Federated Learning: Collaborative train a machine learning model without sharing/revealing training data introduced in [2]

Vertical FL
Parties have different features
Only one party has label
Together they form the complete feature set
Privacy or regulatory constraints

Overview of FedV

Existing HB-based Solution

Federated Learning

Experimental Evaluation: FedV reduces in average
- 10-20% in training and
- 60-90% in data transfer

BACKGROUND

Suppose participants A, B (B owns labels) in VFL - target loss function is mean squared loss

Gradient Descent in Vertical FL

Gradient Descent:
\[ E_D(w) = 1/n \sum_{x \in D} (f(x; w) - y)^2 \]
\[ E_D(w) = -2/n \sum_{x \in D} (f(x; w) - y) \cdot \nabla E_D(w) \]
\[ \Delta w = -(1/n) \nabla E_D(w) \]

Inner-Product Functional Encryption Schemes

Allows a decryptor to compute \( x \cdot y = \sum \alpha \beta \cdot x \beta \) over ciphertext \( E_p(x) \) of \( x \) without learning \( x \)

NOTE: \( x, x_1, \ldots, x_N \) is a vector, how is \( x \) composed?

Single-Input FE \( \mathcal{F}_1 \)
All elements in \( x \) are from source \( P_i \), i.e., all \( x_i \) are from source \( P_i \)
- \( P_i \) has a public key \( \mathcal{K}_i \)
- \( P_i \) encrypts the entire vector \( x \)

Multi-Input FE \( \mathcal{F}_k \)
Elements in \( x \) are from multiple sources \( P_i, \ldots, P_k \), i.e., \( x_i \) is just from source \( P_i \)
\( C = (E_{\mathcal{K}_i}(x_i), \ldots, E_{\mathcal{K}_k}(x_k)) \)
- Each source has its own secret key, i.e., \( P_i \) has a secret key \( \mathcal{K}_i \)
- Each source encrypts its data, i.e., \( P_i \) encrypts the element \( x_i : E_{\mathcal{K}_i}(x_i) \)

EXPERIMENTAL EVALUATION

Comparable model accuracy, training time reduced by 10% to 70%
Data transfer reduced by 80% to 90%
Work well on large size of dataset

Comparison of Communication Topology – FedV and SOTA

<table>
<thead>
<tr>
<th>Feature</th>
<th>FedV</th>
<th>FedV-SCerG</th>
<th>SOTA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Work: Additive HE Approach for SGD</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>