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

Yeting Guo, Zhiping Cai, Nong Xiao: National University of Defense Technology

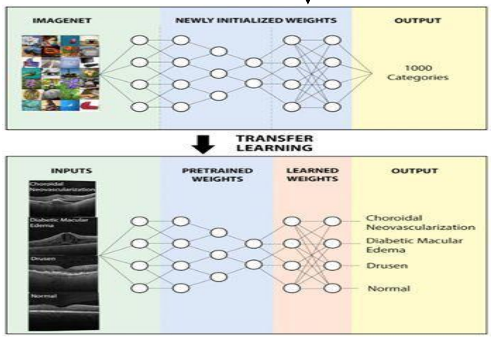
Fang Liu: Sun Yat-Sen University

Li Chen: University of Louisiana at Lafayette

AI enables smart healthcare

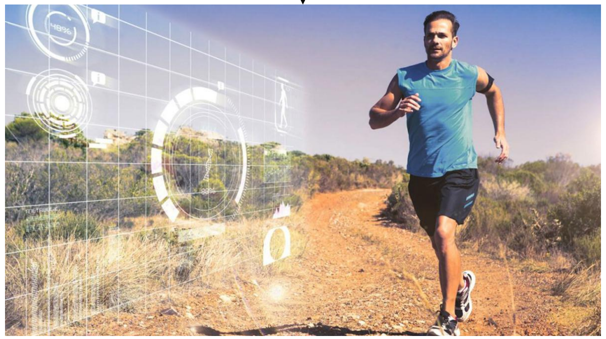
The scale of
smart medical market
is rapidly growing.

Drug Research



Diagnosis of Disease

...



Chronic disease prediction

Challenge 1: Medical records face **serious security breach**

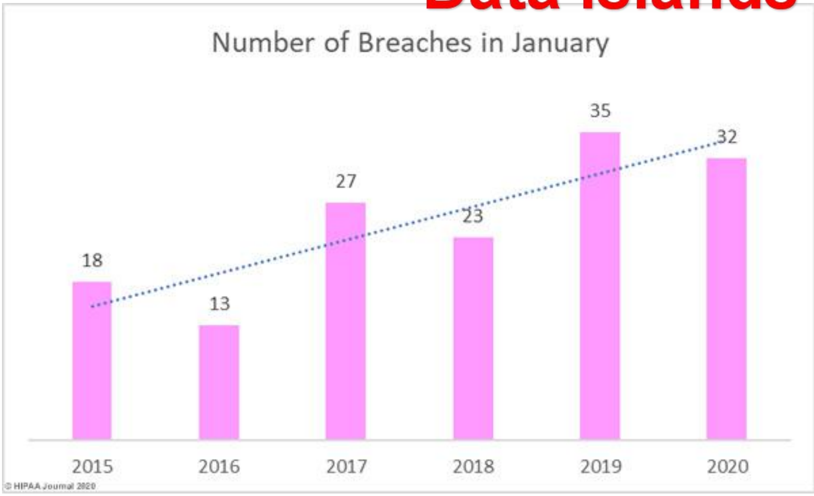
2,550 data breaches have compromised over **189 million healthcare records** in the last decade.
(Source: HIPAA Journal)

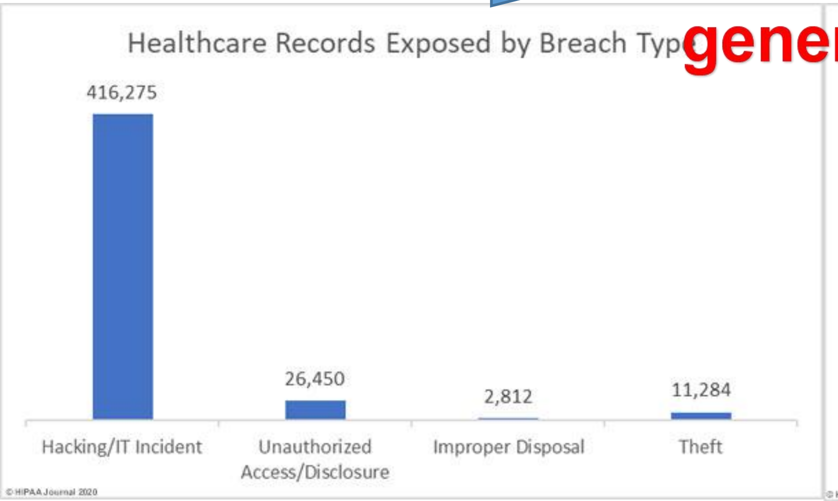
The average cost of a data breach in the healthcare industry is **$6.45 million.** (Source: IBM)

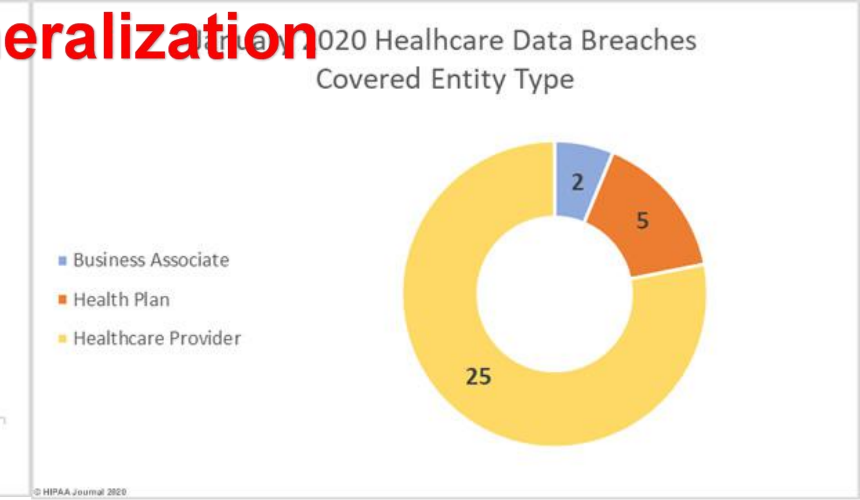
46% of healthcare organizations have been damaged by **insider threats**.
(Source: 2019 Verizon Insider Threat Report)

168 hacking incidents in the first half of 2019 has led to **31 million breached records**.
(Source: Protenus Breach Barometer)

Data Islands → **Models with low quality and poor generalization**







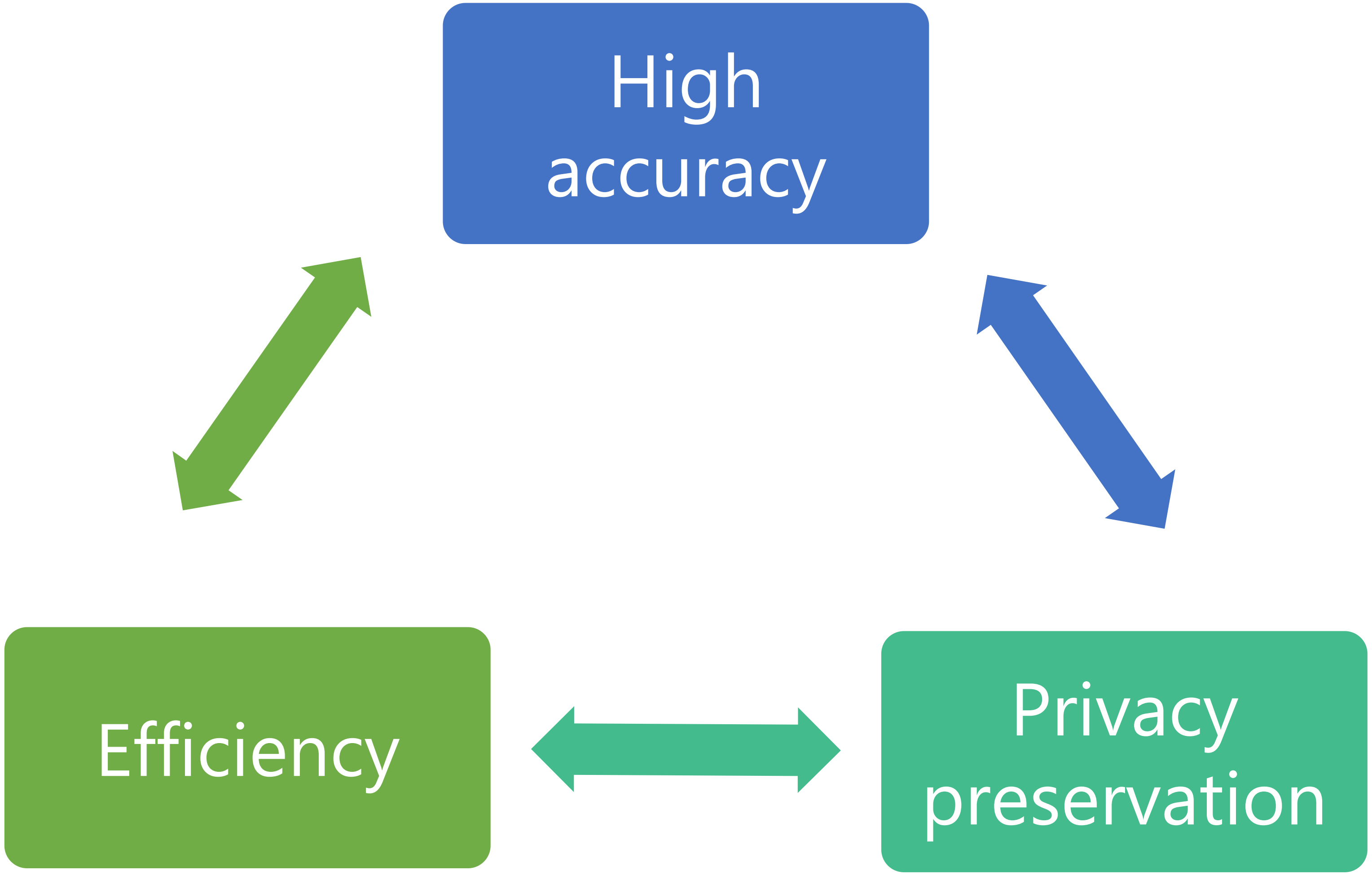
Challenge 2: Mobile medical devices are **resource-limited**

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?

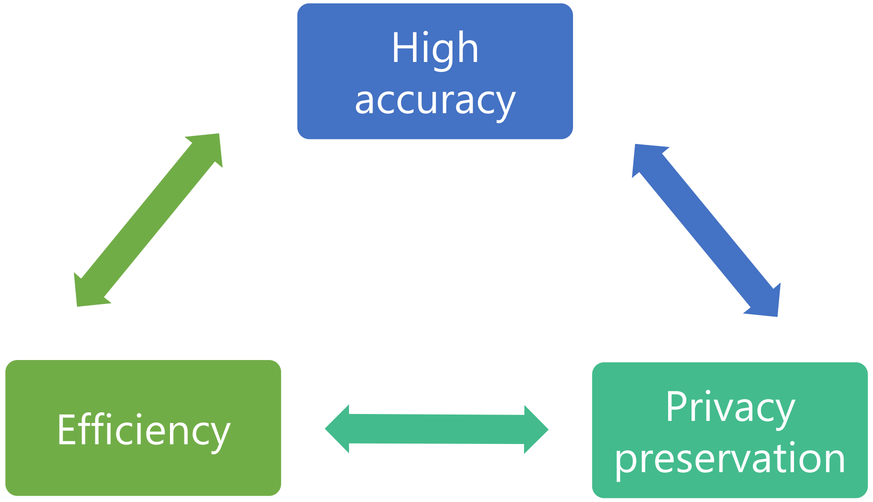


Contributions

1. Efficient health monitoring and model training

2. Accurate diagnosis without raw data leakage

3. Study on privacy and performance

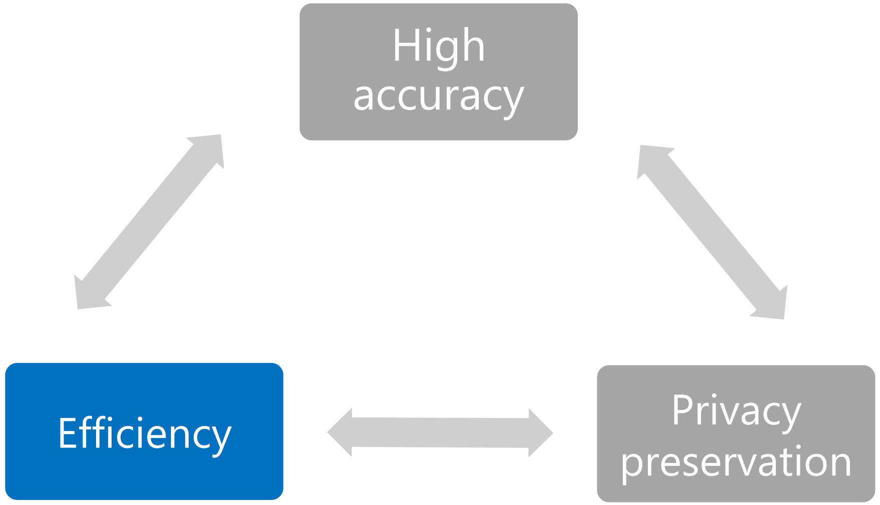


Contributions

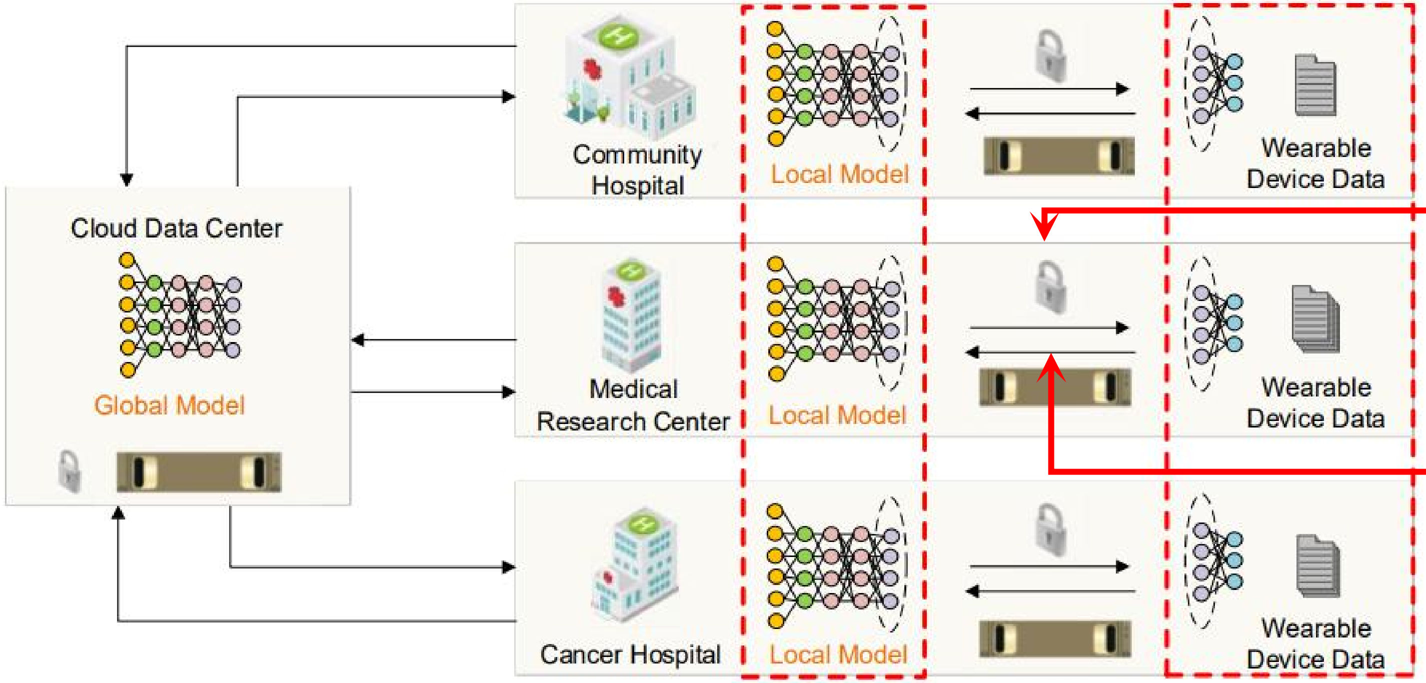
1. **Efficient health monitoring and model training**

2. **Accurate diagnosis without raw data leakage**

3. **Study on privacy and performance**



Edge-based efficient medical model training and health monitoring



noised output of the middel layers
data labels

gradient of loss to noised output

Procedure Server
- download W_{center}
- $W_{server} \leftarrow W_{center}$
- **while** *1* **do**
  - receive $O_k^{'}$ and L_j from the mobile device
  - $W_{server} \leftarrow W_{server} - \eta \cdot \nabla Loss(W_{server})$
  - send $\nabla Loss(O_k^{'})$ to the device

$O_k^{'}, L_j$

$\nabla Loss(O_k^{'})$

Procedure Client
- initialize W_{client}
- divide *Data* into *l* batches $\{D_1, D_2, \cdots D_l\}$
- **for** *each epoch* $i \in [1, Epochs]$ **do**
  - **for** *each batch* $D_j \in Data$ **do**
    - $O_k \leftarrow Output(D_j, W_{client})$
    - $O_k^{'} \leftarrow Dp\_1(O_k, D_j, W_{client})$
    - send $O_k^{'}$ and L_j to the hospital private server
    - receive $\nabla Loss(O_k^{'})$ from the server
    - $W_{client} \leftarrow W_{client} - \eta \cdot \nabla Loss(O_k^{'}) \cdot \nabla O_k^{'}(W_{client})$

Setup -- Experiment Platform

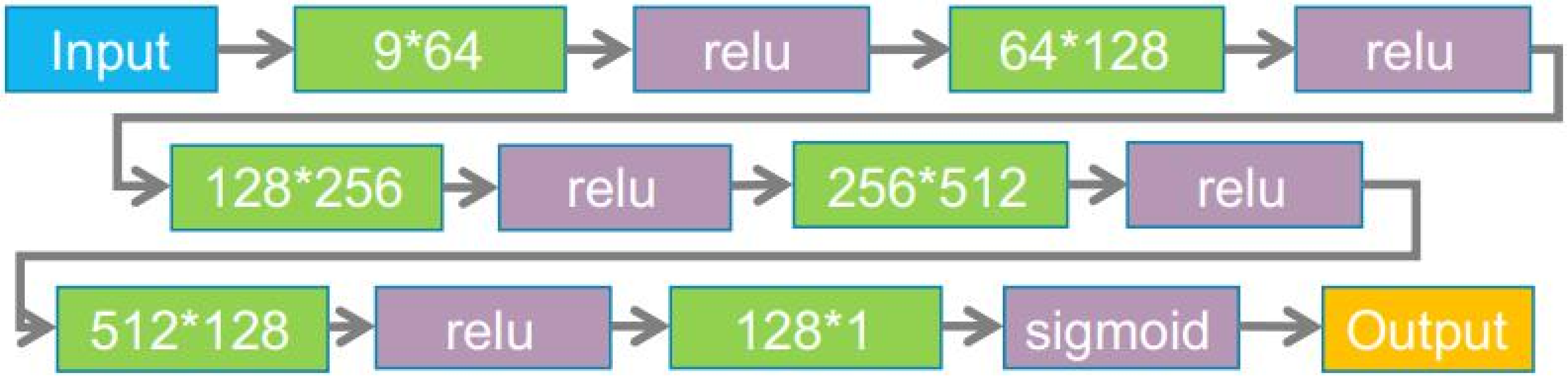
Simulation Node		Configuration
Mobile Devices	CPU	8* Snapdragon 660 @ 2.2GHZ
	Memory	4GB
	System	Android 7.1
Hospital Servers	CPU	4* Intel(R) Core(TM) i5-4590 CPU @ 3.30GHZ
	Memory	8GB
	System	Windows 10
Cloud Center	CPU	20*Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz
	Memory	62GB
	System	Ubuntu 16.04

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

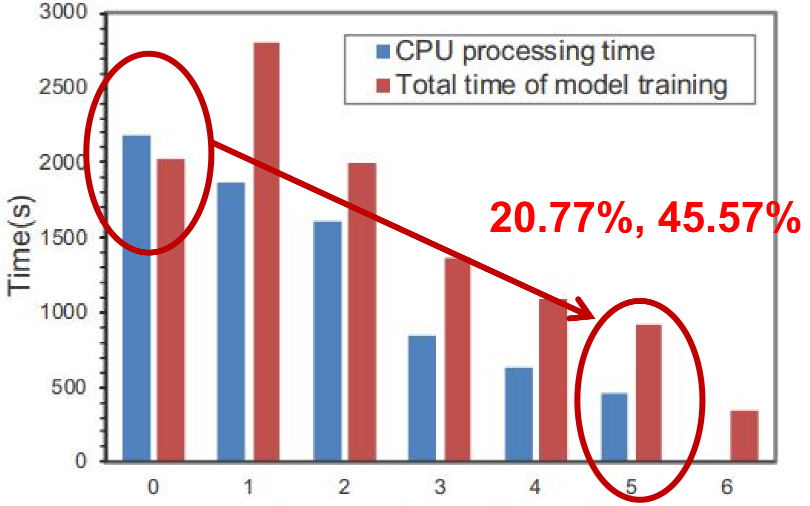
Training Model



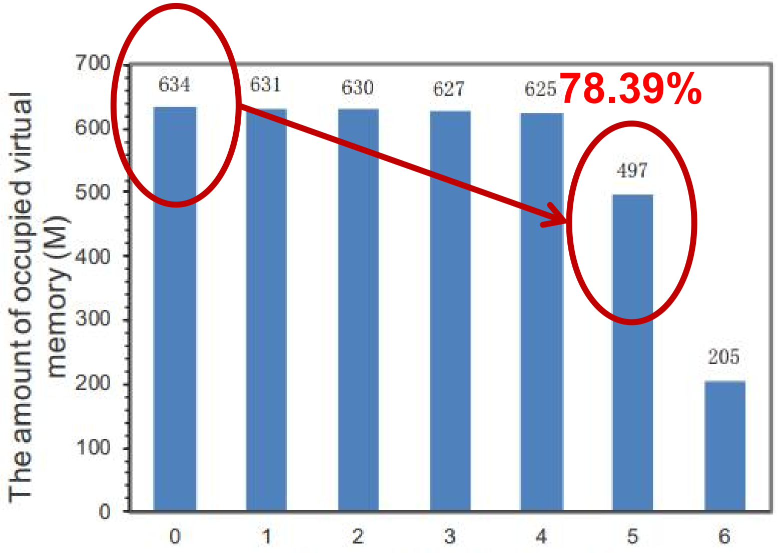
Our loss function is binary-cross-entropy, and compilation environment is Keras

[1] Olvi L Mangasarian and William H Wolberg. 1990. Cancer diagnosis via linear programming. Technical Report. University of Wisconsin-Madison Department of Computer Sciences. https://archive.ics.uci.edu/ml/machine-learning-databases/ breast- cancer- wisconsin/

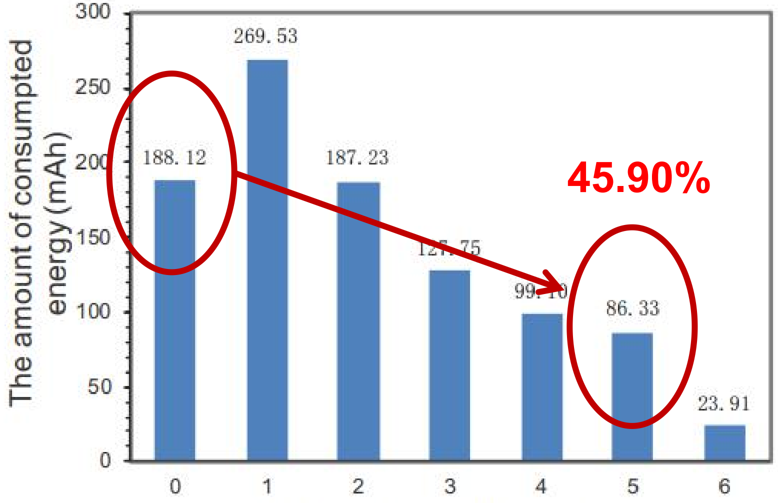
Results -- Resource Consumption



(a) Time Consumption



(b) Memory Consumption



(c) Energy Consumption.

Traditional learning paradigm without efficiency consideration

Offloading total model to edge without privacy consideration

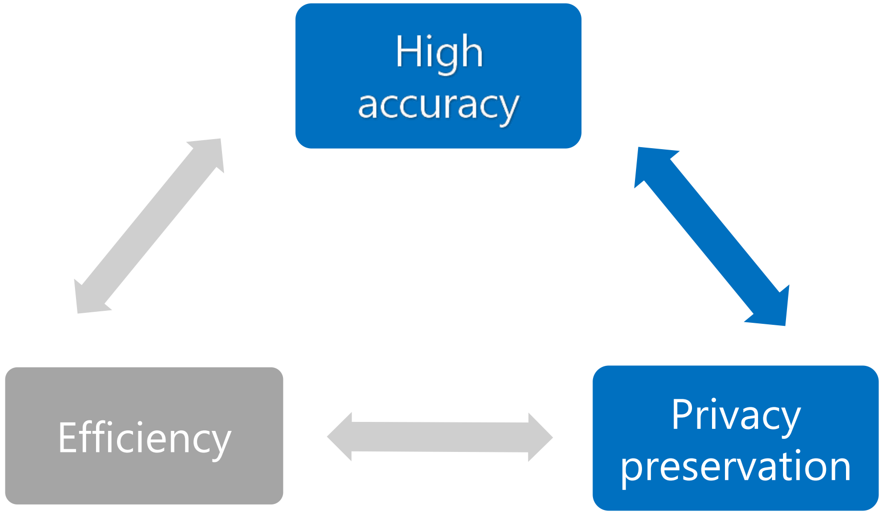
Our best practice

Contributions

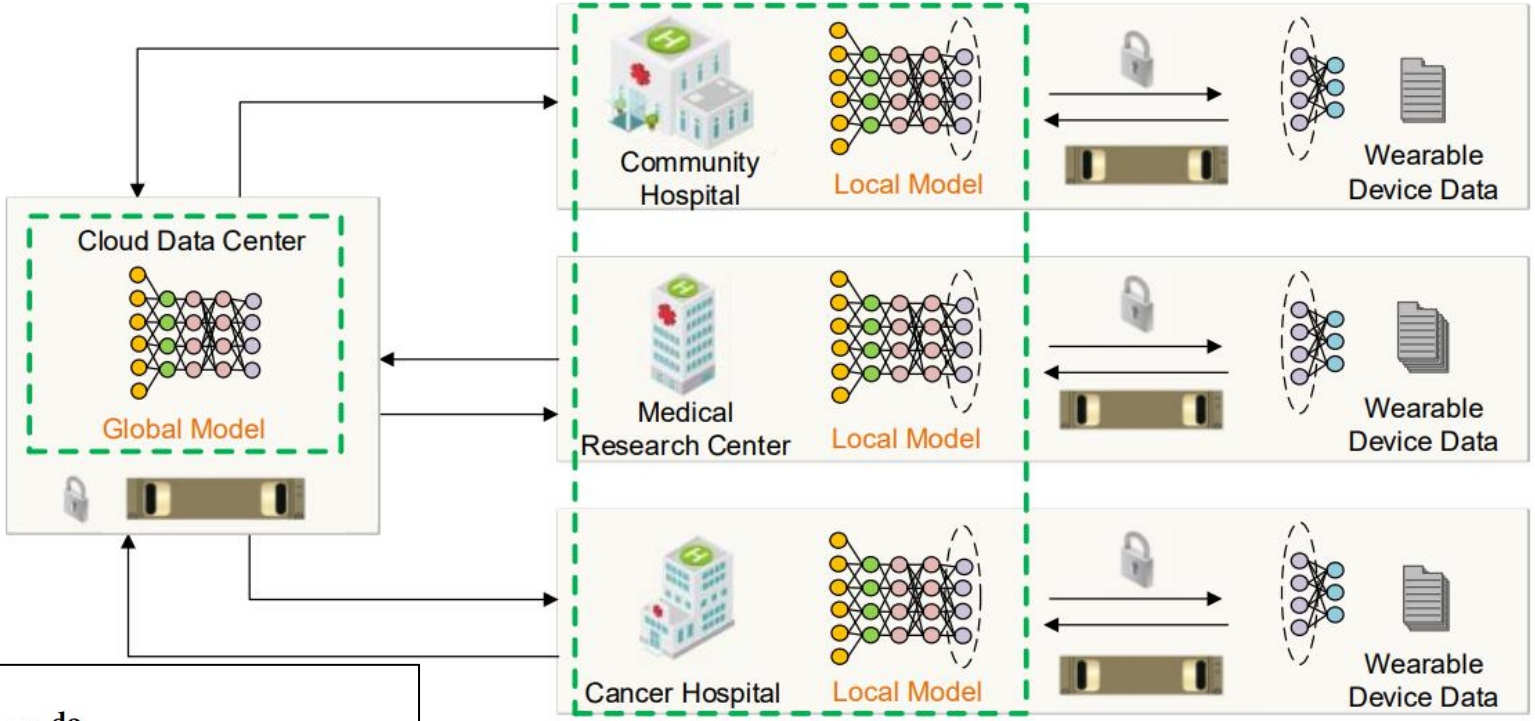
1. Efficient health monitoring and model training

2. Accurate diagnosis without raw data leakage

3. Study on privacy and performance



Privacy-preserving medical model aggregation



initialize W_{center}
for *each round* $t = 1, 2, \cdots$ **do**
  $Z_t \leftarrow$ random subset of M hospitals
  $\Delta W \leftarrow \oslash$
  for *each hospital* $m \in Z_t$ *in parallel* **do**
    send W_{center} to m
    m obtains W^m_{server} via collaboration with mobile devices
    receive W^m_{server} from m
    $W^m_{diff} \leftarrow W^m_{server} - W_{center}$
    $\Delta W \leftarrow \Delta W \cup W^m_{diff}$
  $\Delta W' \leftarrow Dp\_2(\Delta W)$
  $W_{center} \leftarrow W_{center} + \frac{1}{|Z_t|}\Delta W'$

W_{center}

W_{server}

Procedure Server
  download W_{center}
  $W_{server} \leftarrow W_{center}$
  while *1* **do**
    receive O_k' and L_j from the mobile device
    $W_{server} \leftarrow W_{server} - \eta \cdot \nabla Loss(W_{server})$
    send $\nabla Loss(O_k')$ 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

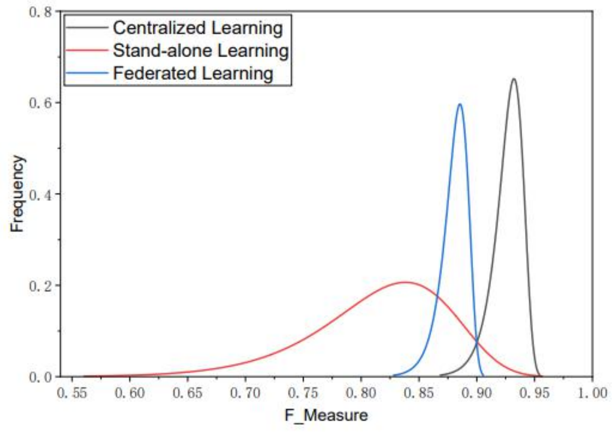
We distribute these training samples among 100 hospitals. Considering that the user data are not independent and identically distributed in multiple hospitals, we distribute these samples with following existing works [2].

Table 4: Distribution of training samples.

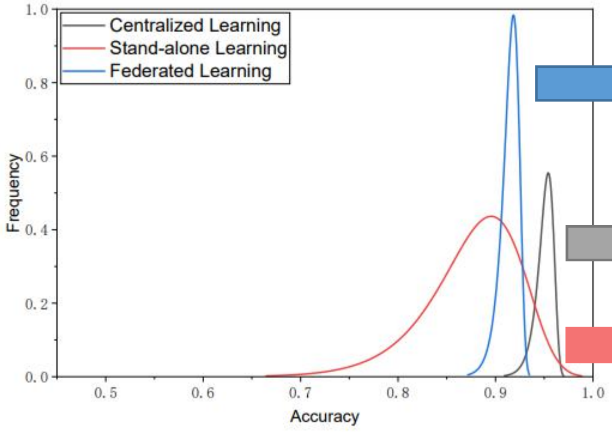
Value	1	2	3	4	5	6	7	8	9	10
Number	112	23	72	58	100	24	16	33	10	49

[1] Olvi L Mangasarian and William H Wolberg. 1990. Cancer diagnosis via linear programming. Technical Report. University of Wisconsin-Madison Department of Computer Sciences. https://archive.ics.uci.edu/ml/machine-learning-databases/ breast- cancer- wisconsin/
[2] Robin C. Geyer, Tassilo Klein, and Moin Nabi. 2017. Differentially Private Federated Learning: A Client Level Perspective. CoRR abs/1712.07557 (2017). arXiv:1712.07557 http://arxiv.org/abs/1712.07557

Results -- Diagnosis Performance



(a) F-Measure

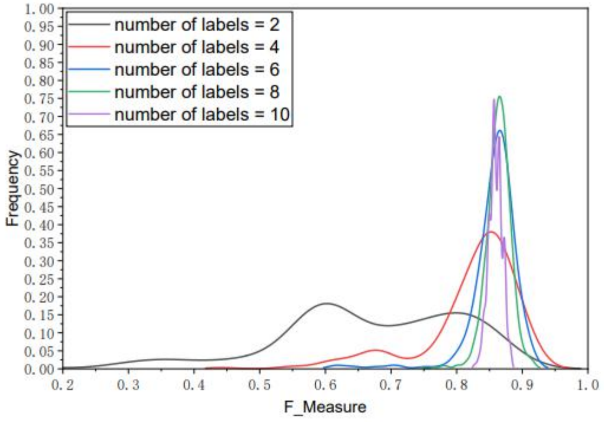


(b) Accuracy

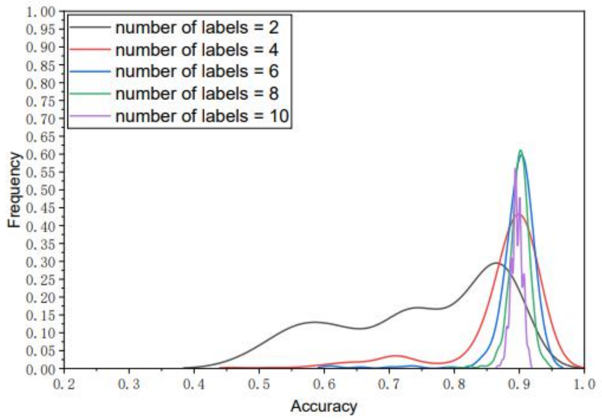
Federated Learning
(Near-Optimal performance without raw data leakage)

Centralized Learning
(Best performance but no privacy protection)

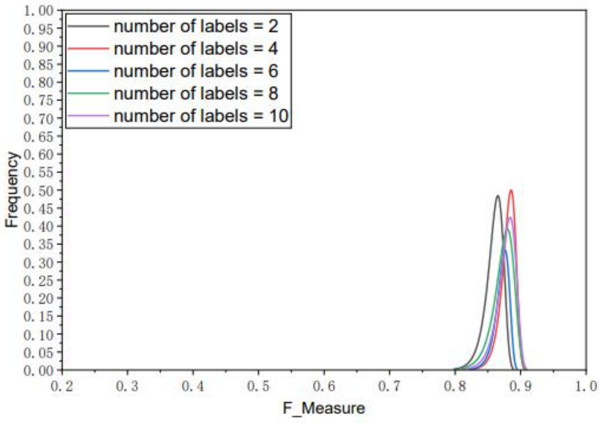
Stand-alone Learning
(Strong privacy protection but poor performance)



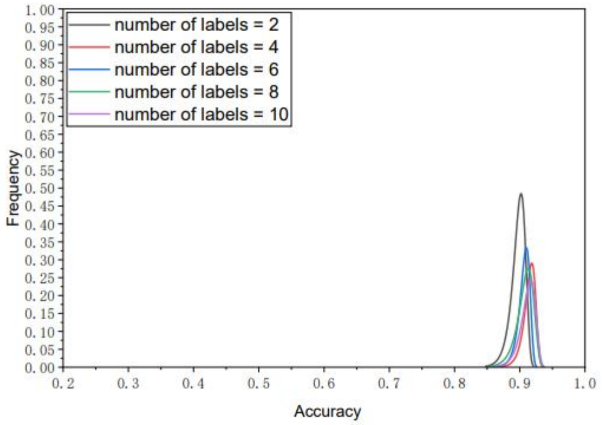
(a) F-Measure



(b) Accuracy



(a) F-Measure



(b) Accuracy

Stand-alone learning (**Fluctuate**)

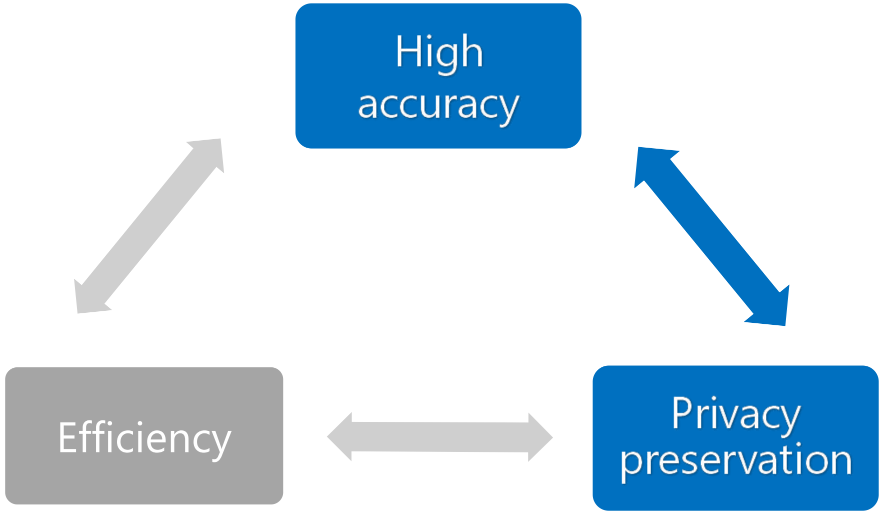
Federated learning (**Stable**)

Contributions

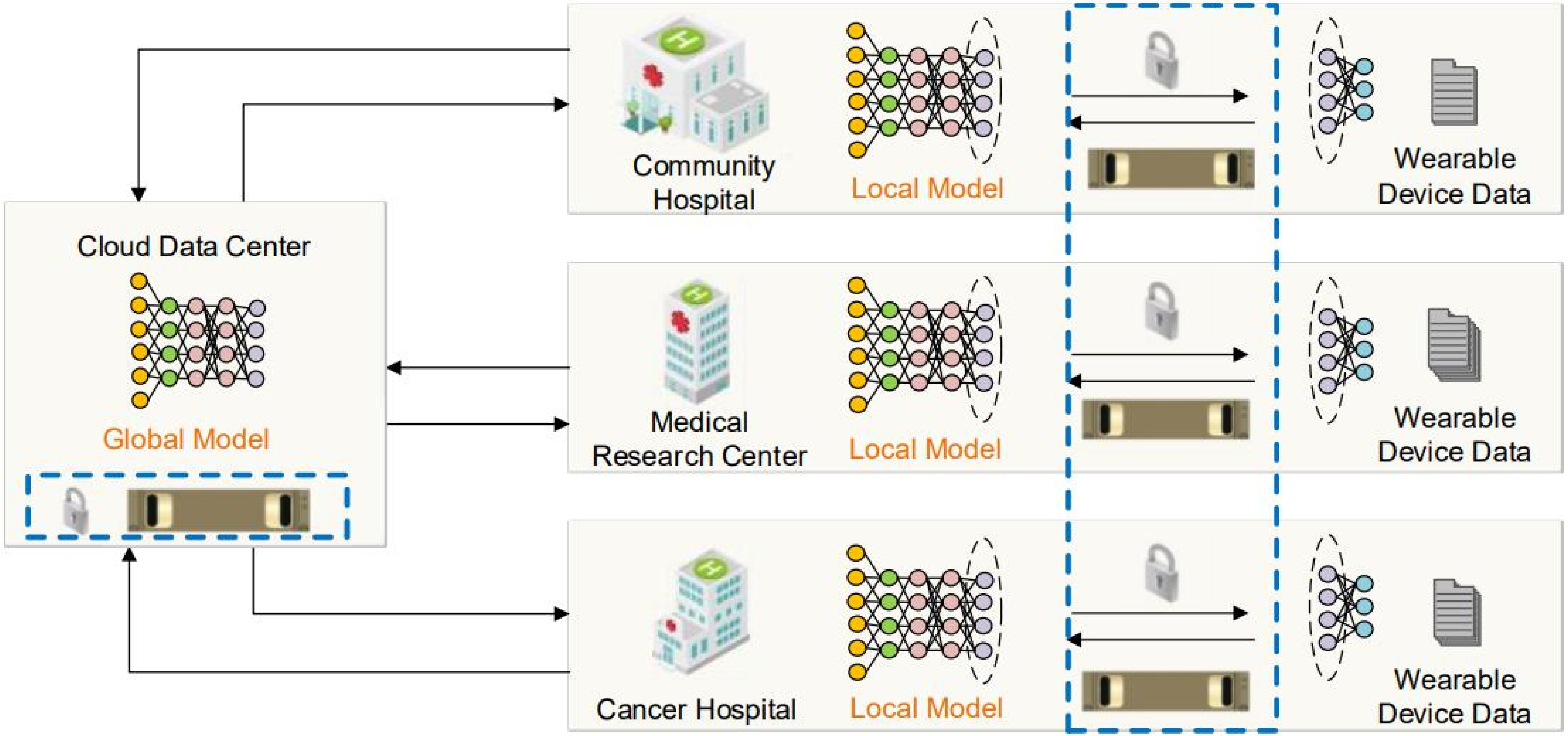
1. Efficient health monitoring and model training

2. Accurate diagnosis without raw data leakage

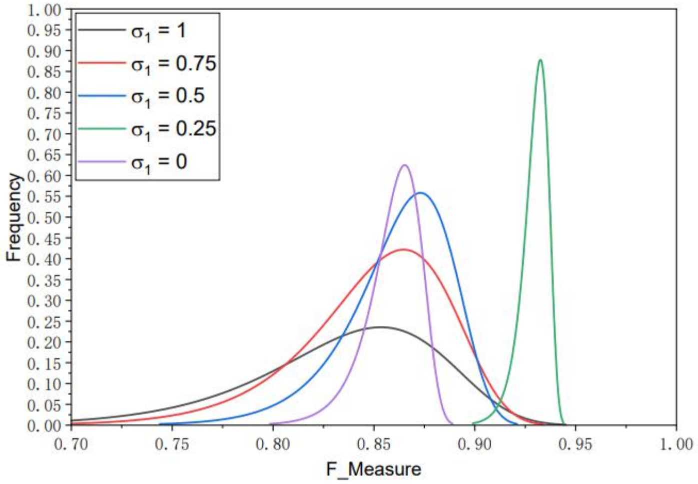
3. Study on privacy and performance



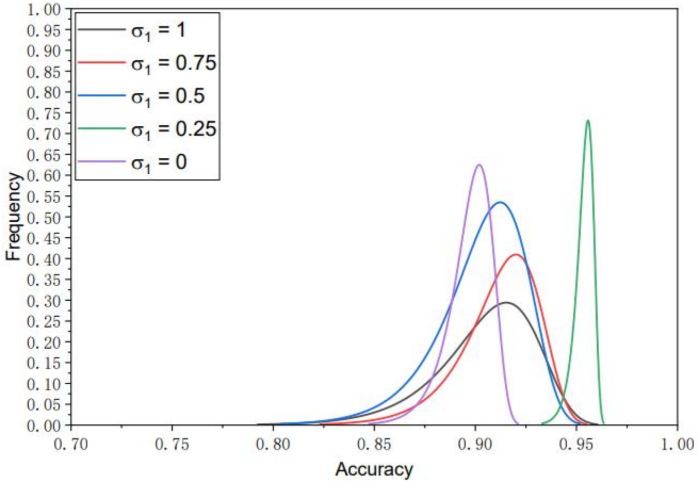
Privacy-preserving differential privacy scheme



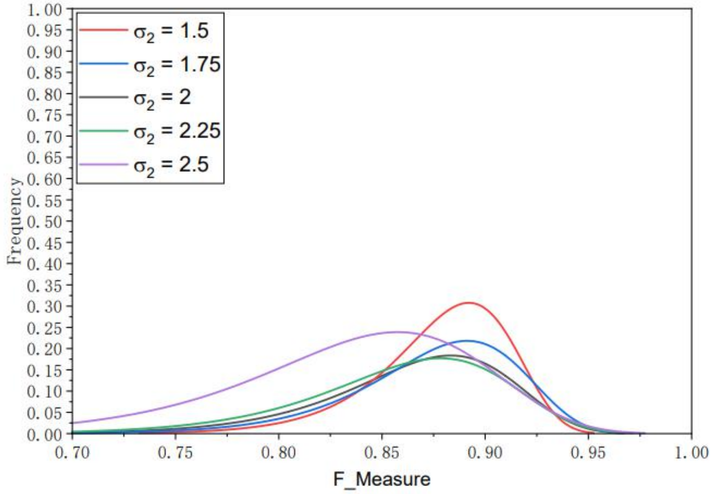
Results -- Sensitivity of σ1 and σ2



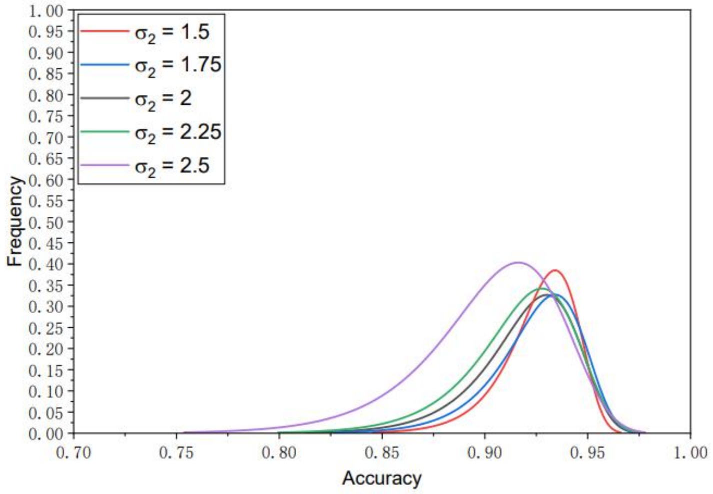
(a) F-Measure



(b) Accuracy



(a) F-Measure



(b) Accuracy

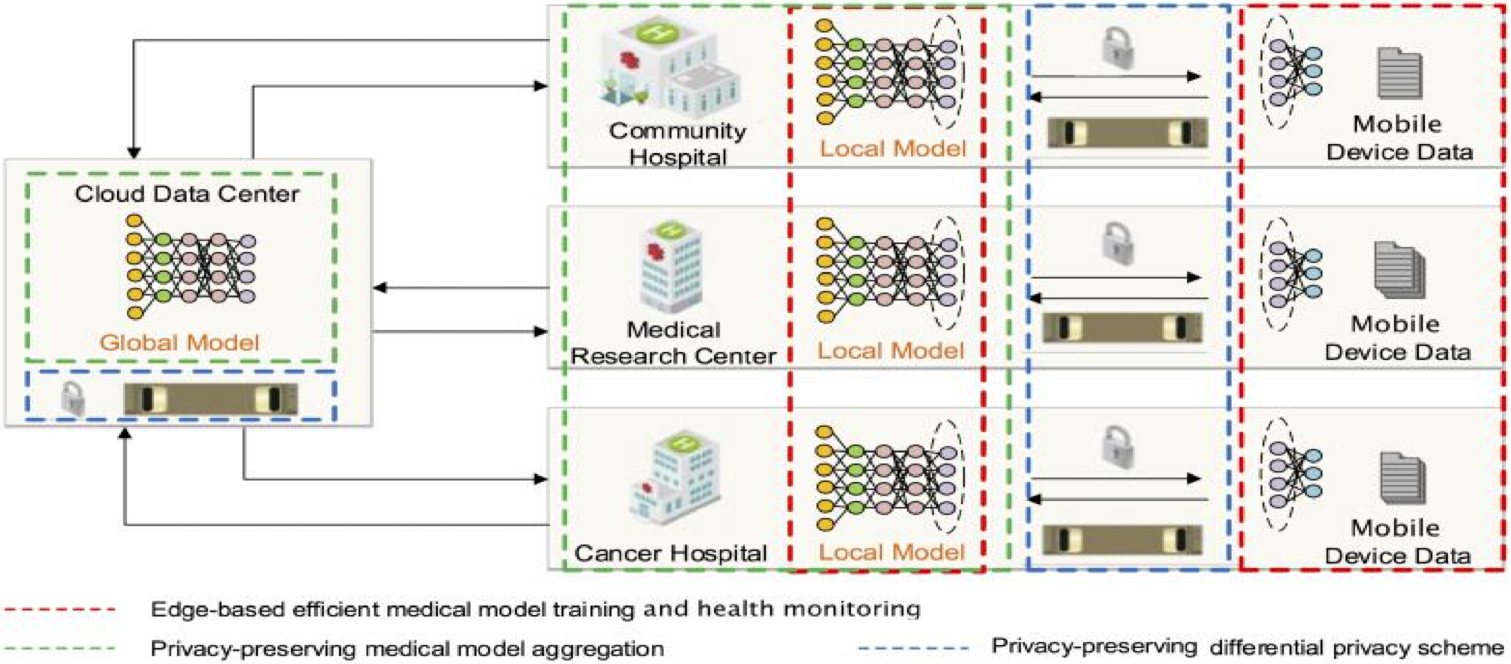
The performance gradually decreases with the increase of noise level. Considering both privacy and performance, we select σ1 and σ2 as 0.5 and 2.25, respectively.

Conclusion

Problem:

Address the inefficient and insecure scheme in mobile medical data training.

Key idea: FEderated Edge Learning (FEEL) system



Evaluation:

FEEL reduces the mobile devices' resource occupation (CPU time, memeory, energy et al.) and 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