Vertically Federated Graph Neural Network for Privacy-Preserving Node Classification

Chaochao Chen\textsuperscript{1}, Jun Zhou\textsuperscript{1,2}, Longfei Zheng\textsuperscript{2}, Huiwen Wu\textsuperscript{2}, Lingjuan Lyu\textsuperscript{3}, Jia Wu\textsuperscript{4}, Bingzhe Wu\textsuperscript{5}, Ziqi Liu\textsuperscript{2}, Li Wang\textsuperscript{2}, Xiaolin Zheng\textsuperscript{3,6}\textsuperscript{*}

\textsuperscript{1}College of Computer Science and Technology, Zhejiang University, Hangzhou, China
\textsuperscript{2}Ant Group, Hangzhou, China
\textsuperscript{3}Sony AI, Tokyo, Japan
\textsuperscript{4}Macquarie University, Sydney, NSW 2109, Australia
\textsuperscript{5}Peking University, Beijing, China
\textsuperscript{6}JZTData Technology, Hangzhou, China

\{zjucc, xlzheng\}@zju.edu.cn, Lingjuan.Lv@sony.com, jia.wu@mq.edu.au, wubingzhe@pku.edu.cn, \{jun.zhoujun, zlf206411, huiwen.whw, ziqiliu, raymond.wangl\}@antgroup.com

Abstract

Graph Neural Network (GNN) has achieved remarkable progresses in various real-world tasks on graph data. High-performance GNN models always depend on both rich features and complete edge information in graph. However, such information could possibly be isolated by different data holders in practice, which is the so-called data isolation problem. To solve this problem, in this paper, we propose Vertically Federated Graph Neural Network (VFGNN), a federated GNN learning paradigm for privacy-preserving node classification task under data vertically partitioned setting, which can be generalized to existing GNN models. Specifically, we split the computation graph into two parts. We leave the private data (i.e., features, edges, and labels) related computations on data holders, and delegate the rest of computations to a semi-honest server. We also propose to apply differential privacy to prevent potential information leakage from the server. We conduct experiments on three benchmarks and the results demonstrate the effectiveness of VFGNN.

1 Introduction

Graph Neural Network (GNN) has gained increasing attentions from both academy and industry due to its ability to model high-dimensional feature information and high-order adjacent information on both homogeneous and heterogeneous graphs [Wu et al., 2019]. An important ingredient for high-performance GNN models is high-quality graph data including rich node features and complete adjacent information. However, in practice, such information could possibly be isolated by different data holders, which is the so-called data isolation problem. Such a data isolation problem presents a serious challenge for the development of Artificial Intelligence, which becomes a hot research topic recently.

Problem. Figure 1 shows a privacy-preserving node classification problem under vertically partitioned data setting. Here, we assume there are three data holders (A, B, and C) and they have four same nodes. The node features are vertically split, i.e., A has f1, f2, and f3, B has f4 and f5, and C has f6 and f7. Meanwhile, A, B, and C may have their own edges. For example, A has social relation between nodes while B and C have payment relation between nodes. We also assume A is the party who has the node labels. The problem is to build federated GNN models using the graph data of A, B, and C.

Related work. To date, many kinds of privacy-preserving machine learning models have been proposed, e.g., logistic regression [Chen et al., 2021], decision tree [Fang et al., 2021], and neural network [Wagh et al., 2019]. There are also several work on studying the privacy issues in GNN, e.g., graph publishing [Sajadmanesh and Gatica-Perez, 2020], GNN inference [He et al., 2020], and federated GNN when data are horizontally partitioned [Zheng et al., 2021; Wu et al., 2021]. Unlike previous privacy-preserving machine learning models that assume only samples (nodes) are held by different parties and they have no relationship, our task is more challenging because GNN relies on the relationships between samples, which are also private to data holders.

Naive solution. A direct way to build privacy-preserving GNN is employing advanced cryptographic algorithms, such
as homomorphic encryption (HE) and secure multi party computation (MPC) [Mohassel and Zhang, 2017]. Such a pure cryptographic way can provide high security guarantees, however, it suffers high computation and communication costs, which limits their efficiency [Osia et al., 2019].

Our solution. We propose VFGNN, a vertically federated GNN learning paradigm for privacy-preserving node classification task. Motivated by the existing work in split learning [Vepakomma et al., 2018; Osia et al., 2019; Gu et al., 2018], we split the computation graph of GNN into two parts for privacy and efficiency concern, i.e., the private data related computations carried out by data holders and non-private data related computations conducted by a semi-honest server. Specifically, data holders first apply MPC techniques to compute the initial layer of the GNN using private node feature information collaboratively, which acts as the feature extractor module, and then perform neighborhood aggregation using private edge information individually, similar as the existing GNNs [Velickovic et al., 2017], and finally get the local node embeddings. Next, we propose different combination strategies for a semi-honest server to combine local node embeddings from data holders and generate global node embeddings, based on which the server can conduct the successive non-private data related computations, e.g., the non-linear operations in deep network structures that are time-consuming for MPC techniques. Finally, the server returns the final hidden layer to the party who has labels to compute prediction and loss. Data holders and the server perform forward and back propagations to complete model training and prediction, during which the private data (i.e., features, edges, and labels) are always kept by data holders themselves. Moreover, we adopt differential privacy, on the exchanged information between server and data holders, to further protect potential information leakage from the server.

Contributions. We summarize our main contributions as:

• We propose a novel VFGNN learning paradigm, which not only can be generalized to most existing GNNs, but also enjoys good accuracy and efficiency.
• We propose different combination strategies for the server to combine local node embeddings from data holders.
• We evaluate our proposals on three real-world datasets, and the results demonstrate the effectiveness of VFGNN.

2 Preliminaries

2.1 Security Model

In this paper, we assume the adversary is honest-but-curious (semi-honest). That is, data holders and the server strictly follow the protocol, but they also use all intermediate computation results to infer as much information as possible. We also assume that the server does not collude with any data holders. This security setting is similar as most existing work [Mohassel and Zhang, 2017; Hardy et al., 2017].

2.2 Additive Secret Sharing

Additive Secret Sharing has two main procedures [Shamir, 1979]. To additively share \( \text{Shr}(\cdot) \) an \( \ell \)-bit value \( a \) for party \( i \in \mathcal{P} = \{1, \ldots, I\} \), party \( i \) generates \( \{a_j \in \mathbb{Z}_{2^\ell}, j \in \mathcal{P} \text{ and } j \neq i\} \) uniformly at random, sends \( a_j \) to party \( j \), and keeps \( a_i = a - \sum_j a_j \mod 2^\ell \). We use \( \langle a \rangle_i = a_i \) to denote the share of party \( i \). To reconstruct \( \text{Rec}(\cdot, \cdot) \) a shared value \( \langle a \rangle \), each party \( i \) sends \( \langle a \rangle_i \) to one who computes \( \sum_j a_i \mod 2^\ell \). For simplification, we denote additive sharing by \( \langle \cdot \rangle \). Addition in secret sharing can be done by participants locally. Multiplication in secret sharing usually relies on Beaver’s triplet technique [Beaver, 1991].

2.3 Differential Privacy

Definition 1. (Differential Privacy [Dwork et al., 2014]). A randomized algorithm \( \mathcal{M} \) that takes as input a dataset consisting of individuals is \((\epsilon, \delta)\)-differentially private (DP) if for any pair of neighbouring data \( x, y \) that differ in a single entry, and any event \( E \),

\[
P[\mathcal{M}(x) \in E] \leq \exp(\epsilon)P[\mathcal{M}(y) \in E] + \delta,
\]

and if \( \delta = 0 \), we say that \( \mathcal{M} \) is \( \epsilon \)-differentially private.

In [Dwork et al., 2014], the authors pointed out that the \( \ell_2 \)-sensitivity of a function \( f \) measures the magnitude by which a single individual’s data can change the function in the worst case.

Definition 2. (\( \ell_2 \)-sensitivity [Dwork et al., 2014]). Suppose \( x \) and \( y \) are neighbouring inputs that differ in one entry. The \( \ell_2 \)-sensitivity of a function \( f : \mathcal{D} \to \mathbb{R}^d \) is:

\[
\Delta_2 f = \max_{x, y \in \mathcal{D}, \|x - y\|_1 = 1} \|f(x) - f(y)\|_2.
\]

Definition 3. (The Gaussian Mechanism [Dwork et al., 2014]) Given a function \( f : \mathcal{D} \to \mathbb{R}^d \) over a dataset \( \mathcal{D} \), the Gaussian mechanism is defined as:

\[
\mathcal{M}_G(x, f(\cdot), \epsilon) = f(x) + (Y_1, \cdots, Y_k),
\]

where \( Y_i \) are i.i.d. random variables drawn from \( \mathcal{N}(0, \sigma^2 \Delta_2 f^2) \) and \( \sigma = \frac{\sqrt{2 \ln(1.25/\delta)}}{\epsilon} \).

Theorem 1. [Dwork et al., 2014] The Gaussian mechanism defined in Definition 3 preserves \((\epsilon, \delta)\)-DP for each publication step.

3 The Proposed Model

3.1 Overview of VFGNN

As described in Section 1, for the sake of privacy and efficiency, we design a vertically federated GNN (VFGNN) learning paradigm by splitting the computational graph of GNN into two parts. That is, we keep the private data related computations to data holders for privacy concern, and delegate the non-private data related computations to a semi-honest server for efficiency concern. In the context of GNN, the private data refers to node features, labels, and edges (node relations). To be specific, we divide the computational graph into the following three sub-Computational Graphs (CG), as is shown in Figure 2.

CG1: private feature and edge related computations. The first step of GNN is generating initial node embeddings using node’s private features, e.g., user features in social networks. In vertically data split setting, each data holder has partial
node features, as shown in Figure 1. We will present how data holders collaboratively learn initial node embeddings later. In the next step, data holders generate local node embeddings by aggregating multi-hop neighbors’ information using different aggregator functions.

**CG2: non-private data related computations.** We delegate non-private data related computations to a semi-honest server for efficiency concern. First, the server combines the local node embeddings from data holders with different COMBINE strategies, and obtains the global node embeddings. Next, the server can perform the successive computations using plaintext data. Note that this part has many non-linear computations such as max-pooling and activation functions, which are not cryptographically friendly and need to be approximated [Mohassel and Zhang, 2017; Hardy et al., 2017]. Delegating these plaintext computations to server will not only improve our model accuracy, but also significantly improve our model efficiency. After this, the server gets a final hidden layer (xL) and sends it back to the data holder who has label to calculate the prediction, where L is the total number of layers of the deep neural network.

**CG3: private label related computations.** The data holder who has label can compute prediction using the final hidden layer it receives from the server. For node classification task, the Softmax activation function is used for the output layer [Kipf and Welling, 2016], which is defined as \( \text{softmax}(z_c) = \frac{1}{\sum_c \exp(z_c)} \) with \( c \in C \) be the node class and \( Z = \sum_c \exp(z_c) \).

In the following subsections, we will describe three important components of VFGNN.

### 3.2 Generate Initial Node Embeddings

Initial node embeddings are generated by using node features. Under vertically partitioned data setting, each data holder has partial node features. There are two methods for data holders to generate initial node embeddings, i.e., individually and collaboratively, as shown in Figure 3.

The ‘individually’ method means that data holders generate initial node embeddings using their own node features, individually. For data holder \( i \in P \), this can be done by \( h^0_i = (x^i)^T \cdot W^i \), where \( x^i \) and \( W^i \) are node features and weight matrix of data holder \( i \). As the example in Figure 3 (a), \( A, B, \) and \( C \) generate their initial node embeddings using their own features separately. Although this method is simple and data holders do not need to communicate with each other, it cannot capture the relationship between features of data holders and thus causes information loss.

To solve the shortcoming of ‘individually’ method, we propose a ‘collaboratively’ method. It indicates that data holders generate initial node embeddings using their node features, collaboratively, and meanwhile keep their private features secure. Technically, this can be done by using cryptographic methods such as secret sharing and homomorphic encryption [Acar et al., 2018]. In this paper, we choose additive secret sharing due to its high efficiency.

### 3.3 Generate Local Node Embeddings

We generate local node embeddings by using multi-hop neighborhood aggregation on graphs, based on initial node embeddings. Note that, *neighborhood aggregation should be done by data holders separately*, rather than cooperatively, to protect the private edge information. This is because one may infer the neighborood information of \( v \) given the neighborood aggregation results of \( k \)-hop \( (h^k_i(i)) \) and \( k+1 \)-hop \( (h^{k+1}_i(i)) \), if neighborhood aggregation is done by data holders jointly. For \( \forall v \in V \) at each data holder, neighborhood aggregation is the same as the traditional GNN. Take GraphSAGE [Hamilton et al., 2017] for example, it introduces aggregator functions to update hidden embeddings by sampling and aggregating features from a node’s local neighborhood:

\[
\begin{align*}
\mathbf{h}^k_{N(v)} &\leftarrow \text{AGG}_k(\{\mathbf{h}^{k-1}_u, \forall u \in N(v)\}), \\
\mathbf{h}^k_v &\leftarrow (\mathbf{W}^k \cdot \text{CONCAT}(\mathbf{h}^{k-1}_u, \mathbf{h}^k_{N(v)})),
\end{align*}
\]

where we follow the same notations as GraphSAGE, and the aggregator functions AGG are of three types, i.e., Mean, LSTM, and Pooling. After it, data holders send local node embeddings to a semi-honest server for combination and further non-private data related computations.

### 3.4 Generate Global Node Embeddings

The server combines the local node embeddings from data holders and gets global node embeddings. The combination strategy (COMBINE) should be trainable and maintaining high representational capacity, and we design three of them.

**Concat.** The concat operator can fully preserve local node embeddings learnt from different data holders. That is, Line 14 in Algorithm 2 becomes

\[
\mathbf{h}^k \leftarrow \text{CONCAT}(\mathbf{h}^k_1, \mathbf{h}^k_2, \ldots, \mathbf{h}^k_I).
\]
Algorithm 1 Information publishing mechanisms of data holders to server using differential privacy

**Input:** Local information of data holders $x$, dimension of local information $d$, noise multiplier $\sigma$, clipping value $C$.

**Output:** Differentially private node embeddings.

1. Scale local information $\bar{x} = \min(1, C/||x||)x$;
2. Draw i.i.d. samples from $N(0, \sigma^2C^2)$, which forms a $d$-dimension noise vector $n$;
3. Gaussian Mechanism:
4. Add noise $\tilde{x} = x + n$;
5. James-Stein Estimator:
6. Compute James-Stein Estimator $\tilde{x}_{JS} = \left(1 - \frac{(d - 2)\sigma^2C^2}{||x||^2}\right)\bar{x}$;
7. return $\tilde{x}$ or $\tilde{x}_{JS}$.

Mean. The mean operator takes the elementwise mean of the vectors in $(\{h^K_i(i), \forall i \in \mathcal{P}\})$, assuming data holders contribute equally to the global node embeddings, i.e.,

$$h^K_i \leftarrow \text{MEAN}(h^K_i(1) \cup h^K_i(2) \cup ... \cup h^K_i(I)).$$

Regression. The above two strategies treat data holders equally. In reality, the local node embeddings from different data holder may contribute diversely to the global node embeddings. We propose a Regression strategy to handle this kind of situation. Let $\omega_i$ be the weight vector of local node embeddings from data holder $i \in \mathcal{P}$, then

$$h^K_i \leftarrow \omega_1 \odot h^K_i(1) + \omega_2 \odot h^K_i(2) + ... + \omega_I \odot h^K_i(I),$$

where $\odot$ is element-wise multiplication.

These different combination operators can utilize local node embeddings in diverse ways, and we will empirically study their effects on model performances in experiments.

3.5 Enhancing Privacy by Adopting DP

Data holders directly send the local information, e.g., local node embeddings during forward propagation and gradient update during back propagation, to the server may cause potential information leakage [Lyu et al., 2020], and we propose to apply differential privacy to further enhance privacy. In this section, we introduce two DP based data publishing mechanisms, to further enhance the privacy of our proposed VFGNN. Such that with a single entry modification in the local information of data holders, there is a large probability that the server cannot distinguish the difference before or after the modification. We present the two mechanisms, i.e., Gaussian Mechanism and James-Stein Estimator, in Algorithm 1. We have described Gaussian mechanism in Section 2.3, we present James-Stein Estimator as follows.

Theorem 2. (James-Stein Estimator and its adaptivity [Balle and Wang, 2018]). Suppose $d \geq 3$, substituting $w$ in $\tilde{x}_{\text{Bayes}}$ with its maximum likelihood estimate under $x \sim N(0, w^2I)$, $\tilde{x}|x \sim N(x, \sigma^2C^2I)$, and $\tilde{x}_{\text{Bayes}} = \text{argmin}_x ||\tilde{x} - x||^2$ produces James-Stein Estimator $\tilde{x}_{JS} = \left(1 - \frac{(d - 2)\sigma^2C^2}{||x||^2}\right)x$.

Moreover, it has an Mean Squared Error (MSE) of

$$E[||\tilde{x}_{JS} - x||^2] = d\sigma^2 \left(1 - \frac{(d - 2)\sigma^2C^2}{||x||^2}\right).$$

The MSE of Gaussian Mechanism $\tilde{x}$ to exact $x$ is $E[||\tilde{x} - x||^2] = d\sigma^2C^2$, while the MSE of James-Stein Estimator is reduced with a factor of $\left(1 - \frac{(d - 2)\sigma^2C^2}{w^2 + \sigma^2C^2}\right)$. Both methods preserve $(\epsilon, \delta)$-DP while James-Stein estimator shows reductions in MSE, thus improves utility. By the definition of Gaussian mechanism (Definition 3), we have the privacy loss for both information publishing mechanisms in Algorithm 1. By combining it with Moment Accountant (MA) [Abadi et al., 2016], we present the overall privacy for $T$ iterations.

Theorem 3. Suppose each iteration of Algorithm 1 is $(\epsilon, \delta)\text{-DP}$, there exist constants $c_1$ and $c_2$ so that given the sampling probability $q$ and the number of iterations $T$, and $\epsilon < c_1q\sqrt{T}$, Algorithm 1 over $T$ iteration is $(\epsilon', \delta')\text{-DP}$, with $\epsilon' = c_2q\sqrt{T\epsilon}$.

Proof. By Definition 3 and Theorem 1, to ensure one iteration $(\epsilon, \delta)\text{-DP}$, we set $\sigma = \sqrt{\frac{2\ln(1.25/\delta)}{\epsilon}}$. By Theorem 1 in [Abadi et al., 2016], with $\sigma = \sqrt{\frac{2\ln(1.25/\delta)}{\epsilon}}$ and the appropriate choice of $\epsilon, q, T$, such that $\epsilon < c_1q\sqrt{T\epsilon}$, the privacy loss over $T$ iterations is $\epsilon' = c_2q\sqrt{T\log(1/\delta)} = c_2q\sqrt{T\epsilon}$.

3.6 Putting Together

By combining CG1-CG3, we complete the forward propagation of VFGNN. To describe the procedures in details, without loss of generality, we take GraphSAGE [Hamilton et al., 2017] for example and present its forward propagation process in Algorithm 2. VFGNN can be learnt by gradient descent through minimizing the cross-entropy error over all labeled training examples. As can be seen, in VFGNN, both private data and model are hold by data holders themselves, thus data privacy can be better guaranteed.

4 Experiments

We conduct experiments to answer the following questions. Q1: whether VFGNN outperforms the GNN models that are trained on the isolated data. Q2: how does VFGNN behave comparing with the traditional insecure model trained on the plaintext mixed data. Q3: how does VFGNN perform comparing with the naïve solution in Section 1. Q4: are our proposed combination strategies effective to VFGNN. Q5: what is the effect of the number of data holders on VFGNN. Q6: what is the effect of differential privacy on VFGNN.

4.1 Experimental Setup

Datasets. We use four benchmark datasets, i.e., Cora, Pubmed, Citeseer [Sen et al., 2008], and arXiv [Hu et al., 2020]. We use exactly the same dataset partition of training, validation, and test following the prior work [Kipf and Welling, 2016; Hu et al., 2020]. Besides, in data isolated GNN setting, both node features and edges are hold by different parties. For all the experiments, we use five-fold cross validation and adopt average accuracy as the evaluation metric.

Comparison methods. We compare VFGNN with GraphSAGE models [Hamilton et al., 2017] that are trained using isolated data and mixed plaintext data to answer Q1 and Q2.
We also compare VFGNN with the naive solution described in Section 1 to answer Q3. To answer Q4, we vary the proportion of the data (features and edges) held by \(A\) and \(B\), and change VFGNN with different combination strategies. We vary the number of data holders in VFGNN to answer Q5, and vary the parameters of differential privacy to answer Q6. For all these models, we choose Mean operator as the aggregator function.

Parameter settings. For all the models, we use TanH as the active function of neighbor propagation, and Sigmoid as the active function of hidden layers. For the deep neural network on server, we set the dropout rate to 0.5 and network structure as \((d, d, |C|)\), where \(d \in \{32, 64, 128\}\) is the dimension of node embeddings and \(|C|\) the number of classes. We vary \(\epsilon \in \{1, 2, 4, 8, 16, 32, 64, \infty\}\), set \(\delta = 1/e^{-4}\) and the clip value \(C = 1\) to study the effects of differential privacy on our model. Since we have many comparison and ablation models, and they achieve the best performance with different parameters, we cannot report all the best parameters. Instead, we report the range of the best parameters. We vary the propagation depth \(K \in \{2, 3, 4, 5\}\), L2 regularization in \(10^{-2} - 10^{-4}\), and learning rate in \(10^{-2} - 10^{-3}\). We tune parameters based on the validate dataset and evaluate model performance on the test dataset.

4.2 Comparison Results and Analysis

To answer Q1–Q3, we assume there are two data holders (\(A\) and \(B\)) who have equal number of node features and edges, i.e., the proportion of data held by \(A\) and \(B\) is 5:5, and compare our models with GraphSAGEs that are trained on isolated data individually and on mixed plaintext data. We also set \(\epsilon = \infty\) during comparison and will study its effects later. We summarize the results in Table 2, where VFGNN_C, VFGNN_M and VFGNN_R denote VFGNN with Concat, Mean, and Regression combination strategies.

**Result1:** answer to Q1. We first compare VFGNNs with the GraphSAGEs that are trained on isolated data individually and on mixed plaintext data. VFGNNs have comparable performance with GraphSAGEs on all the three datasets. Take Cora for example, our model significantly outperforms GraphSAGE by as high as 28.10% and 51.64%, in terms of accuracy.

**Analysis of Result1.** The reason of result1 is straightforward. GraphSAGE has only partial feature and edge information held by \(A\) and \(B\). In contrast, VFGNNs provide a solution for \(A\) and \(B\) to jointly train GNNs without compromising their own data. By doing this, VFGNNs can use the information from the data of both \(A\) and \(B\) simultaneously, and therefore achieve better performance.

**Result2:** answer to Q2. We then compare VFGNNs with GraphSAGE that is trained on the mixed plaintext data, i.e., GraphSAGE_E. We can see from Table 2 that VFGNNs have comparable performance with GraphSAGE_E, e.g., 0.8090 vs. 0.8150 on Cora dataset and 0.6950 vs. 0.7001 on Citeseer dataset.

**Analysis of Result2.** It is easy to explain why our proposal has comparable performance with the model that are trained

---

### Table 1: Dataset statistics.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>#Node</th>
<th>#Edge</th>
<th>#Features</th>
<th>#Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cora</td>
<td>2,708</td>
<td>5,429</td>
<td>1,433</td>
<td>7</td>
</tr>
<tr>
<td>Pubmed</td>
<td>19,717</td>
<td>44,338</td>
<td>500</td>
<td>3</td>
</tr>
<tr>
<td>Citeseer</td>
<td>3,327</td>
<td>4,732</td>
<td>3,703</td>
<td>6</td>
</tr>
<tr>
<td>arXiv</td>
<td>169,343</td>
<td>2,315,989</td>
<td>128</td>
<td>40</td>
</tr>
</tbody>
</table>

### Table 2: Comparison results on three datasets (Q1 and Q2).

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Cora</th>
<th>Pubmed</th>
<th>Citeseer</th>
<th>arXiv</th>
</tr>
</thead>
<tbody>
<tr>
<td>GraphSAGE_A</td>
<td>0.611</td>
<td>0.672</td>
<td>0.541</td>
<td>0.471</td>
</tr>
<tr>
<td>GraphSAGE_B</td>
<td>0.606</td>
<td>0.703</td>
<td>0.457</td>
<td>0.482</td>
</tr>
<tr>
<td>VFGNN_C</td>
<td>0.790</td>
<td>0.774</td>
<td>0.685</td>
<td>0.513</td>
</tr>
<tr>
<td>VFGNN_M</td>
<td>0.809</td>
<td>0.781</td>
<td>0.695</td>
<td>0.522</td>
</tr>
<tr>
<td>VFGNN_R</td>
<td>0.802</td>
<td>0.782</td>
<td>0.693</td>
<td>0.518</td>
</tr>
<tr>
<td>GraphSAGE_A+B</td>
<td>0.815</td>
<td>0.791</td>
<td>0.700</td>
<td>0.529</td>
</tr>
</tbody>
</table>

---

**Algorithm 2** Privacy-preserving GraphSAGE for node label prediction (forward propagation)

**Input:** Data holder \(\forall i \in \mathcal{P}\); Graph \(G(V, E)\) and node features \(\{x_i, \forall v \in V\}\); depth \(K\); aggregator functions \(\text{AGG}_k, \forall k \in \{1, \ldots, K\}\); weight matrices \(W_k, \forall k \in \{1, \ldots, K\}\); max layer \(L\); weight matrices \(W_{l}, \forall l \in \{0, \ldots, L\}\); non-linearity \(\sigma\); neighbor functions \(N_i: v \rightarrow 2^V\); node labels on data holder \(p \in \mathcal{P}\) and \(c \in C\)

**Output:** Node label predictions \(\{\hat{y}_{vc}, \forall v \in V, \forall c \in C\}\)

1. **# CG1:** private feature and edge related computations
2. **Data holders:** jointly calculate initial node embeddings \(h_0(i) \leftarrow x_i, \forall i \in \mathcal{P}, \forall v \in V\)
3. for \(i \in \mathcal{P}\) in parallel do
4. for \(k = 1\) to \(K\) do
5. for \(v \in V\) do
6. **Data holder:** calculates \(h^K_{N(v)}(i) \leftarrow \text{AGG}_k(h^{k-1}_u(i), \forall u \in N^i(v))\)
7. end for
8. **Data holder:** calculates \(h^K(i) \leftarrow \sigma(W^K \cdot \text{CONCAT}(h^{k-1}_u(i), h^K_{N(v)}(i)))\)
9. end for
10. **Data holder:** calculates local node embeddings \(h^K(i) \leftarrow h^K(i)/||h^K(i)||_2, \forall v \in V\) and sends (publishes) it to server using differential privacy
11. end for
12. **# CG2:** non-private data related computations
13. for \(v \in V\) do
14. **Server:** combines the local node embeddings from data holders \(h^K = \text{COMBINE}(\{h^K(i), \forall i \in \mathcal{P}\})\)
15. **Server:** forward propagation based on the global node embeddings \(z_L = \sigma(W_{L-1} \cdot \sigma(...\sigma(W_0 \cdot h^K)))\)
16. **Server:** sends \(z_L\) to data holder \(p\)
17. end for
18. **# CG3:** private label related computations
19. **Data holder:** \(p\): makes prediction by \(\hat{y}_{vc} \leftarrow \text{softmax}(W_L \cdot z_L), \forall v \in V, \forall c \in C\)
We propose VFGNN, a vertically federated GNN learning paradigm for privacy-preserving node classification task. We finish this by splitting the computation graph of GNN. We leave the private data related computations on data holders and delegate the rest computations to a server. Experiments on real world datasets demonstrate that our model significantly outperforms the GNNs by using the isolated data and has comparable performance with the traditional GNN by using the mixed plaintext data insecurely.

5 Conclusion

We propose VFGNN, a vertically federated GNN learning paradigm for privacy-preserving node classification task. We finish this by splitting the computation graph of GNN. We leave the private data related computations on data holders and delegate the rest computations to a server. Experiments on real world datasets demonstrate that our model significantly outperforms the GNNs by using the isolated data and has comparable performance with the traditional GNN by using the mixed plaintext data insecurely.

<table>
<thead>
<tr>
<th>Model</th>
<th>VFGNN_C</th>
<th>VFGNN_M</th>
<th>VFGNN_R</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prop.=9:1</td>
<td>0.809</td>
<td>0.805</td>
<td>0.809</td>
</tr>
<tr>
<td>Prop.=8:2</td>
<td>0.802</td>
<td>0.796</td>
<td>0.807</td>
</tr>
<tr>
<td>Prop.=7:3</td>
<td>0.793</td>
<td>0.793</td>
<td>0.803</td>
</tr>
</tbody>
</table>

Table 3: Comparison of combination operators on Cora by varying the proportion of data hold by $A$ and $B$ (Q4).

<table>
<thead>
<tr>
<th>No. of DH</th>
<th>VFGNN_C</th>
<th>VFGNN_M</th>
<th>VFGNN_R</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.790</td>
<td>0.809</td>
<td>0.802</td>
</tr>
<tr>
<td>3</td>
<td>0.749</td>
<td>0.774</td>
<td>0.760</td>
</tr>
<tr>
<td>4</td>
<td>0.712</td>
<td>0.733</td>
<td>0.722</td>
</tr>
</tbody>
</table>

Table 4: Comparison results on Cora by varying the number of data holders (Q5).

on the mixed plaintext data. First, we propose a secret sharing based protocol for $A$ and $B$ to generate the initial node embeddings from their node features, which are the same as those generated by using mixed plaintext features. Second, although $A$ and $B$ generate local node embeddings by using their own edge data to do neighbor aggregation separately (for security concern), we propose different combination strategies to combine their local node embeddings. Eventually, the edge information from both $A$ and $B$ is used for training the classification model. Therefore, VFGNN achieves comparable performance with GraphSAGE$_{A+B}$.

Result3: answer to Q3. In VFGNN, we delegate the non-private data related computations to server. One would be curious about what if these computations are also performed by data holders using existing secure neural network protocols, i.e., SecureML [Mohassel and Zhang, 2017]. To answer this question, we compare VFGNN with the secure GNN model that is implemented using SecureML, which we call SecureGNN, where we use 3-degree Taylor expansion to approximate TanH and Sigmoid. The accuracy and running time per epoch (in seconds) of VFGNN vs. SecureGNN on Pubmed are 0.8090 vs. 0.7970 and 18.65 vs. 166.81, respectively, where we use local area network.

Analysis of Result3. From the above comparison results, we find that our proposed VFGNN learning paradigm not only achieves better accuracy, but also has much better efficiency. This is because the non-private data related computations involve many non-linear functions that are not cryptographically friendly, which have to be approximately calculated using time-consuming MPC techniques in SecureML.

4.3 Ablation Study

We now study the effects of different combination operators and different number of data holders on VFGNN.

Result4: answer to Q4. Different combination operators can utilize local node embeddings in diverse ways and make our proposed VFGNN adaptable to different scenarios, we study this by varying the proportion (Prop.) of data (node features and edges) hold by $A$ and $B$ in {9: 1, 8: 2, 7: 3}. The results on Cora dataset are shown in Table 3.

Analysis of Result4. From Table 3, we find that with the proportion of data hold by $A$ and $B$ being even, i.e., from {9: 1} to {7: 3}, the performances of most strategies tend to decrease. This is because the neighbor aggregation is done by data holders individually, and with a bigger proportion of data hold by a single holder, it is easier for this party to generate better local node embeddings. Moreover, we also find that Mean operator works well when data are evenly split, and Regression operator is good at handling the situations where data holders have different quality of data, since it treats the local node embeddings from each data holder differently, and assigns weights to them intelligently.

Result5: answer to Q5. We vary the number of data holders in {2, 3, 4} and study the performance of VFGNN. We report the results in Table 4, where we use the Cora dataset and assume data holders have even feature and edge data.

Analysis of Result5. From Table 4, we find that, as the number of data holders increases, the accuracy of all the models decreases. This is because the neighborhood aggregation in VFGNN is done by each holder individually for privacy concern, and each data holder will have less edge data when there are more data holders, since they split the original edge information evenly. Therefore, when more participants are involved, more information will be lost during the neighborhood aggregation procedure.

Result6: answer to Q6. We present the privacy loss of each iteration in Table 5 and the overall privacy in Theorem 3. We vary $\epsilon$ and set $\delta = 1e^{-4}$ to study the effects of DP on VFGNN. We report the results in Table 5, where we use Cora dataset, use MEAN as the combination operator, and assume data holders have even feature and edge data.

Analysis of Result6. From Table 5, we can see that the accuracy of VFGNN increases with $\epsilon$. In other words, there is a trade-off between accuracy and privacy. The smaller $\epsilon$, the more noise will be added into the local node embeddings, which causes stronger privacy guarantee but lower accuracy. We also find James-Stein estimator consistently works better than Gaussian mechanism, since it can reduce MSE, as we have analyzed in Section 3.5.

5 Conclusion

We propose VFGNN, a vertically federated GNN learning paradigm for privacy-preserving node classification task. We finish this by splitting the computation graph of GNN. We leave the private data related computations on data holders and delegate the rest computations to a server. Experiments on real world datasets demonstrate that our model significantly outperforms the GNNs by using the isolated data and has comparable performance with the traditional GNN by using the mixed plaintext data insecurely.
Acknowledgements
This work was supported in part by the National Natural Science Foundation of China (No. 62172362) and “Leading Goose” R&D Program of Zhejiang (No. 2022C01126).

References


