FEEL: A Federated Edge Learning System for Efficient and Privacy-Preserving Mobile Healthcare

Yeting Guo, Zhiping Cai, Nong Xiao: National University of Defense Technology
Fang Liu: Sun Yat-Sen University
Li Chen: University of Louisiana at Lafayette
AI enables smart healthcare

The scale of smart medical market is rapidly growing.

Drug Research

Diagnosis of Disease

Chronic disease prediction
Challenge 1: Medical records face serious security breach

2,550 data breaches have compromised over **189 million healthcare records** in the last decade.
(Source: HIPAA Journal)

The average cost of a data breach in the healthcare industry is **$6.45 million**. (Source: IBM)

46% of healthcare organizations have been damaged by **insider threats**.
(Source: 2019 Verizon Insider Threat Report)

168 hacking incidents in the first half of 2019 has led to **31 million breached records**.
(Source: Protenus Breach Barometer)
Challenge 2: Mobile medical devices are resource-limited

MOTO 360 smartwatch: Memory 512MB, Storage 4GB, 320mAh battery

Huawei GT 2e smartwatch: Memory 16MB, Storage 4GB, 455mAh battery

As neural network training is extremely computation-intensive, it easily drains the battery and starves the normal operations of the device. Training on mobile wearables is inefficient.
What makes a good mobile healthcare system?

- High accuracy
- Efficiency
- Privacy preservation
Contributions

1. Efficient health monitoring and model training
2. Accurate diagnosis without raw data leakage
3. Study on privacy and performance
Contributions

1. Efficient health monitoring and model training
2. Accurate diagnosis without raw data leakage
3. Study on privacy and performance
Edge-based efficient medical model training and health monitoring

Procedure Server
- download $W_{center}$
- $W_{server} \leftarrow W_{center}$
- while $i$ do
  - receive $O_k'$ and $L_j$ from the mobile device
  - $W_{server} \leftarrow W_{server} - \eta \cdot \nabla \text{Loss}(W_{server})$
  - send $\nabla \text{Loss}(O_k')$ to the device

Procedure Client
- initialize $W_{client}$
- divide $Data$ into $l$ batches $\{D_1, D_2, \cdots, D_l\}$
- for each epoch $i \in [1, \text{Epochs}]$ do
  - for each batch $D_j \in Data$ do
    - $O_k \leftarrow \text{Output}(D_j, W_{client})$
    - $O_k' \leftarrow D_{p_1}(O_k, D_j, W_{client})$
    - send $O_k'$ and $L_j$ to the hospital private server
    - receive $\nabla \text{Loss}(O_k')$ from the server
    - $W_{client} \leftarrow W_{client} - \eta \cdot \nabla \text{Loss}(O_k') \cdot \nabla \text{Loss}(W_{client})$
Setup -- Experiment Platform

<table>
<thead>
<tr>
<th>Simulation Node</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Devices</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>8* Snapdragon 660 @ 2.2GHZ</td>
</tr>
<tr>
<td>Memory</td>
<td>4GB</td>
</tr>
<tr>
<td>System</td>
<td>Android 7.1</td>
</tr>
<tr>
<td><strong>Hospital Servers</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>4* Intel(R) Core(TM) i5-4590 CPU @ 3.30GHZ</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
</tr>
<tr>
<td>System</td>
<td>Windows 10</td>
</tr>
<tr>
<td><strong>Cloud Center</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>20*Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>62GB</td>
</tr>
<tr>
<td>System</td>
<td>Ubuntu 16.04</td>
</tr>
</tbody>
</table>
Setup -- Dataset and Training Models

Dataset

We leverage breast cancer data as the private medical data set, which contains 497 training samples and 151 testing samples

Training Model

![Diagram of the training model]

Our loss function is binary-cross-entropy, and compilation environment is Keras

Results -- Resource Consumption

Traditional learning paradigm without efficiency consideration

Offloading total model to edge without privacy consideration

Our best practice
1. Efficient health monitoring and model training

2. Accurate diagnosis without raw data leakage

3. Study on privacy and performance
Privacy-preserving medical model aggregation

```
1. Initialize $W_{\text{center}}$
2. For each round $t = 1, 2, \ldots$ do
   3. $Z_t \leftarrow$ random subset of $M$ hospitals
   4. $\Delta W \leftarrow \emptyset$
   5. For each hospital $m \in Z_t$ in parallel do
      6. Send $W_{\text{center}}$ to $m$
      7. $m$ obtains $W_{\text{server}}^m$ via collaboration with mobile devices
      8. Receive $W_{\text{server}}^m$ from $m$
      9. $W_{\text{diff}}^m \leftarrow W_{\text{server}}^m - W_{\text{center}}$
     10. $\Delta W \leftarrow \Delta W \cup W_{\text{diff}}^m$
     11. $\Delta W' \leftarrow D_{p,2}(\Delta W)$
     12. $W_{\text{center}} \leftarrow W_{\text{center}} + \frac{1}{|Z_t|} \Delta W'$

Procedure Server
1. Download $W_{\text{center}}$
2. $W_{\text{server}} \leftarrow W_{\text{center}}$
3. While 1 do
   4. Receive $O_k'$ and $L_j$ from the mobile device
   5. $W_{\text{server}} \leftarrow W_{\text{server}} - \eta \cdot \nabla \text{Loss}(W_{\text{server}})$
   6. Send $\nabla \text{Loss}(O_k')$ to the device
```
Setup -- Dataset and Distribution

Dataset
We leverage breast cancer data [1] as the private medical data set, which contains 497 training samples and 151 testing samples.

Distribution
We distribute these training samples among 100 hospitals. Considering that the user data are not independent and identically distributed in multiple hospitals, we distribute these samples with following existing works [2].

Table 4: Distribution of training samples.

<table>
<thead>
<tr>
<th>Value</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>112</td>
<td>23</td>
<td>72</td>
<td>58</td>
<td>100</td>
<td>24</td>
<td>16</td>
<td>33</td>
<td>10</td>
<td>49</td>
</tr>
</tbody>
</table>


Results -- Diagnosis Performance

Federated Learning
(Near-Optimal performance without raw data leakage)

Centralized Learning
(Best performance but no privacy protection)

Stand-alone Learning
(Strong privacy protection but poor performance)

(a) F-Measure  
(b) Accuracy

Federated learning (Stable)

(a) F-Measure  
(b) Accuracy

Stand-alone learning (Fluctuate)
Contributions

1. Efficient health monitoring and model training

2. Accurate diagnosis without raw data leakage

3. Study on privacy and performance
Privacy-preserving differential privacy scheme
The performance gradually decreases with the increase of noise level. Considering both privacy and performance, we select $\sigma_1$ and $\sigma_2$ as 0.5 and 2.25, respectively.
Conclusion

Problem:
Address the \textit{inefficient and insecure} scheme in mobile medical data training.

Key idea: \textbf{FEderated Edge Learning (FEEL) system}

Evaluation:
FEEL reduces the mobile devices' \textit{resource occupation} (CPU time, memory, energy et al.) and \textit{performs near optimal with privacy protection}. 
Thank You!

guoyeting13@nudt.edu.cn

FEEL: A Federated Edge Learning System for Efficient and Privacy-Preserving Mobile Healthcare

Yeting Guo, Fang Liu, Zhiping Cai, Li Chen, Nong Xiao