北京郵電大學
Beijing University of Posts and Telecommunications

清華大學
Tsinghua University

Privacy as a Resource in Differentially Private Federated Learning

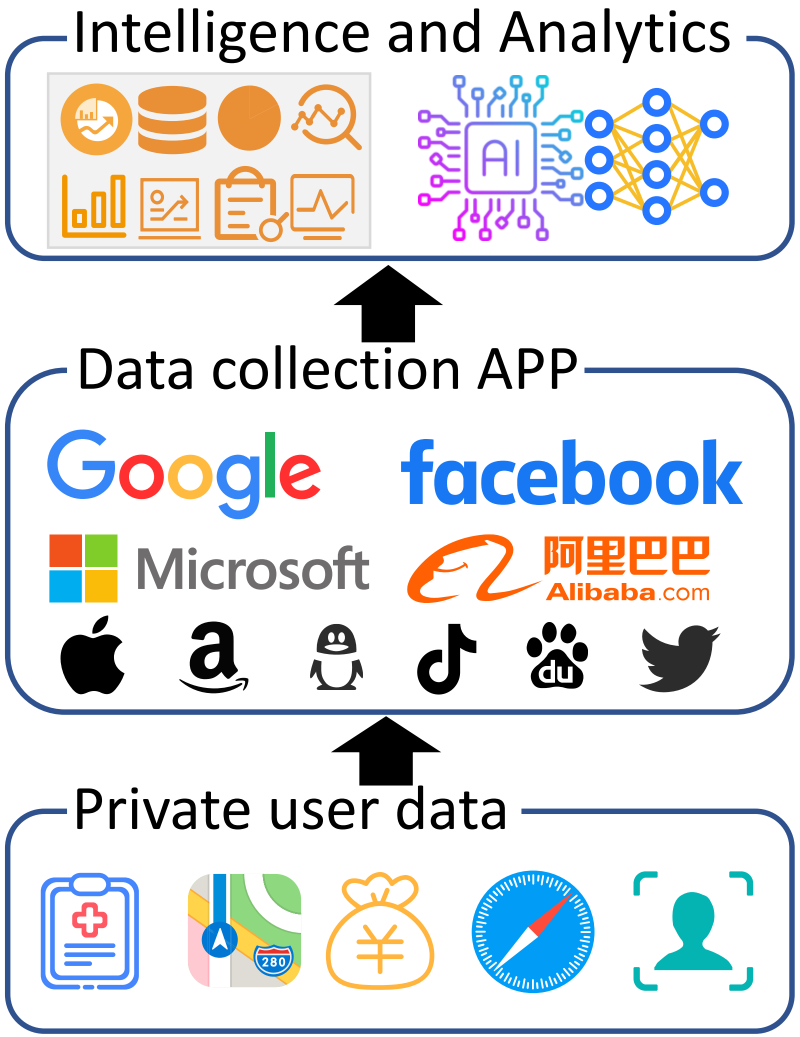
Jinliang Yuan[1], Shangguang Wang[1], Shihe Wang[1], Yuanchun Li[2], Xiao Ma[1], Ao Zhou[1] and Mengwei Xu[1]

[1]Beijing University of Posts and Telecommunications, China
[2]Tsinghua University, China

Privacy as a Resource in Differentially Private Federated Learning

- Motivation
- Design
- Evaluation

Privacy Leakage in Data-driven Mobile Applications


Intelligence and Analytics

Data collection APP

Private user data

Centralized data intelligence system

2018

facebook
VIDEO 00:39
Facebook ups users impact by Cambridge Analytica to 87 million

Facebook exposed 87 million user data

2019

Capital one bank leaked 106 million

2020

Microsoft exposed 250 million records

2021

Alibaba leaked 1.2 billion records

2022

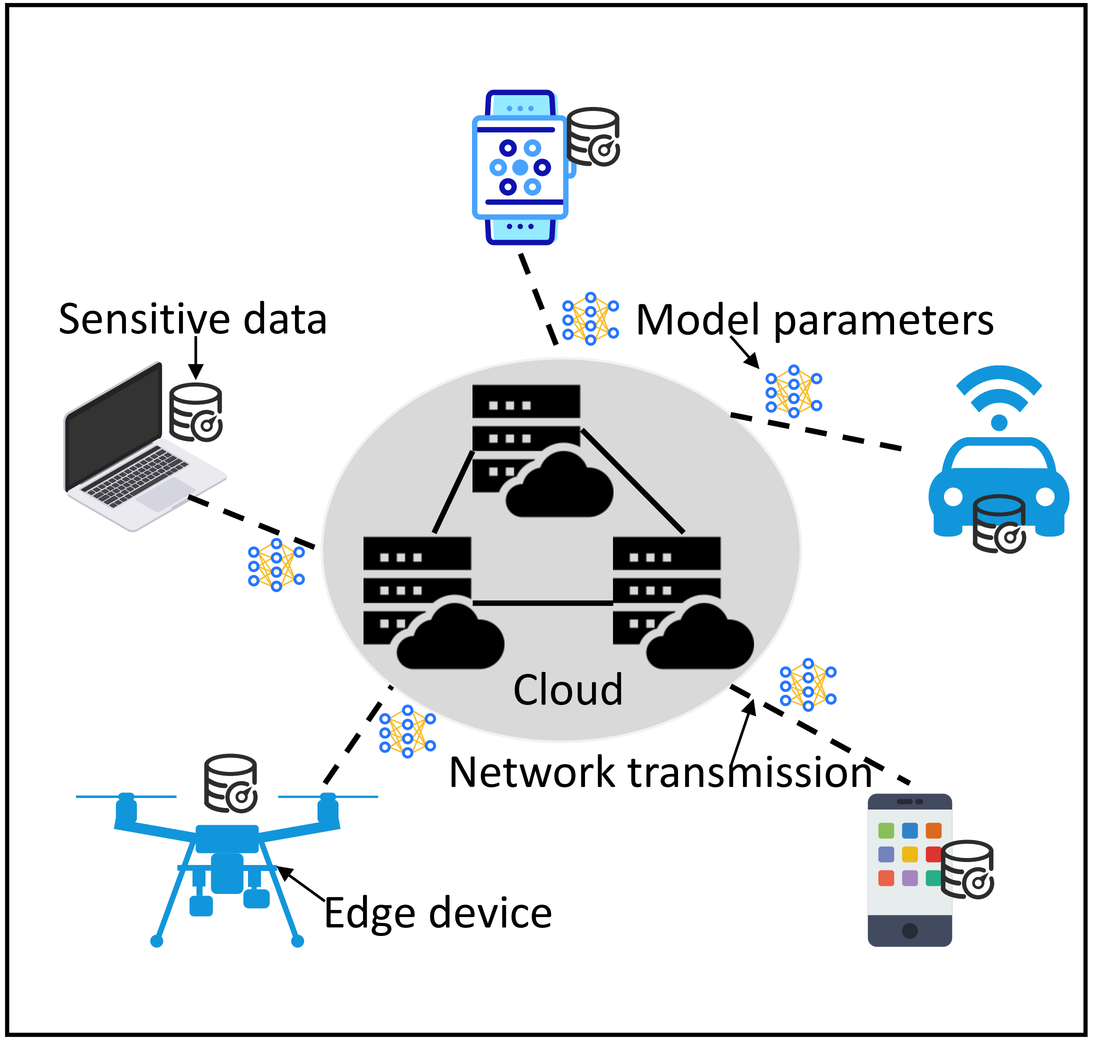
Cash app exposed 8 million records

Serious privacy leakage on user sensitive data

Federated Learning to Enhance Data Privacy

Cross-device Federated Learning System

Cons???

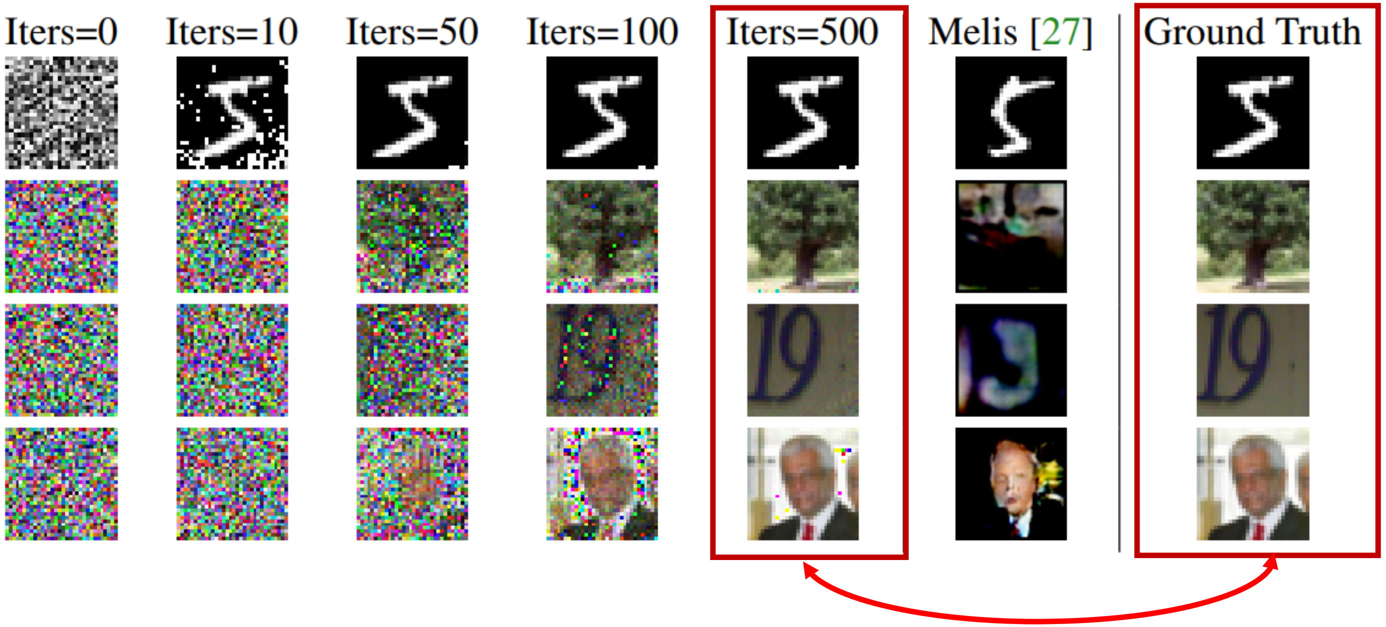


Main workflow:

- ➢ **Keep sensitive data on device**
- ➢ On-device model training
- ➢ **Model transmission through network**
- ➢ Model aggregation on cloud

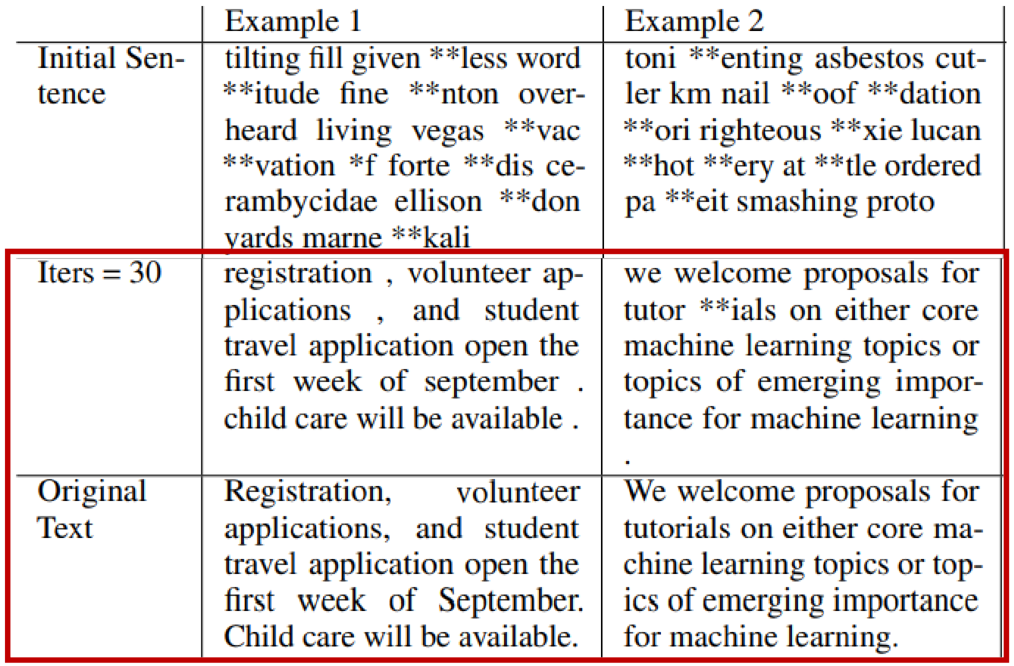
Pros: Decentralized data storage and model training, instead of a centralized way

Deep Leakage From Gradients



Nearly the same

(1) computer vision



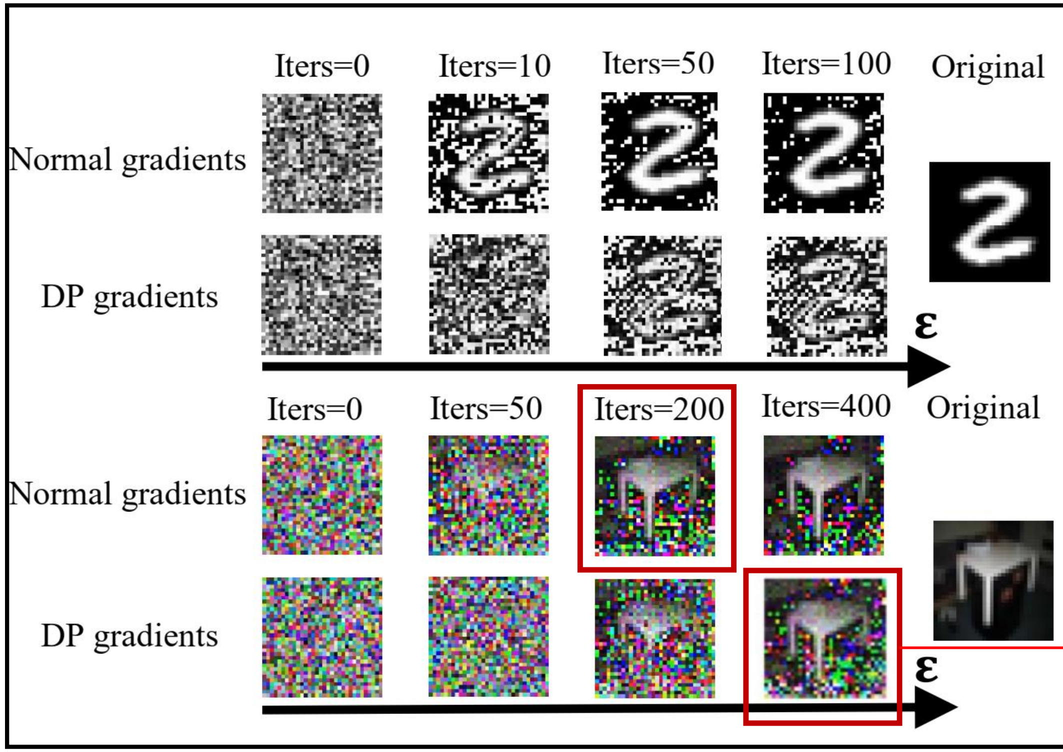
	Example 1	Example 2
Initial Sentence	tilting fill given **less word **itude fine **nton overheard living vegas **vac **vation *f forte **dis cerambycidae ellison **don yards marne **kali	toni **enting asbestos cutler km nail **oof **dation **ori righteous **xie lucan **hot **ery at **tle ordered pa **eit smashing proto
Iters = 30	registration , volunteer applications , and student travel application open the first week of september . child care will be available .	we welcome proposals for tutor **ials on either core machine learning topics or topics of emerging importance for machine learning .
Original Text	Registration, volunteer applications, and student travel application open the first week of September. Child care will be available.	We welcome proposals for tutorials on either core machine learning topics or topics of emerging importance for machine learning.

(2) natural language processing

Contribution: It is possible to obtain the private training data from the publicly shared gradients, which means the raw model transmission through network in FL is not safe.

Reference: Deep leakage from gradients; Advances in neural information processing systems; Massachusetts Institute of Technology; 2019

Differential Privacy to Protect Gradient Exchange



1× more rounds

Illustration of privacy leakage on MNIST and CIFAR100 with **normal gradients and DP randomized gradients** with a Gaussian noise $\varepsilon \sim N(0, \delta^2 I)$

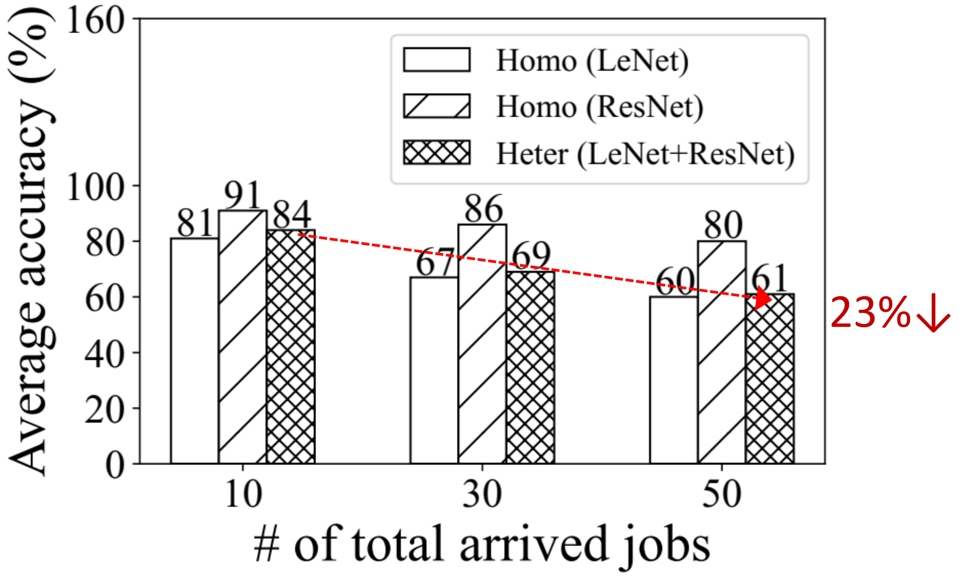
DP is the most popular and effective solution, currently [refs]

Ref #1: Learning **differentially private** recurrent language models; ICLR-18; Google
Ref #2: Privacy accounting and quality control in the sage **differentially private** ML platform; SOSP; Columbia University
Ref #3: FLAME: **differentially private** federated learning in the shuffle model; IJCAI-21; Renmin University of China
Ref #4: LDP-FL: practical private aggregation in federated learning with local **differential privacy**; IJCAI-21; Lehigh University
Ref #5: Renyi **differential privacy** of the subsampled shuffle model in distributed learning; NeurIPS-21; University of California

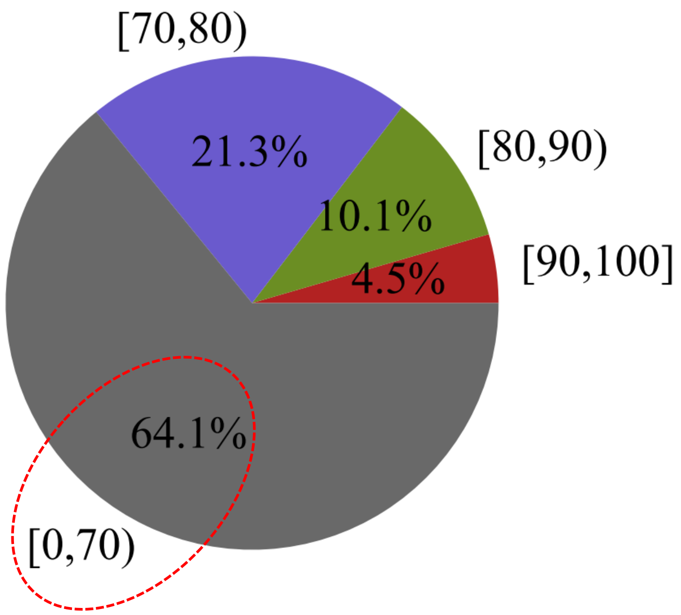
Challenges of Differentially Private FL System

System or platform perspective

Although differential privacy technology performs well on a **single FL task**, it causes **serious performance degradation** in more practical scenario with **multiple submitted FL jobs**.

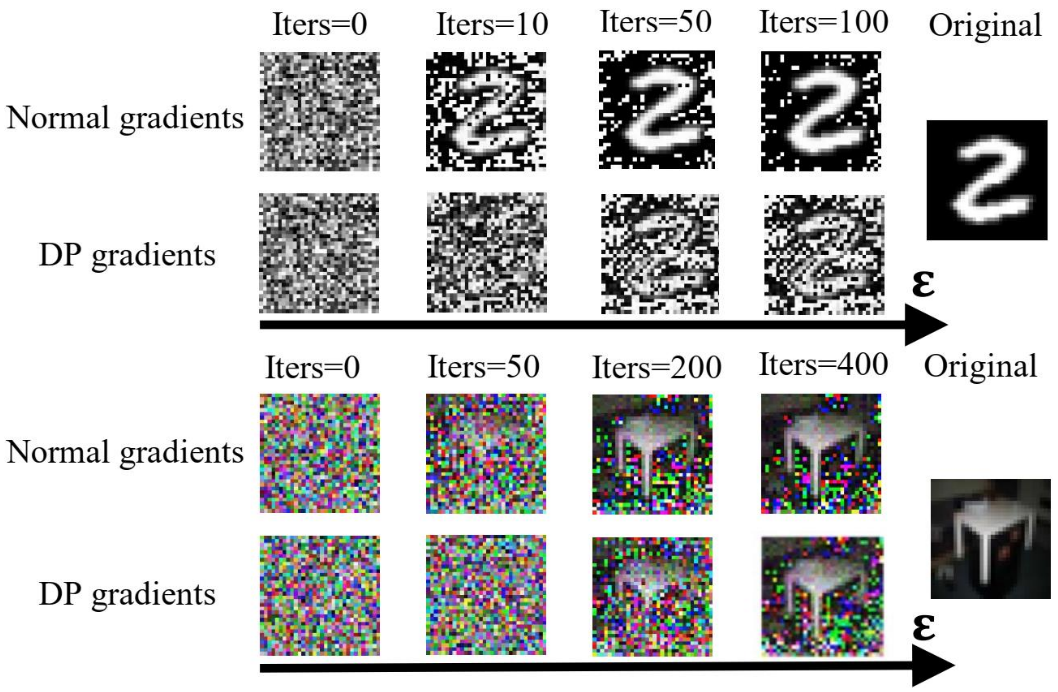


(a) Average accuracy of allocated jobs decreased significantly (23%↓) as the number of jobs increased.

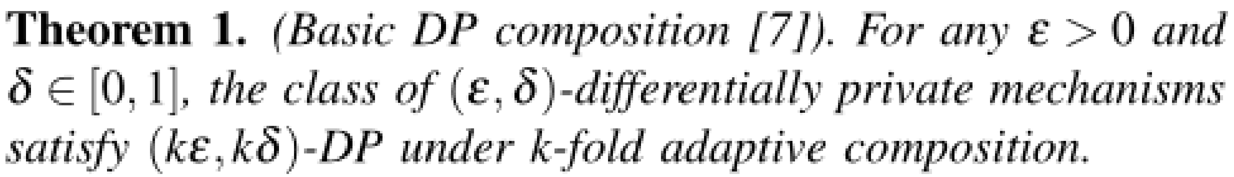


(b) Only a very small number of jobs (14.6%) obtained acceptable model accuracy (e.g., ≥ 80%), and most jobs' accuracy is too low (e.g., < 70%).

Underlying Rationales



(a) Trade-off between privacy budget and model accuracy



Theorem 1. *(Basic DP composition [7]). For any $\varepsilon > 0$ and $\delta \in [0,1]$, the class of (ε,δ)-differentially private mechanisms satisfy $(k\varepsilon, k\delta)$-DP under k-fold adaptive composition.*

(b) More jobs, more budget

Goals

Our goal is to develop a unified differentially private FL platform that coordinates dynamically arrived FL jobs with sensitive user data streams. The platform aims to enforce a global (ε,δ)-DP guarantee across participating devices to control the leakage of user information.

To improve the utility of sensitive user data, it focuses on **how to schedule the global privacy budget to deliver more completed jobs and reduce SLO violation rate**.

In short, how to serve more FL jobs with tight privacy budget?

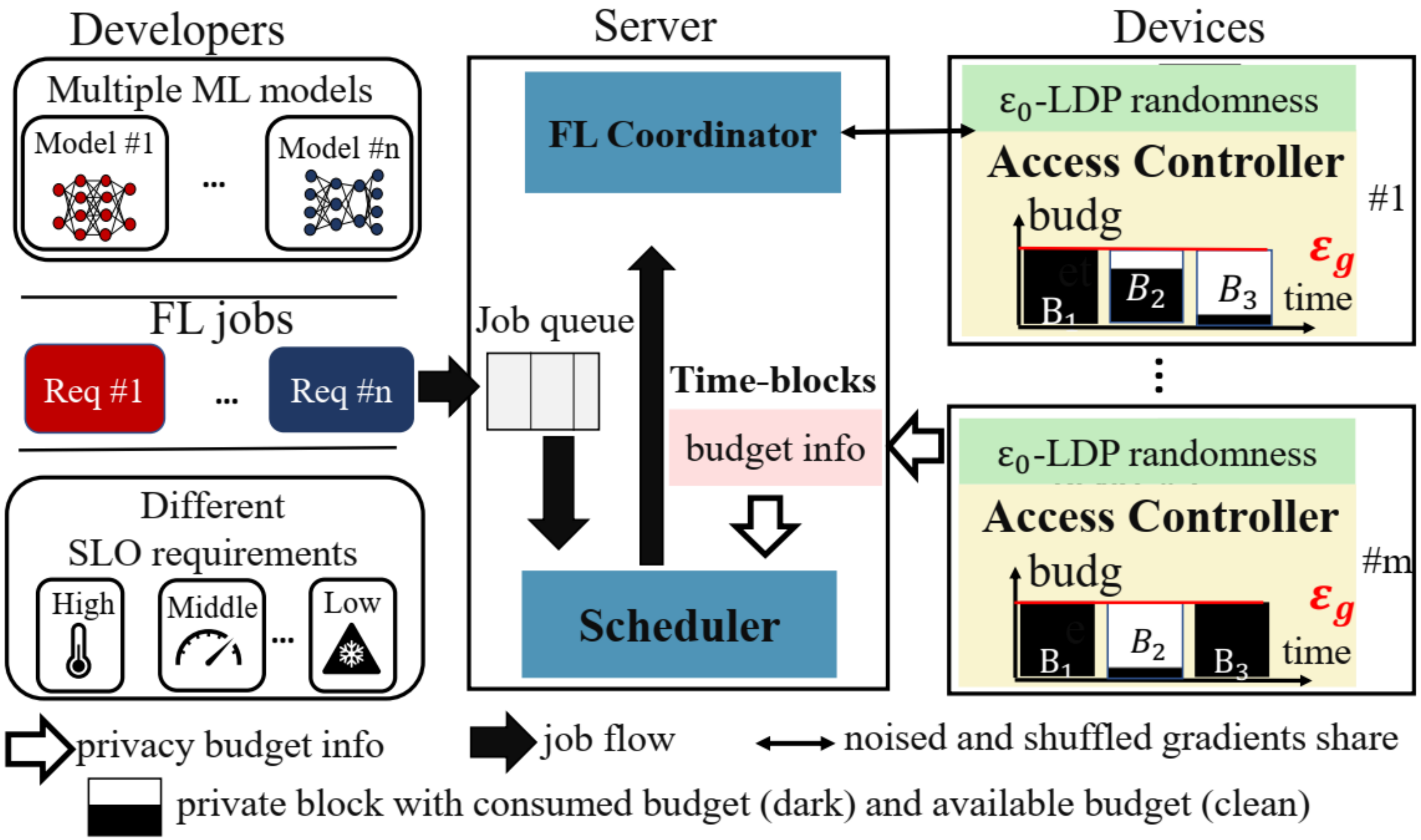
FLScheduler: Privacy as a Resource

Design Overview

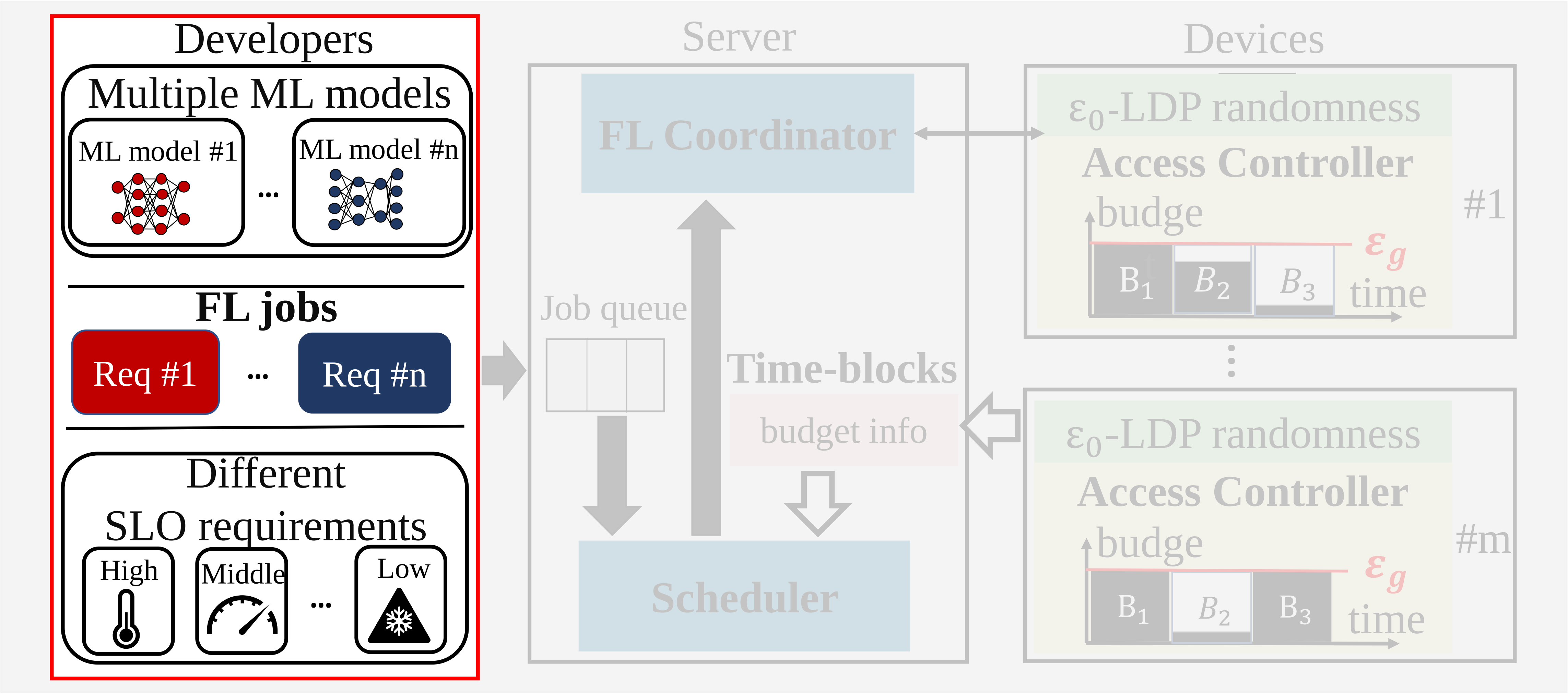
- ➢ Enable “endless” privacy budget consumption as time goes by
  - spilt data stream to time-frame blocks
  - time-blocks composition theorem

- ➢ Support fine-grained privacy budget scheduling
  - AaR algorithm to reduce SLO violation rate
  - Best-effort to serve more complete jobs

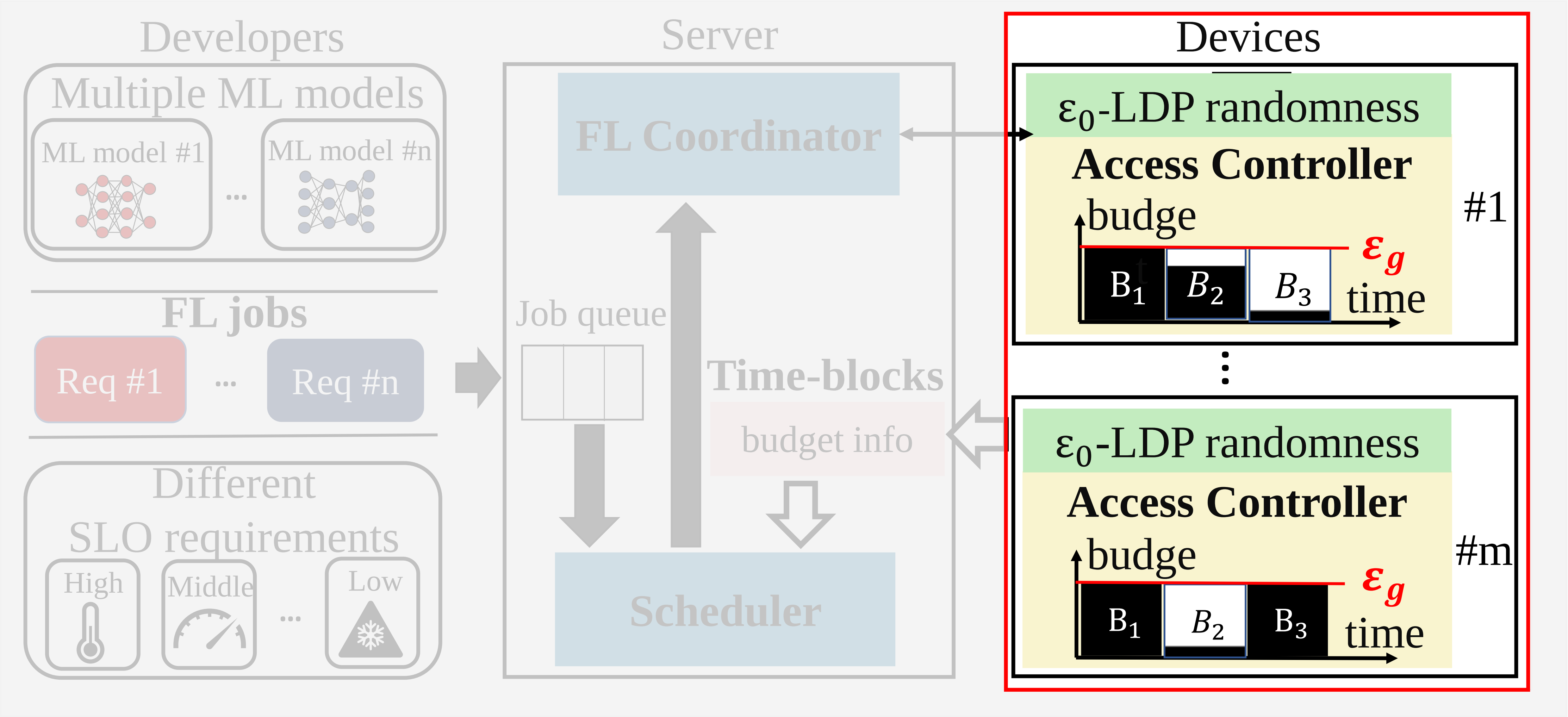
Overview of our differentially private FL platform



FLScheduler: Privacy as a Resource

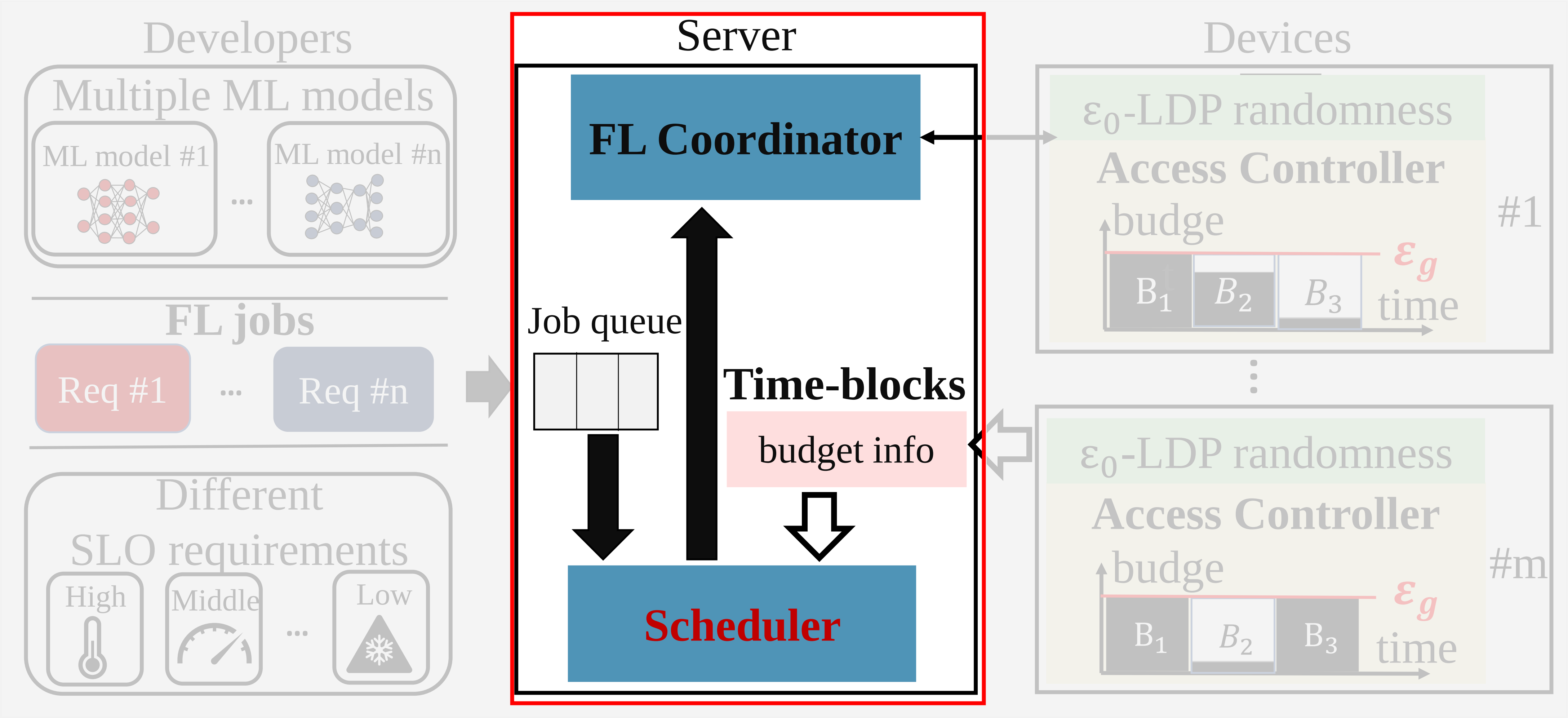


FLScheduler: Privacy as a Resource



▄ private block with consumed budget (dark) and available budget (clean)

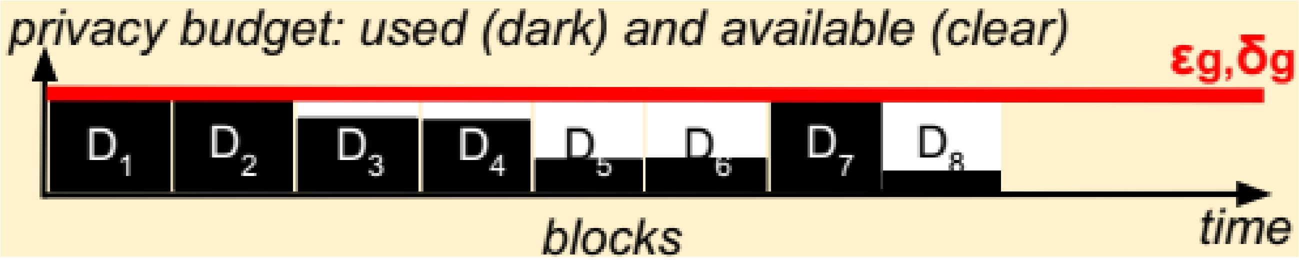
FLScheduler: Privacy as a Resource



Time-blocks Composition Theorem

DP mechanism accounts for privacy loss at the granularity of whole data streams, which leads to a critical **challenge** in FL: running out of privacy budget quickly

- Unused data points suffer the same privacy loss as the samples data points on each device.
- Unused devices suffer the same privacy loss as the sampled devices during FL training.
- Newly-generated data over time suffers the same privacy loss as the used data.



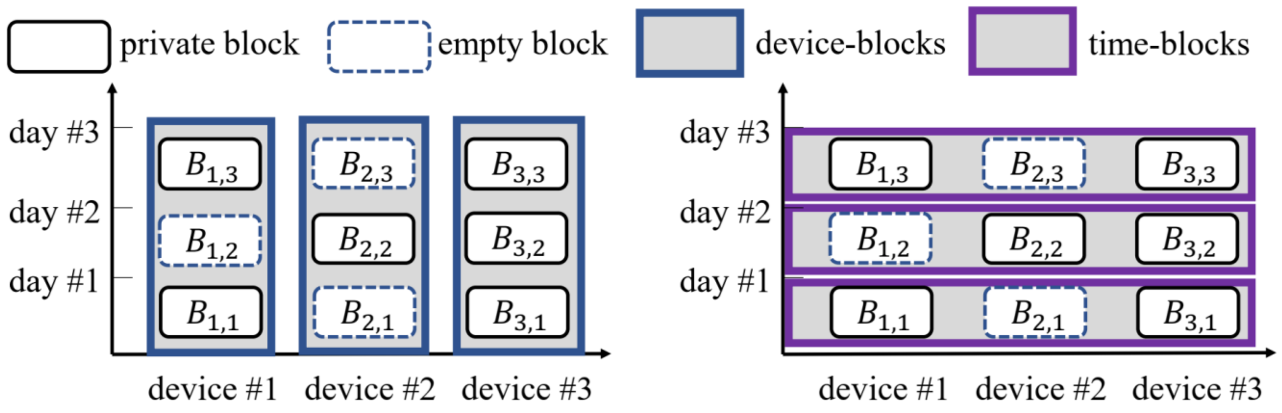
Sage proposed a new privacy accounting method on the split data block, namely block composition theorem, in a centralized ML platform. **Address #1 and #3.**

*Reference: Privacy accounting and quality control in the **sage** differentially private ML platform; SOSP-19; Columbia University*

Time-blocks Composition Theorem

However, the **centralized block composition** can not account for the privacy loss on blocks across **distributed devices,** because the SOTA DP mechanism in FL accounts for privacy loss at the granularity of whole data streams **across all devices.**

- Unused data points suffer the same privacy loss as the samples data points on each device.
- **Unused devices suffer the same privacy loss as the sampled devices during FL training.**
- Newly-generated data over time suffers the same privacy loss as the used data.



(a) device-blocks

(b) time-blocks

Time-blocks Composition Theorem

Privacy accounting at the granularity of time-blocks when running multiple FL jobs with different SOTA DP mechanisms.

Two-stage Privacy Budget Scheduling

Our goal is carefully scheduling such a scarce resource to maximize the number of complete jobs while reducing the SLO violation rate. However, it is **substantially differs** from traditional resource scheduling, like CPU cycles, memory……

- Privacy is a non-replenishable resource.
- All-or-nothing principle.
- Budget requirements changing with FL's uncertain block/device selection

Dominant Private Block Fairness, DPF [ref]

DPF's key idea is twofold:
(1) **unlock privacy budget** for each block progressively, so the budget remains for the future;
(2) follow DRF's max-min fairness design to allocate these blocks fairly among different jobs.

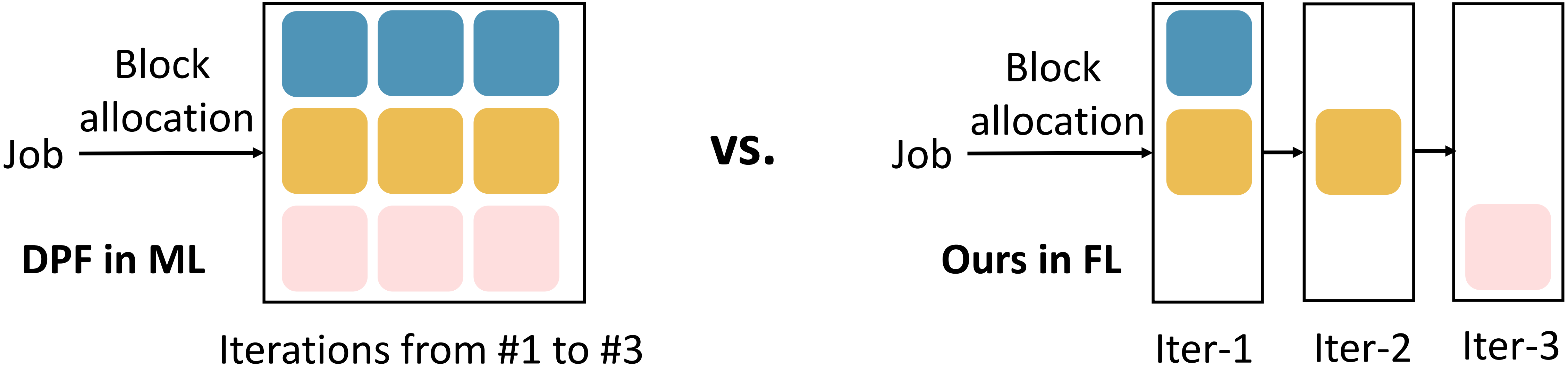
Reference: Privacy budget scheduling; OSDI-21; Columbia University

Two-stage Privacy Budget Scheduling

However, DPF assumes a prior and fixed privacy budget consumption for each job**, which is not appropriate in cross-device FL scenario.**

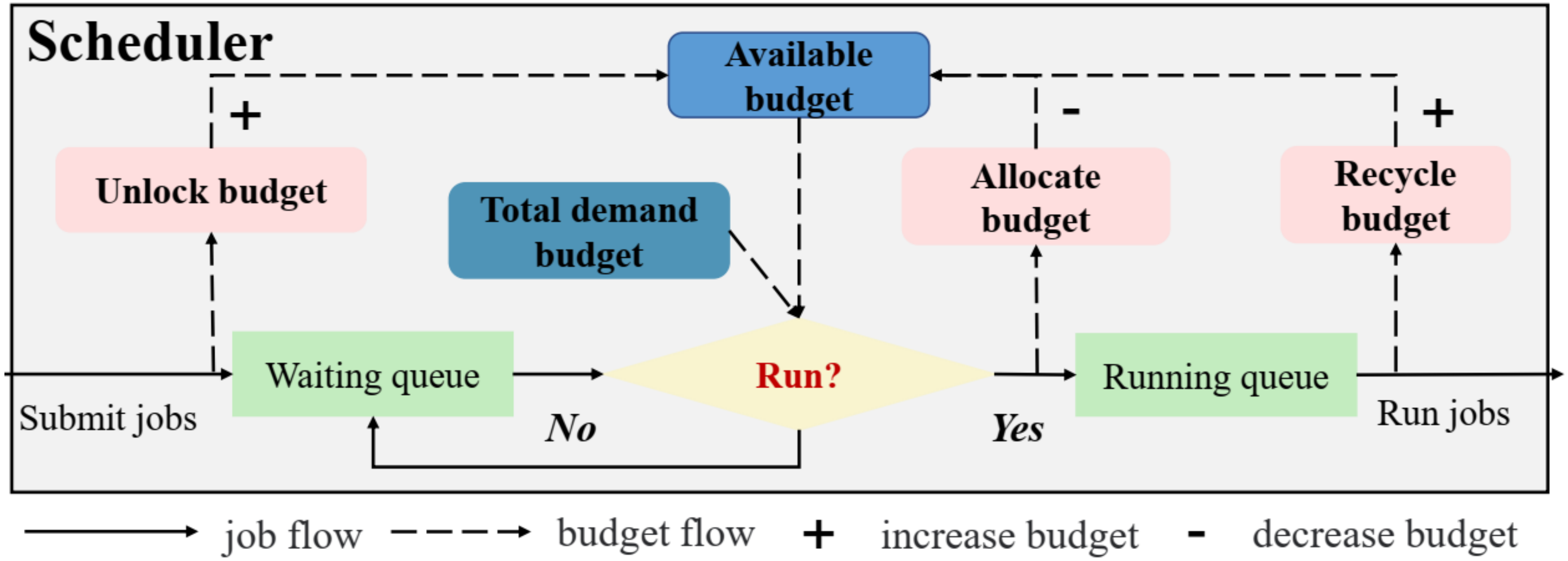
- Privacy is a non-replenishable resource.
- All-or-nothing principle.
- **Budget requirements changing with FL's uncertain block/device selection.**

Fixed and prior requirements of block **VS.** Iteration-level dynamic block/device selection



Two-stage Privacy Budget Scheduling

Our solution: Allocation and Recycle (AaR)
Key idea consists of two core stages: (1) a pre-allocation of an **estimated upper-bound privacy budget** at each FL job arrival; (2) and a **progressive recycling** of the un-consumed privacy budget during FL training.



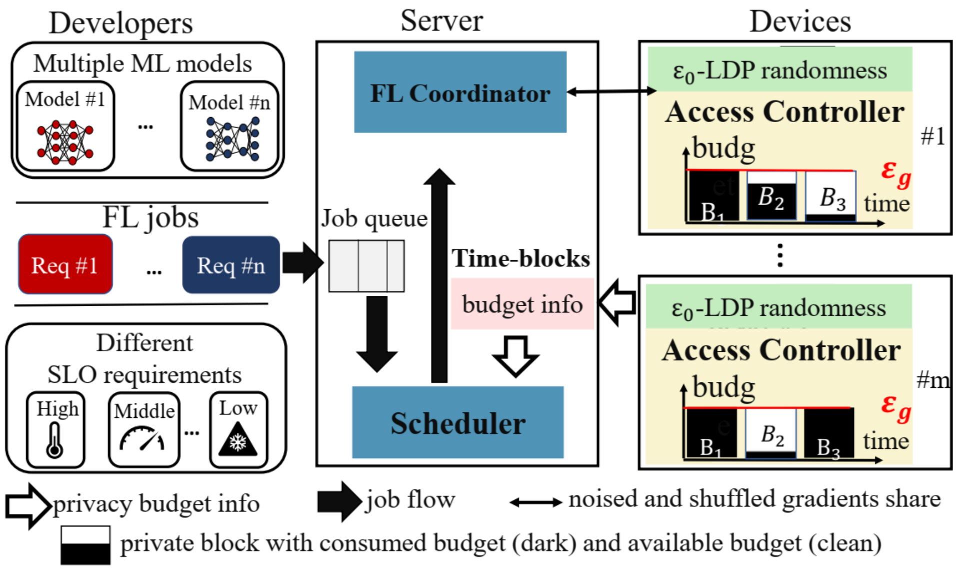
Evaluation

Experiment Settings

Simulation platform atop FedML integrated with 4 major functional modules:

- LDP-based FL training
- block-related data preprocessing
- block-related privacy accounting
- job scheduler

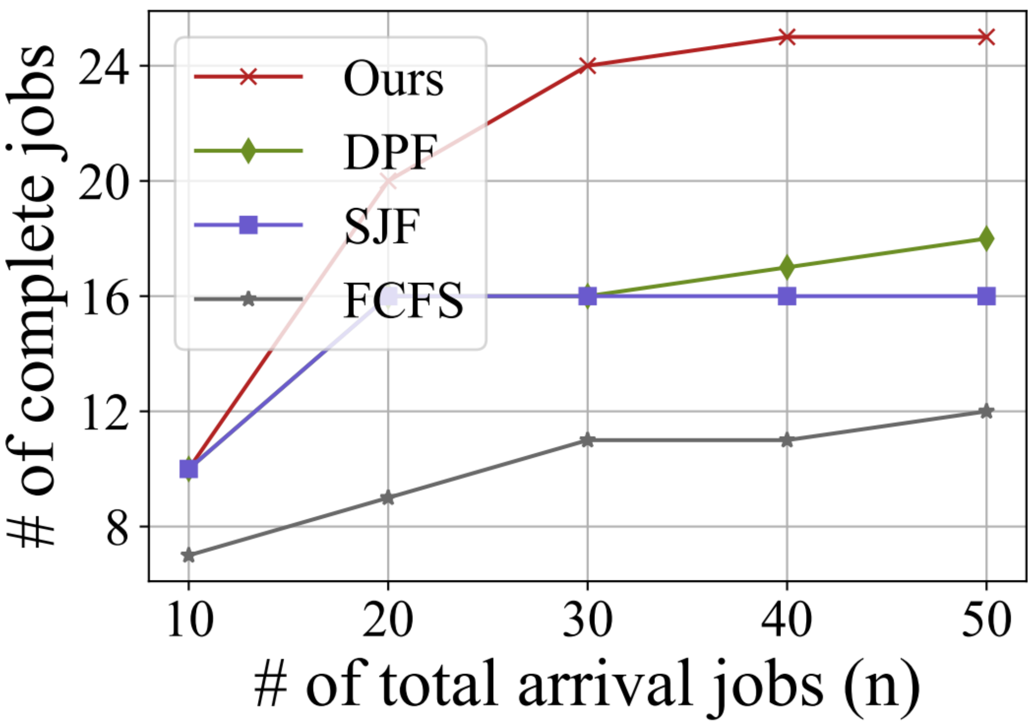
https://github.com/UbiquitousLearning/FLScheduler



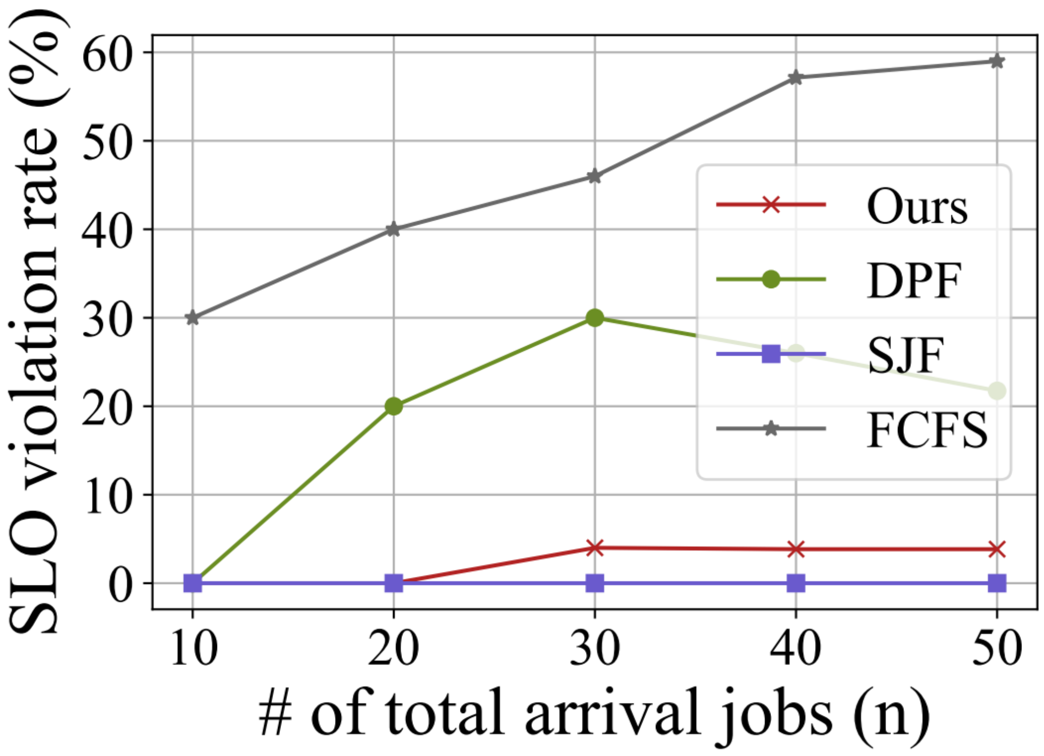
- ➢ FL jobs to train LeNet and ResNet models with requirements (r, ε_0)
- ➢ Schedule algorithm: FCFS, SJF, DPF
- ➢ 10000 devices with 10 time-blocks each
- ➢ Metrics: number of completed jobs and SLO violation rate

Evaluation

End-to-end performance



(a) Increase complete jobs (2×)

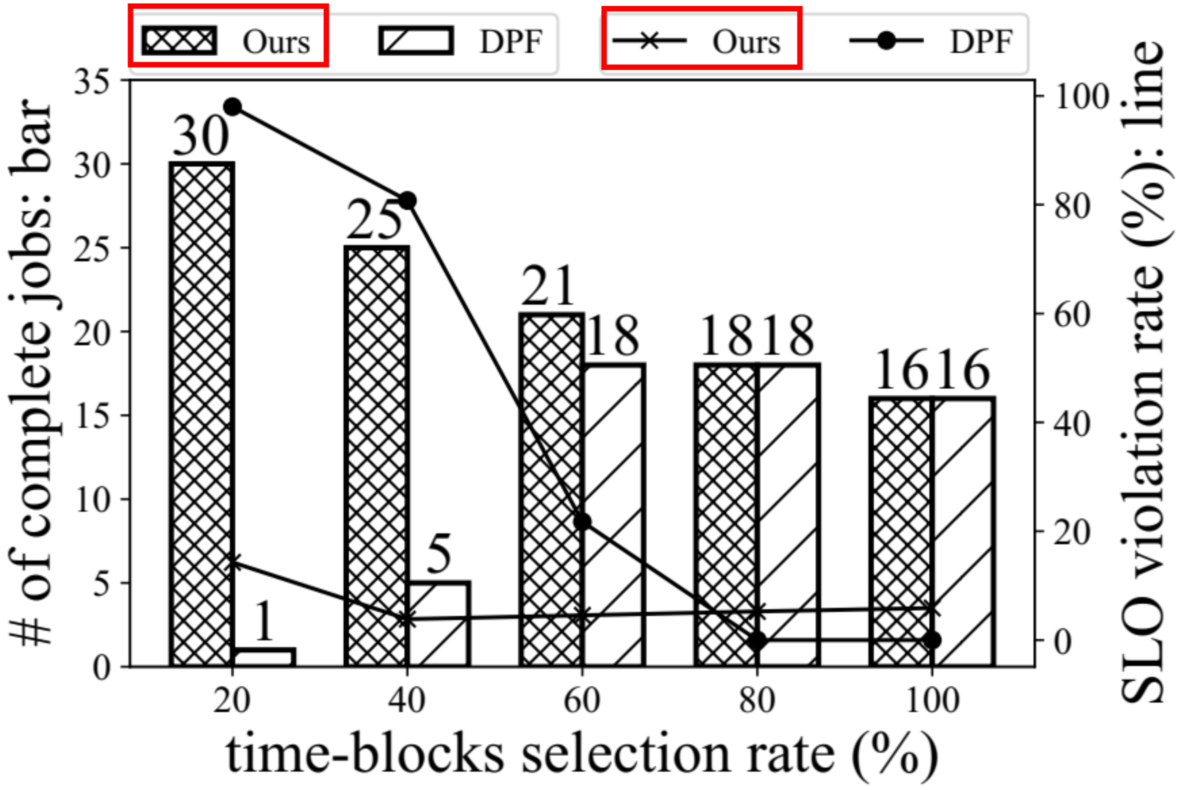


(b) Reduce violation rate (55%)

Our algorithm achieves more complete jobs with a lower violation rate.

Evaluation

Sensitivity analysis: Impact of Time-blocks Selection Rate



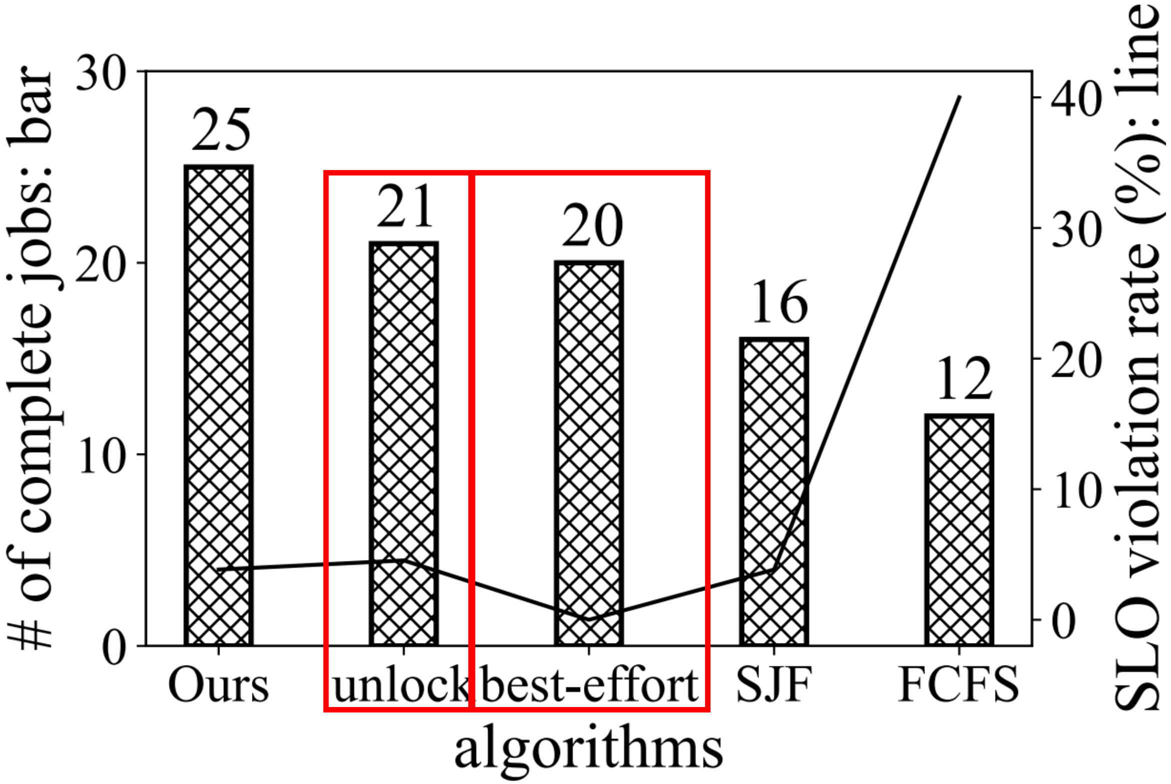
(1) Trade-off between the two metrics: higher bar and lower line

(2) Fewer selected time-blocks attributes more complete jobs with lower violation rate

(3) Rationale: ours fine-grained block sampling strategy allows the model to be trained by more samples at a lower expense of privacy budget.

Evaluation

Ablation Results: AaR’s unlock and best-effort design



(1) They both outperform SJF and FCFS

(2) But, 20% and 16% less than ours with they both enabled

FLScheduler: Privacy is also a resource that needs to be well scheduled

https://github.com/UbiquitousLearning/FLScheduler
yuanjinliang@bupt.edu.cn

FLScheduler

- Specific time-blocks selection for cross-device FL
- Fine-grained privacy budget scheduling for more complete jobs

Thank you

北京郵電大學
Beijing University of Posts and Telecommunications