FL, and addresses the FL security concerns by applying encryption, FHE. The proposed framework for secure and privacy preserving prediction

mode is applied for Customer churn prediction in the banking industry. Our approach aims to address the limitations of centralized models, offering a collaborative learning solution that safeguards sensitive customer data while enhancing predictive accuracy.

1.3 Related Work

1.3.1 Homomorphic encryption in federated settings

HE has gained power in FL to safeguard model privacy without sacrificing training efficiency. Key implementations include:

i. H. Fang *et al.,* used Paillier Federated Multi-Layer Perceptron (PFMLP), in 2021 [5] to implement a secure privacy preserving framework based on partially HE and FL where gradients are encrypted to secure the model against attacks, also the computation issue is considered where Paillier algorithm is used to speed up the training by around 25%.
ii. Zhang *et al.,* proposed BatchCrypt [6], this system utilizes a quantization scheme for secure FL in cross-silo settings, encoding weight updates as a batch of gradients processed using SIMD techniques. This method, supported by the Paillier scheme, enhances training efficiency with minimal accuracy loss.
iii. In Truex *et al.,* [7] and POSEIDON [8]: Both employ differential privacy and additive HE in federated settings. However, their approach of encrypting the entire FL process, including local training, results in significant computational burdens.
iv. Ma *et al.,* [9] They leverage the CKKS scheme through a multi-key approach (xMK-CKKS) that uses an aggregated public key, enabling model decryption only after clients exchange secret key information.
v. B. Wang *et al.,* proposed PPFLHE: A privacy-preserving federated learning scheme with HE & FL for health care data in 2023 [11] Where to encrypt the training model shared by users to ensure its security and privacy, HE is used. In addition, Access Control (AC) technology is used to prevent access attacks by confirming the user's identity and removing the dropped or unresponsive users temporarily to reduce the waiting delay and communication overhead. high data utility and classification accuracy (81.53%), and low communication delay is shown by achieved results while achieving privacy preserving.
vi. M. Arrazi *et al*., in 2023 proposed a global behavioural fingerprinting model for a target object, by analysing its interactions with different peers in the network using FL in addition to using HE and blockchain to guarantee the privacy of both the target object and the different workers achieving a secure privacy preserving framework with good prediction accuracy [12].

1.3.2 Using homomorphic encryption in federating setting for banking

i. PV4FAD, by S. Kadhe *et al.,* in 2023, proposed as a solution for privacy preserving training and inference of a predictor for financial anomaly detection. PNS and Banks train collaboratively using random decision tree where banks obtain encrypted leaf node labels using HE. Differential privacy is used to prevent inference threats [13].
ii. HYFL by H. Zhang *et al.,* in 2023, proposed a hybrid federated learning system that offers secure and privacy-aware learning and inference for financial crime detection. The server only has the model of feature extractors, but no features from the account clients while, the transaction client only has the extracted features but not the encoders, so it cannot recover the data from the features. Also to tackle privacy risks sources DP and HE are used [14].

1.3.3 Research Gap

The sensitive nature of banking customer data is the main challenge for using ML prediction models. The need for privacy preserving models is rising and FL is one of the main solutions that are proposed to resolve the privacy issue. However, applying FedML in banking domain still has a lot of security concerns and limitations due to the security vulnerabilities and attacks over FedML framework main components which are: the aggregation server, clients, and the communications between them.

1.4 Methods and Algorithms

1.4.1 Machine learning prediction models

Artificial Neural Network (ANN): Multilayer perceptron feedforward ANN with 2 hidden layers and a single sigmoid output for binary classification. The Multi-Layer Perceptron consists of millions of neurons patterned in layers and connected via weights. The first layer is called the input layer, followed by three hidden layers (3 layers) - input size 9 *36 features. Finally, the output layer exists, as shown in Figure 1. The significant benefit of increasing the hidden layers is increasing the ability of the network to extract the non-linearity of data.

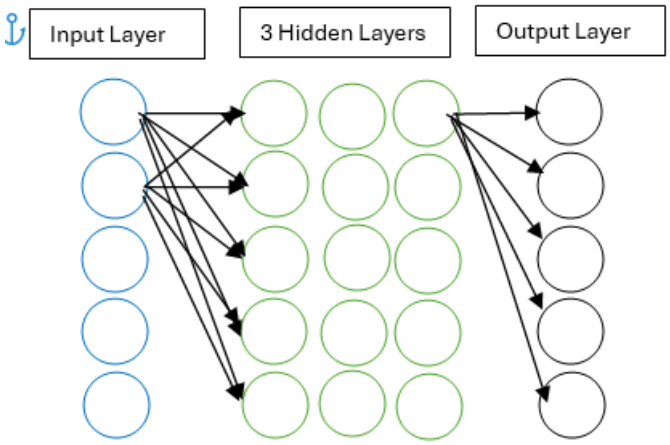

Fig. 1. Deep neural network

Convolutional Neural Network (CNN): In fully feed-forward neural networks, each neuron has a weighted connection to all neurons in the next layer. CNNs are a specific type of feed-forward neural networks in which the connectivity pattern between its neurons is inspired by the organization of the animal visual cortex. They have proven to be very effective in areas such as image recognition and classification. Neurons in different layers are of different types. Neurons in the input layer only get one input and output which is the same value. Neurons in hidden layers are more complex; they get inputs, compute the weighted summation of inputs, operate a function on the summation and then output the value of the function. These functions could be Sigmoid, Max, or Mean functions and are called activation functions (or transfer functions). CNN model used in proposed solution is 1 dimensional for classification, and it has three layers: convolutional layer, Pooling Layer, Fully Connected Layers, and activation functions. The learning rate 0.005 works well for CNN. A neuron represents a computational node in a layer. Each neuron takes input from previous layer and applies a transformation involving weights and biases to produce an output. Figure 2 shows 1 Dimensional CNN.

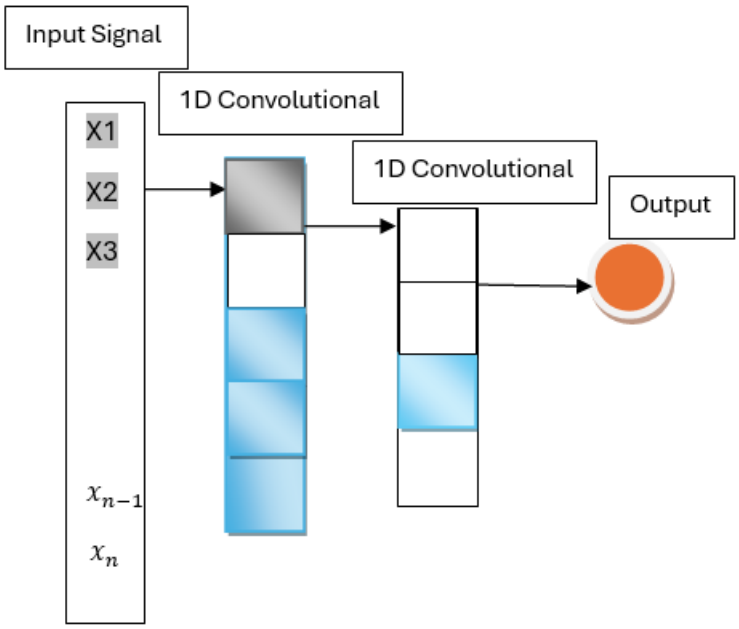

Fig. 2. 1 Dimensional CNN

1.4.2 Federated learning (FL)

Introduced by McMahan *et al.,* in 2017 [15], FL enables model training across mobile devices using private data that remains on-device. The Federated Average (FedAvg) algorithm, commonly employed in FL, involves training models locally, aggregating them periodically to form a new global model, and distributing it for further training rounds. FL originated from Google as a solution for multi-party ML, aiming to enhance data privacy and collaborative learning. Initially intended for local model updates on Android devices, its scope has expanded to include applications in medical data privacy, natural language processing, and recommendation systems. Recent advancements include integrating differential privacy to mitigate privacy risks and deploying vertical federated learning with homomorphic encryption.

1.4.3 Cross-device federated machine learning (FedML)

Decentralised approach to centralised machine learning. In FL, clients have their own local ML model, whereas the global ML model resides in a central server. Each client uses its private data to train its local model then send all its calculated model parameter to the central server. The central server then aggregates all the model parameters received from the edge devices to develop the global model. Thus, the central server builds a joint global ML model without collecting any personal data as described by C. Jagad *et al.,* [3].

In proposed solution, we applied FedML, however it introduced new threat models, resulting in unique vulnerabilities and bear three potential adversaries: in clients, the aggregator server and outsiders or eavesdroppers. An adversary may hold a mixture of different capabilities and defining them is necessary to understand how different attacks work and provide defence mechanisms accordingly. More details are provided in research by C. Zhang *et al.,* [6]. FedML advantages are privacy, where data remains on the device while only parameter weights and gradient updates are transmitted from edge devices to the server. And reduced server load since most computations occur on client devices. While its main disadvantage is its vulnerability to attacks: like data and model poisoning.

As introduced by N. Buacida *et al.,* [10] FL has several vulnerabilities & defense mechanisms: Sharing FL model parameters and frequent communication expose the system to new risks and potential privacy breaches. Adversaries may exploit these to manipulate model outputs or access sensitive information. Researchers explored these unique security concerns with FL adoption and discussed mitigative strategies like employing FHE to safeguard against these risks.

Sources of vulnerabilities in FL:

i. Communication Security: Leakage during communication between server and clients
ii. Gradient Leakage: Adversaries can infer sensitive information from gradients.
iii. Compromised Clients: Clients in FL have potential to manipulate the model by altering data or parameters.
iv. Server Security: in cloud-based setups, central servers are susceptible to hacking.
v. Aggregation Algorithm: Essential for detecting and mitigating malicious updates from clients, maintaining the global model's integrity.

Defenses in FL: Are critical for mitigating a range of attacks and reducing risk exposure. These defenses ensure the integrity of the global model by promoting adherence to the true statistical distribution of the training data, while minimizing the impact of any malicious updates.

i. Secure Aggregation and communication: Uses cryptographic methods like HE to protect individual model updates during aggregation and prevents eavesdropping when servers compute on encrypted model updates.
ii. Differential Privacy: Applies noise to updates to obscure individual data points, protecting against data inference from aggregated information. Byzantine Fault-Tolerant Aggregation (BFT): Addresses the challenge of nodes behaving maliciously or becoming compromised by maintaining system functionality despite a subset of faulty nodes. Anomaly Detection: Identifies deviations from normal operation, crucial for spotting compromised nodes. However, in our research we used FHE encryption since it is the most compatible to secure the federated framework in terms of its clients and server aggregation. Federated Learning Technologies: As shown by B. Soudan *et al.,* [4] FL frameworks have evolved significantly through academic and industry efforts. In our proposed solution we and used the following technologies:
iii. Flower: An open-source FL framework built on Python, Flower facilitates decentralized model training across devices or servers. Compatible with leading deep learning libraries such as TensorFlow and PyTorch, it supports scalable client-server interactions.
iv. FedML: A research-oriented open library and benchmark, FedML offers support for various FL configurations, including on-device training for edge devices, distributed computing, and simulations on single machines. It is a flexible API and provides robust baseline implementations FedML employs virtual nodes and central server architecture.

Also in our proposed framework, Federated aggregation is used as an optimization algorithm that is different from distributed ML and it has several key properties that differentiate it from a typical distributed optimization: non-IID. The training data on local dataset will not be representative of the population distribution, Unbalanced Similarly, varying amounts of local training data. And Limited communication where Clients are frequently offline or on slow or expensive connections. Weighted averaging of model parameters in FL is shown in Eq. (1)

$$w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^{k} \quad (1)$$

K is the number of participants, n_k is the number of samples of participants k, n is the number of samples of all participants. w_{t+1}^{k} is the local model parameter of participant k.

1.4.4 *Fully homomorphic encryption*

HE facilitates computation on encrypted data without decryption, preserving data structure. Essential for federated learning, it allows secure model updates aggregation. HE types vary by the operations they support: Partially Homomorphic (PHE), Somewhat Homomorphic (SHE), and Fully Homomorphic (FHE), with FHE supporting unlimited operations essential for federated contexts. Additionally, HE, is used in cross-silo FL applications to ensure privacy without compromising accuracy, allowing secure, encrypted data aggregation without prior decryption.

In 2009, Craig Gentry first proposed a fully homomorphic encryption (FHE) algorithm based on ideal lattices which satisfied both additive homomorphism and multiplicative homomorphism [16]. Since FHE has extremely high security, it has been widely used and it made great contributions to privacy protection [17-20].

In proposed solution, we used CKKS algorithm which is a fully homomorphic encryption (HE) scheme used for encrypted computation. Its full name is "Cheon-Kim-Kim-Song" and was proposed by Cheon *et al.,* (2017) [21]. The CKKS algorithm can support encrypted computation for complex and real number data and can achieve relatively high encryption computation accuracy and small ciphertext expansion factors. Unlike other HE schemes, the CKKS scheme supports approximate arithmetic over complex numbers. The CKKS scheme basically consists of those algorithms: key Generation, encryption, decryption, homomorphic addition and multiplication, and rescaling. For a positive integer q, let Rq: $=R/qR$ be the quotient ring of R modulo q. Let χs, χr and χe be distributions over R which output polynomials with small coefficients. These distributions, the initial modulus Q, and the ring dimension n are predetermined before the key generation phase. The key generation algorithm is following and represented in Eq. (2,3,4).

i. Sample a secret polynomial $s \leftarrow \chi s$. Then Sample aa (resp. a') uniform randomly from RQ (resp. R_{PQ}), and e, $e' \leftarrow \chi e$.

ii. Output a secret key:

$$sk \leftarrow (1, s) \in R_Q^2 \tag{2}$$

iii. Output a public key

$$pk \leftarrow (b = -a \cdot s + e, a) \in R_Q^2 \tag{3}$$

iv. Output an evaluation key

$$evk \leftarrow (b' = -a' \cdot s + e' + P \cdot s2, a') \in R_{PQ}^2 \tag{4}$$

The encryption algorithm is following and represented in Eq. (5)

i. Sample an ephemeral secret polynomial $r \leftarrow \chi r$.
ii. For a given message polynomial $m \in R$, output a ciphertext

$ct \leftarrow (c0 = r \cdot b + e0 + m,\ c1 = r \cdot a + e1) \in R_Q^2$ (5)

The decryption algorithm is following and represented in Eq. (6,7).

i. For a given ciphertext $ct \in R_Q^2$, output a message:

$m' \leftarrow \langle ct, sk \rangle$</$math$><$math$> (mod q) (6)

ii. The decryption outputs an approximate value of the original message .

Dec (sk, (pk, m)) ≈mDec(sk, Enc(pk,m))≈m (7)

The homomorphic addition algorithm is following and represented in Eq. (8,9).

i. Given two ciphertexts ct and ct' in R_Q^2, output addition:

$ct_{add} \leftarrow ct + ct' \in R_Q^2$ (8)

ii. The correctness holds as:

Dec(sk,ct_{add})≈Dec (sk, ct) +Dec (sk, ct') (9)

The homomorphic multiplication algorithm is following and represented in Eq. (10,11).

i. Given two ciphertext ct= ($c0$, $c1$) and ct'= ($c0'$, $c1'$) in R_Q^2,

compute ($d0$, $d1$, $d2$) =($c0c0'$,$c0c1'$+$c1c0'$,$c1c1'$)(mod q). $\boldsymbol{ct_{mult}} \leftarrow$ ($d0$, $d1$) +$\lfloor \boldsymbol{P^{-1}} \cdot d2 \cdot evk \rceil \in \boldsymbol{R_Q^2}$ (10)

ii. The correctness holds:

Dec (sk, $ct_{mult} \leftarrow$) ≈Dec(sk, ct)·Dec(sk,ct') (11)

All equations are proposed by Cheon *et al.,* in [21].

2. Methodology

2.1 Proposed Architecture

This research aims to develop a secure, privacy-preserving deep learning model for predicting customer churn in the banking sector. The proposed architecture employs Artificial Neural Networks (ANN) and Convolutional Neural Networks (CNN) to enhance prediction accuracy. To safeguard the sensitive customer data inherent in the banking domain, the model incorporates Federated Learning (FL) and Fully Homomorphic Encryption (FHE), enabling operations on encrypted data without compromising data privacy. The architecture integrates FHE with FL to maintain data privacy and security across distributed computing environments. This dual approach ensures that all machine learning operations are performed on encrypted data (ciphertext), thereby enhancing the security of

the federated learning model. Figure 3 shows the architecture of the proposed framework and demonstrates the steps performed at each party.

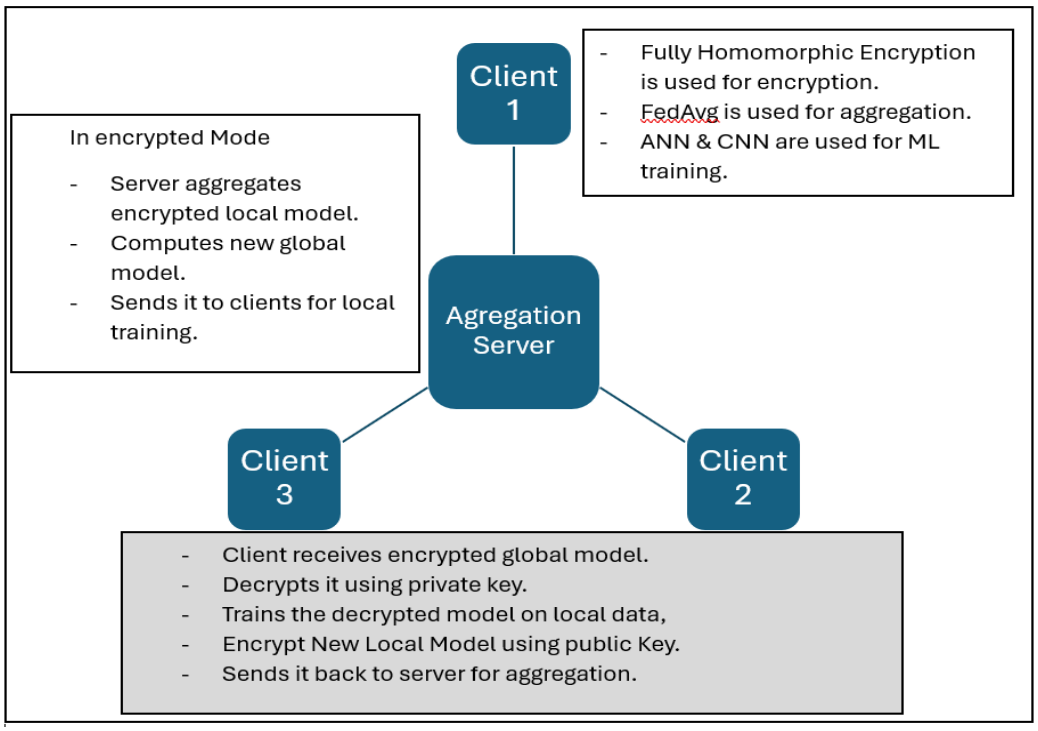

Fig. 3. Secure, Privacy Preserving ML for CCP

2.2 Method and Algorithm

2.2.1 Data preprocessing and federation

The model's objective is to predict bank customer churn using a federated learning framework that integrates ANN and CNN with FHE. The process is structured as follows:

Data Distribution and Preprocessing:
Data is allocated among three clients based on geographical location.
Each client performs the following preprocessing steps:

i. Loading the dataset.
ii. Removing irrelevant columns such as 'Exited', 'RowNumber', 'CustomerId', and 'Surname'.
iii. Encoding categorical variables (e.g., 'Gender').
iv. Normalizing all numerical values to a [0,1] range.
v. Partitioning data into training and testing subsets with an 80%-20% split.
vi. Organizing training data into batches to facilitate model training.

Federated Training Process:
Each client conducts the following operations in parallel for each training round:

i. Training the local model on a batch of data using both CNN and ANN techniques.
ii. Generating corresponding secret and public cryptographic keys.
iii. Encrypting model parameters using the CKKS encryption scheme.
iv. Transmitting the encrypted parameters and the public key to a central server.

The central server performs the following:

i. Aggregating all received encrypted parameters using the Federated Averaging (FedAVG) method.
ii. Sending the aggregated encrypted parameters back to the clients.

Each client then:

i. Decrypts the received parameters using their private key.
ii. Updates the local model parameters with the decrypted values.
iii. Proceeds to retrain the model with new data.

Hence, this architecture aims to demonstrate that integrating FHE with FL can effectively secure data privacy while maintaining high levels of predictive accuracy in a sensitive domain such as banking. The detailed methodology ensures a systematic approach to training and evaluating the model, emphasizing the feasibility of secure, distributed deep learning applications.

2.2.2 *Federated learning with homomorphic encryption*

In a centralized federated learning (FL) environment enhanced with Homomorphic Encryption (HE), the training process involves each participant training a local model on private data, followed by secure aggregation of these models to update the global model without compromising data privacy. The process within an encrypted centralized federation incorporates critical steps of encryption, encrypted aggregation, and decryption, ensuring data privacy throughout the model training and aggregation phases.

i. Encryption:
   - Each participant, referred to as a learner, encrypts their locally trained model using an HE schemes. This is achieved through the equation:

   Encrypted Model N=HE public key (Model N) Encrypted Model*i*=HE public key (Model*i*)

   - The model parameters are treated as vectors of ciphertext objects, each representing an array of the model. The encrypted data from each learner is aggregated into a concatenated collection of flattened data-vectors.

ii. Encrypted Weighted Aggregation:
   - Upon receiving the encrypted models, the federation controller performs a secure, weighted aggregation to compute the new encrypted global model. This step is crucial as it prevents the decryption or exposure of individual models.
   - The weight proportional to the dataset size of the client, aligning with the Federated Averaging (FedAvg) algorithm. This method ensures that models trained on larger datasets have a proportionally greater influence on the global model.

iii. Decryption and Local Training:
- The aggregated encrypted global model is then sent back to all clients. Each client decrypts it using their private key.
- Clients then proceed to train the decrypted global model on their local datasets, further refining the model based on new local data.

2.3 Diagrammatic and Algorithmic Representation

Proposed Framework is illustrated in Figure 4 and Algorithm 1 providing a visual and procedural depiction of the encrypted FL process.

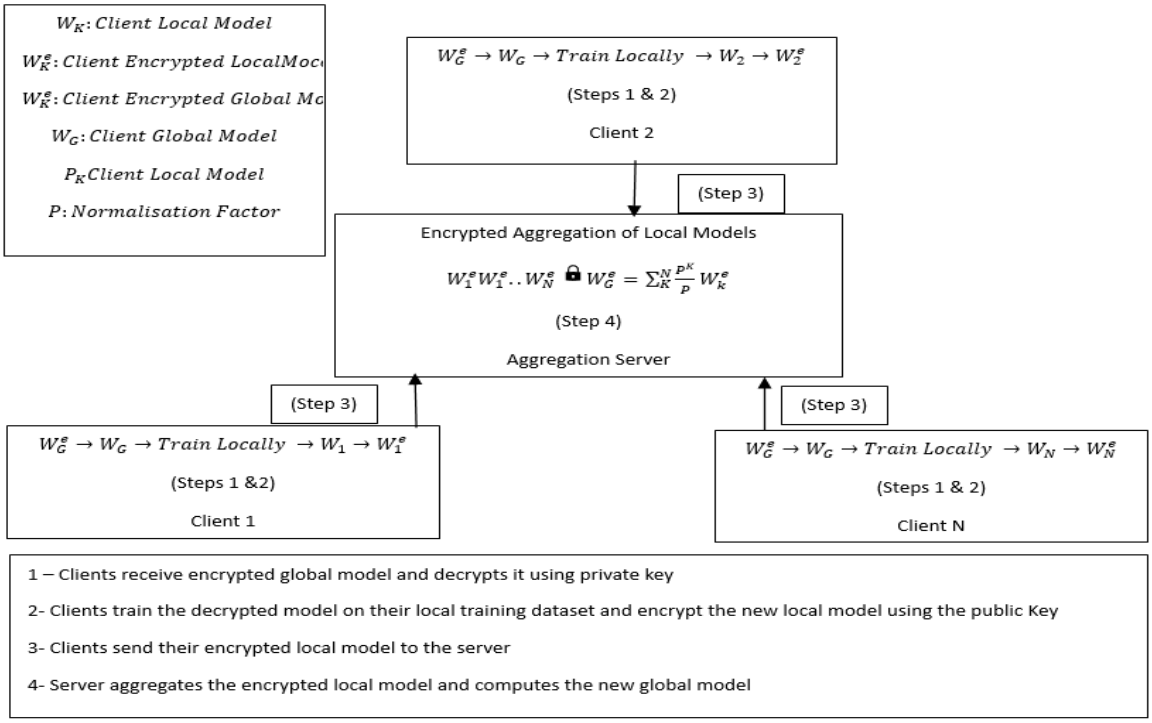

Fig. 4. Schematic representation of proposed framework

Algorithm 1: Federated Learning with Homomorphic Encryption

Encrypted global model W_c^e is computed with N clients, each indexed by k; β is the batch size η is the learning rate. E are the local epochs

Initialize $W_c \eta Server$:

$W_c^e = encrypt\ initial\ global\ model\ for\ t = 0, \dots, T-1\ do$

For each client K $\epsilon\ N$ in parallel do

Send encrypted global model W_c^e

$W_K = Client\ Opt(W_c^e)$

W_c^e= encrypted aggregation of all W_k

$W_t = decrypt\ \ global\ model\ W_t^e B$

$- Split\ training\ data\ D_k^T into\ batches\ of\ size\ \beta\ for\ i\ \epsilon\ E\ do$

For b ϵ B do

W_{t+1}^e= encrypt W_{t+1}send $W_{t+1}^e$to controller

3. Results

3.1 Experimental Dataset and Environment

In this research we face a very strong challenge which is getting real banking dataset for implementing proposed solution experiment. This challenge is due to the sensitivity of customer data and the sacristy of customer churn datasets for banking applications. In our experiment we wanted to have a various number of clients, where model can be run separately at each client. Which is the main concept of running FedML model. A publicly available dataset is used to rum our experiment and provide a proof of concept for the proposed solution, which is a public churn modelling data set, downloaded from Kaggle website, specifically for banking domain, where customer churn selected features are used for prediction. The training data has:

i. Data of 10,000 customer
ii. 10 selected features.
iii. Classified: with a decision (Exited or not)
iv. Divided into 3 different locations countries. (France, Spain & Germany)
v. Features are mentioned below:
vi. For each client, 80% of the dataset is used for training. 20 % is used for testing.

Table 1
Dataset features

Feature	Discerption
Credit Score	Can influence customer churn since a customer with a higher credit score is less likely to leave the bank.
Geography	A customer's location can affect their decision to leave the bank.
Gender	It's interesting to explore whether gender plays a role in a customer leaving the bank.
Age	Older customers are less likely to leave their bank than younger ones.
Tenure	Refers to the number of years that the customer has been a client of the bank. Normally, older clients are more loyal and less likely to leave a bank.
Balance	People with a higher balance in their accounts are less likely to leave the bank compared to those with lower balances
Num Of Products	Refers to the number of products that a customer has purchased through the bank
Has Credit Card	Denotes whether a customer has a credit card. This column is also relevant since people with a credit card are less likely to leave the bank
Is Active Member	Active customers are less likely to leave the bank
Estimated Salary	As with balance, people with lower salaries are more likely to leave the bank compared to those with higher salaries

3.2 *Accuracy Comparison*

For comparison, the FedML framework and Encrypted FedML with FHE algorithms are compared using the same network structure for model training while learning the same dataset. Supposing that we have 3 learning clients, we split the dataset into 3 subsets, for each geographical location and distribute them to 3 learning clients: France, Spain & Germany. The experiment is repeated using 2 different DL methodologies to ensure results accuracy using the top 2 prediction techniques with highest prediction results obtained. The first DL methodology that is used is ANN where we run the experiment with FEDML without FHE, then we run it again using FHE. Table 2 shows the results for ANN model.

Table 2
ANN model results comparison

Model	ANN (3 layers)					
Encryption	Non-FHE			FHE		
Client	France	Germany	Spain	France	Germany	Spain
Accuracy	85.34	73.1075	87.7	85.54	73.7051	86.3
Time in Sec.	119.6	80.1078	44.9	98.76	72.5189	50.2
Average Memory per vector	480			1728		

The second DL methodology that is used is CNN where we run the experiment with FEDML without FHE, then we run it again using FHE as shown in Table 3.

Table 3
CNN Model results comparison

Model	CNN					
Encryption	Non-FHE			FHE		
Client	France	Germany	Spain	France	Germany	Spain
Accuracy	85.515	76.545	87.384	88.818	76.545	84.539
Time in Sec.	254.48	203.23	152.008	234.38	203.62	172.665
Average Memory per vector	480			1728		

The experiments on the CCP dataset show that the model trained by ANN / Non FHE can reach an accuracy rate of 0.820 on the testing set, while the model trained by ANN & FHE can reach an accuracy rate of 0.818, just 0.002 lower than that of the non-encrypted FedML. For CNN model, since models on each client learned from the same FedML, we perform a weighted average of the results of the two experiments based on the amount of the testing set and get a final prediction accuracy rate of 0.831. Compared with the FEDML & FHE model with an accuracy rate of 0.833 after learning all the data, the accuracy rate has only increased by 0.002. Therefore, from the experimental results on the same dataset using the 2 different DL algorithms, it shows that the encrypted FedML (With FHE) algorithm can train a model with almost the same accuracy rate as the non-encrypted FedML on all data from multiple clients and using different algorithms.

3.3 *Comparison of Model Training Time for Different Algorithms with & without encryption*

Due to the threat of membership inference attacks, transmitting gradient data in plain text may be exploited by a malicious user to train his own shadow models. The privacy related data security of other clients will be violated. Here, we use FHE. In addition, the encryption is operated during the gradient data transmission, and homomorphic operations are performed in the computing server to ensure that the encrypted gradient data will not be leaked, even if the server has security vulnerabilities. From the above experiment, it shows that, under 2 different models, very close prediction accuracy takes different time in seconds., where average time taken by ANN is 82.5 seconds, while average time taken by CNN is 203.2 seconds. However, there is no big difference between time taken while running non-encrypted model and encrypted model using FHE, where for example time taken for CNN before encryption is 203.23 seconds while the time taken after using FHE is 203.55 seconds. Thus, it says that the time overhead is positively related to the model that is being used for prediction (ANN or CNN)/ While when we use the encrypted FedML solution to

conduct experiments on the dataset and compare the time costs of encryption and decryption with the same gradient data in the same round of iteration, it shows very close results ensuring that the time cost of encryption is relatively not high and acceptable.

4. Conclusion

The integration of HE within FL presents a robust mechanism for maintaining comprehensive data privacy while enabling collaborative model training. By encrypting model parameters before aggregation and only decrypting them at the learner's end, this approach effectively shields sensitive data during the learning process enabling bank to compete with the rising power of FinTech's & entrepreneurship, where a study shows that 12 countries have examined the importance of entrepreneurial interest and the role of entrepreneurship education in developing a culture of innovation, risk-taking, and business creation among university students showing that he potential impact of fintech's on economic development is significant [22].

The use of weighted aggregation based on local dataset sizes optimizes the learning process, ensuring that all data contributions are appropriately valued in the global model's development. This secure framework is vital for sensitive sectors such as healthcare and finance, where data confidentiality is paramount.

Acknowledgement
This research was not funded by any grant.

References

[1] Brito, João BG, Guilherme B. Bucco, Rodrigo Heldt, João L. Becker, Cleo S. Silveira, Fernando B. Luce, and Michel J. Anzanello. "A framework to improve churn prediction performance in retail banking." *Financial Innovation* 10, no. 1 (2024): 17. https://doi.org/10.1186/s40854-023-00558-3

[2] Singh, Pahul Preet, Fahim Islam Anik, Rahul Senapati, Arnav Sinha, Nazmus Sakib, and Eklas Hossain. "Investigating customer churn in banking: A machine learning approach and visualization app for data science and management." *Data Science and Management* 7, no. 1 (2024): 7-16. https://doi.org/10.1016/j.dsm.2023.09.002

[3] Jagad, Chirag, Chirag Jain, Dhrumil Thakore, Om Naik, and Vinaya Sawant. "Federated Machine Learning-Based Bank Customer Churn Prediction." In *Practical Data Mining Techniques and Applications*, pp. 77-88. Auerbach Publications, 2023.

[4] Soudan, Bassel, Sohail Abbas, Ahmed Kubba, Manar Abu Wasif Talib, and Qassim Nasir. 2024. "Scalability and Performance Evaluation of Federated Learning Frameworks: A Comparative Analysis." Research Square. February 9, 2024. https://doi.org/10.21203/rs.3.rs-3934159/v1.

[5] Fang, Haokun, and Quan Qian. "Privacy preserving machine learning with homomorphic encryption and federated learning." *Future Internet* 13, no. 4 (2021): 94. https://doi.org/10.3390/fi13040094

[6] Zhang, Chengliang, Suyi Li, Junzhe Xia, Wei Wang, Feng Yan, and Yang Liu. "{BatchCrypt}: Efficient homomorphic encryption for {Cross-Silo} federated learning." In *2020 USENIX annual technical conference (USENIX ATC 20)*, pp. 493-506. 2020.

[7] S. Treux, N. Baracaldo." A Hybrid Approach to Privacy-Preserving Federated Learning." [*Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*], CCS Concepts (2019). https://doi.org/10.48550/arXiv.1812.03224

[8] Sav, S., Pyrgelis, A., Troncoso-Pastoriza, J., Froelicher, D., Bossuat, J.-P., Sousa, J. S., and Hubaux, J., "Poseidon: Privacy-preserving federated neural network learning." Network and Distributed Systems Security (NDSS) Symposium 2021. ArXiv abs/2009.00349 (2021). https://doi.org/10.1016/j.patter.2022.100487

[9] Ma, Jing, Si-Ahmed Naas, Stephan Sigg, and Xixiang Lyu. "Privacy-preserving federated learning based on multi-key homomorphic encryption." *International Journal of Intelligent Systems* 37, no. 9 (2022): 5880-5901. https://doi.org/10.1002/int.22818

[10] Bouacida, Nader, and Prasant Mohapatra. "Vulnerabilities in federated learning." *IEEe Access* 9 (2021): 63229-63249. https://doi.org/10.1109/ACCESS.2021.3075203

[11] B. Wang. H. Li et al. PPFLHE: "A privacy-preserving federated learning scheme with Homomorphic Encryption for Health Care Data." Applied Soft Computing. El Sevier 2023. https://doi.org/10.1016/j.asoc.2023.110677

[12] Arazzi, Marco, Serena Nicolazzo, and Antonino Nocera. "A fully privacy-preserving solution for anomaly detection in iot using federated learning and homomorphic encryption." *Information Systems Frontiers* (2023): 1-24. https://doi.org/10.1007/s10796-023-10443-0

[13] Kadhe, Swanand Ravindra, Heiko Ludwig, Nathalie Baracaldo, Alan King, Yi Zhou, Keith Houck, Ambrish Rawat et al. "Privacy-Preserving Federated Learning over Vertically and Horizontally Partitioned Data for Financial Anomaly Detection." *arXiv preprint arXiv:2310.19304* (2023). https://doi.org/10.48550/arXiv.2310.19304

[14] H. Zhang, J. Hong et al." A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection." Under Review. (2023). https://doi.org/10.48550/arXiv.2302.03654

[15] HB. McMahan, E. Moore *et al.,"* Communication-Efficient Learning of Deep Networks from Decentralized Data." International Conference on Artificial Intelligence and Statistics (AISTATS). (2017) https://doi.org/10.48550/arXiv.1602.05629

[16] C. Gentry. "Fully homomorphic encryption using ideal lattices." In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Washington, DC, USA. (2009) pp. 169–178. https://doi.org/10.1145/1536414.1536440

[17] Van Dijk, Marten, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. "Fully homomorphic encryption over the integers." In *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pp. 24-43. Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-13190-5_2

[18] Ibtihal, Mouhib, El Ouadghiri Driss, and Naanani Hassan. 2017. "Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment." *International Journal of Cloud Applications and Computing* 7 (2): 27–40. https://doi.org/10.4018/ijcac.2017040103

[19] El Makkaoui, Khalid, Abdellah Ezzati, Abderrahim Beni-Hssane, and Slimane Ouhmad. "Fast Cloud–Paillier homomorphic schemes for protecting confidentiality of sensitive data in cloud computing." *Journal of Ambient Intelligence and Humanized Computing* 11, no. 6 (2020): 2205-2214. https://doi.org/10.1007/s12652-019-01366-3

[20] Çatak, Ferhat Özgür, and Ahmet Fatih Mustacoglu. "CPP-ELM: cryptographically privacy-preserving extreme learning machine for cloud systems." *International Journal of Computational Intelligence Systems* 11, no. 1 (2018): 33-44.https://doi.org/10.2991/ijcis.11.1.3

[21] Cheon, Jung Hee, Andrey Kim, Miran Kim, and Yongsoo Song. "Homomorphic encryption for arithmetic of approximate numbers." In *Advances in cryptology–ASIACRYPT 2017: 23rd international conference on the theory and applications of cryptology and information security, Hong kong, China, December 3-7, 2017, proceedings, part i 23*, pp. 409-437. Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-70694-8_15

[22] R. Verawati, M. R. Yacoob, Students' Interest in Start Up Business: "A Systematic Literature Review". Journal of advanced research in business and management studies. September 2024. https://doi.org/10.37934/arbms.36.1.2642