



INTERNATIONAL JOINT CONFERENCE ON NEURAL NETWORKS

IJCNN2025

30 JUNE - 5 JULY 2025 | ROME, ITALY



INTERNATIONAL NEURAL NETWORK SOCIETY

Sequential Privacy: Rethinking Privacy in RL for Sequential Decision-making in the Age of LLMs

A position paper for IJCNN 2025

Flint Xiaofeng Fan, Cheston Tan, Roger Wattenhofer, Yew-Soon Ong



Centre for
Frontier AI
Research

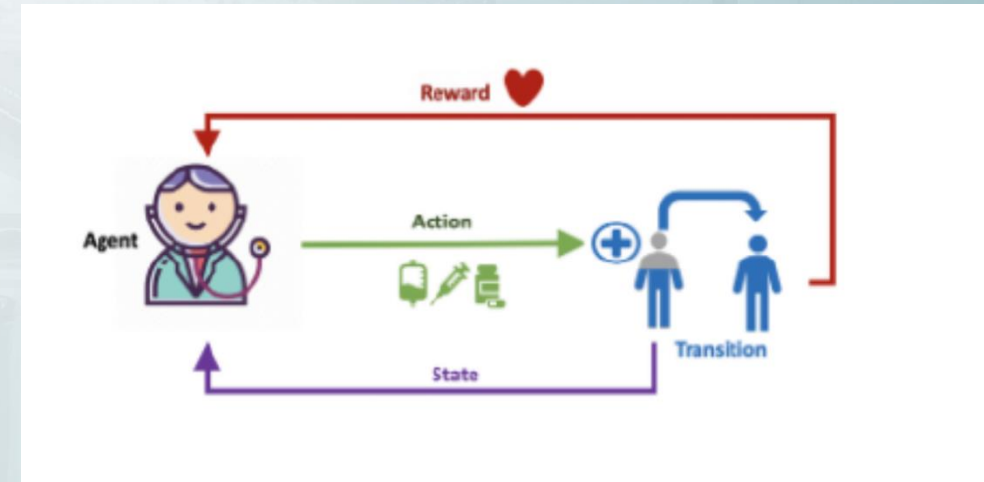
A*STAR CFAR

ETH zürich

The Stakes - A Hospital Scenario

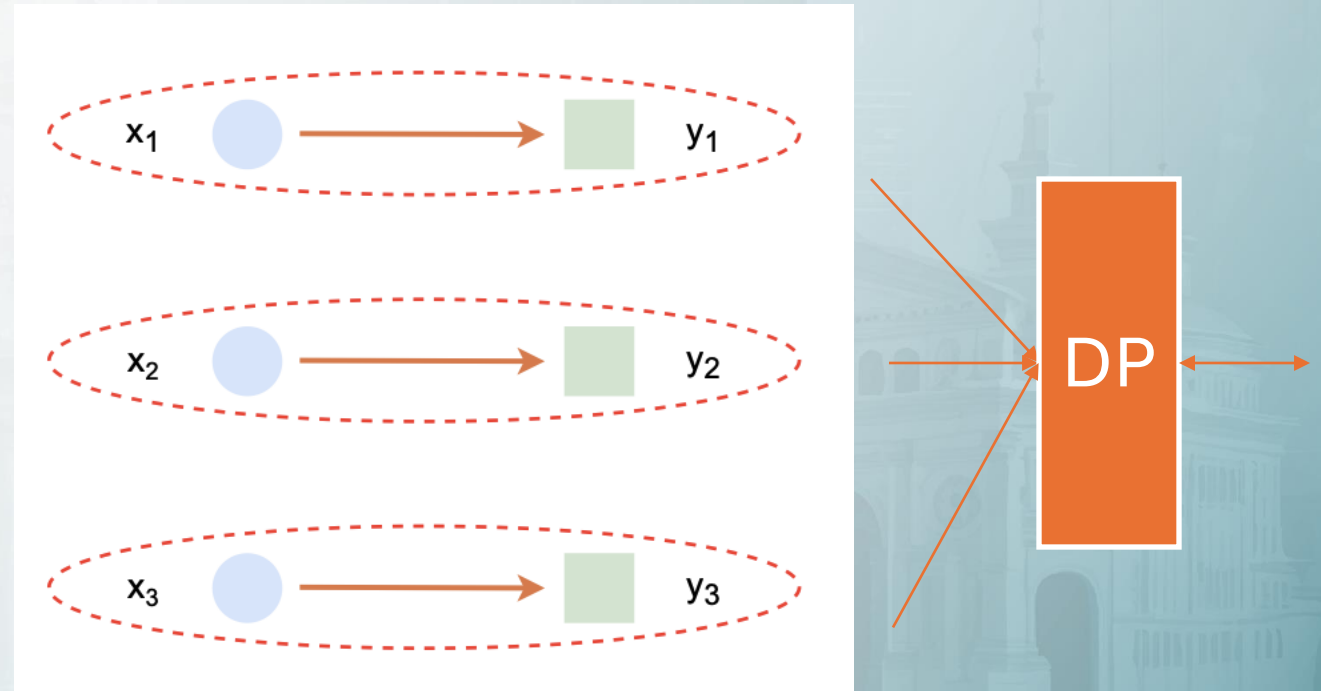


Time (t)	Blood-Glucose (BG_t)	Action ($a_t =$ insulin units)
08:00	200 mg/dL	3 U
09:00	150 mg/dL	1 U
11:30	240 mg/dL (post-lunch)	4 U
13:00	180 mg/dL	2 U



Traditional Privacy Framework – Differential Privacy

- Add calibrated noise to the results of data queries
- Mask out the contribution of any single data point
- With mathematical guarantees about information leakage

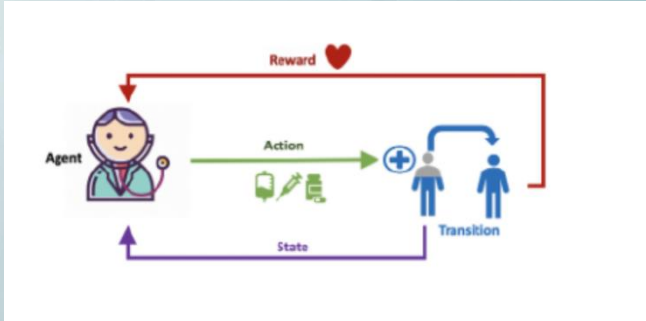




The Stakes - A Hospital Scenario

Time (t)	Blood-Glucose (BG_t)	Action ($a_t =$ insulin units)
08:00	200 mg/dL	3 U
09:00	150 mg/dL	1 U
11:30	240 mg/dL (post-lunch)	4 U
13:00	180 mg/dL	2 U

DP

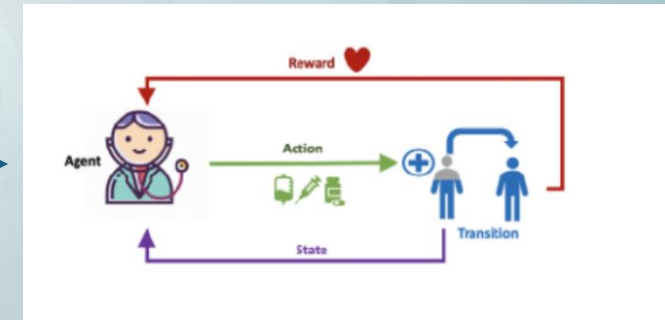




The Stakes - A Hospital Scenario

Time (t)	Blood-Glucose (BG_t)	Action ($a_t =$ insulin units)
08:00	200 mg/dL	3 U
09:00	150 mg/dL	1 U
11:30	240 mg/dL (post-lunch)	4 U
13:00	180 mg/dL	2 U

DP



Eating habits, insulin sensitivity, work schedule, unique physiological response, etc.

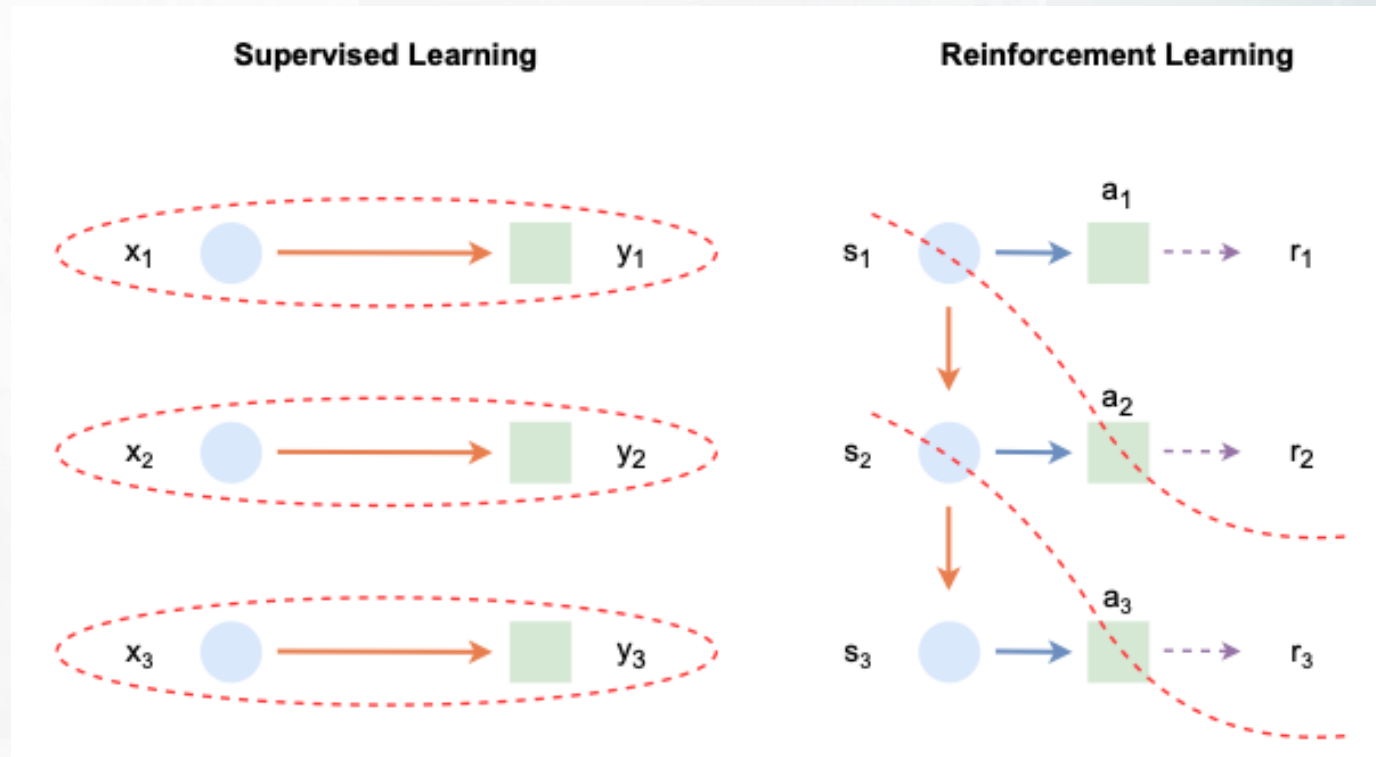


How do we protect privacy that lives in sequence of trajectories, not just individual data points?



INTERNATIONAL JOINT CONFERENCE ON NEURAL NETWORKS
IJCNN2025
30 JUNE - 5 JULY 2025 | ROME, ITALY
INTERNATIONAL NEURAL NETWORK SOCIETY

Why Traditional Framework (DP) Fails for RL



Privacy challenges

- Temporal correlation
- Behavioral privacy
- Collaborative privacy
- Context-dependence

Our Position

Privacy challenges

- Temporal correlation
- Behavioral privacy
- Collaborative privacy
- Context-dependence



Sequential Privacy

- Multi-scale protection
- Behavioral pattern protection
- Collaborative privacy preservation
- Context-aware adaptation

Challenge: Temporal Correlation

Time (t)	Blood-Glucose (BG_t)	Action ($a_t =$ insulin units)
08:00	200 mg/dL	3 U
09:00	150 mg/dL	1 U
11:30	240 mg/dL (post-lunch)	4 U
13:00	180 mg/dL	2 U



Why traditional DP fails

Time (t)	Blood-Glucose (BG_t)	Action ($a_t =$ insulin units)
08:00	200 mg/dL	3 U
09:00	150 mg/dL	1 U
11:30	240 mg/dL (post-meal)	4 U
13:00	180 mg/dL	2 U

Eating habits, insulin sensitivity, work schedule, unique physiological response, etc.



ϵ

Privacy leakage through patterns from the sequence of pairs [44, 48].

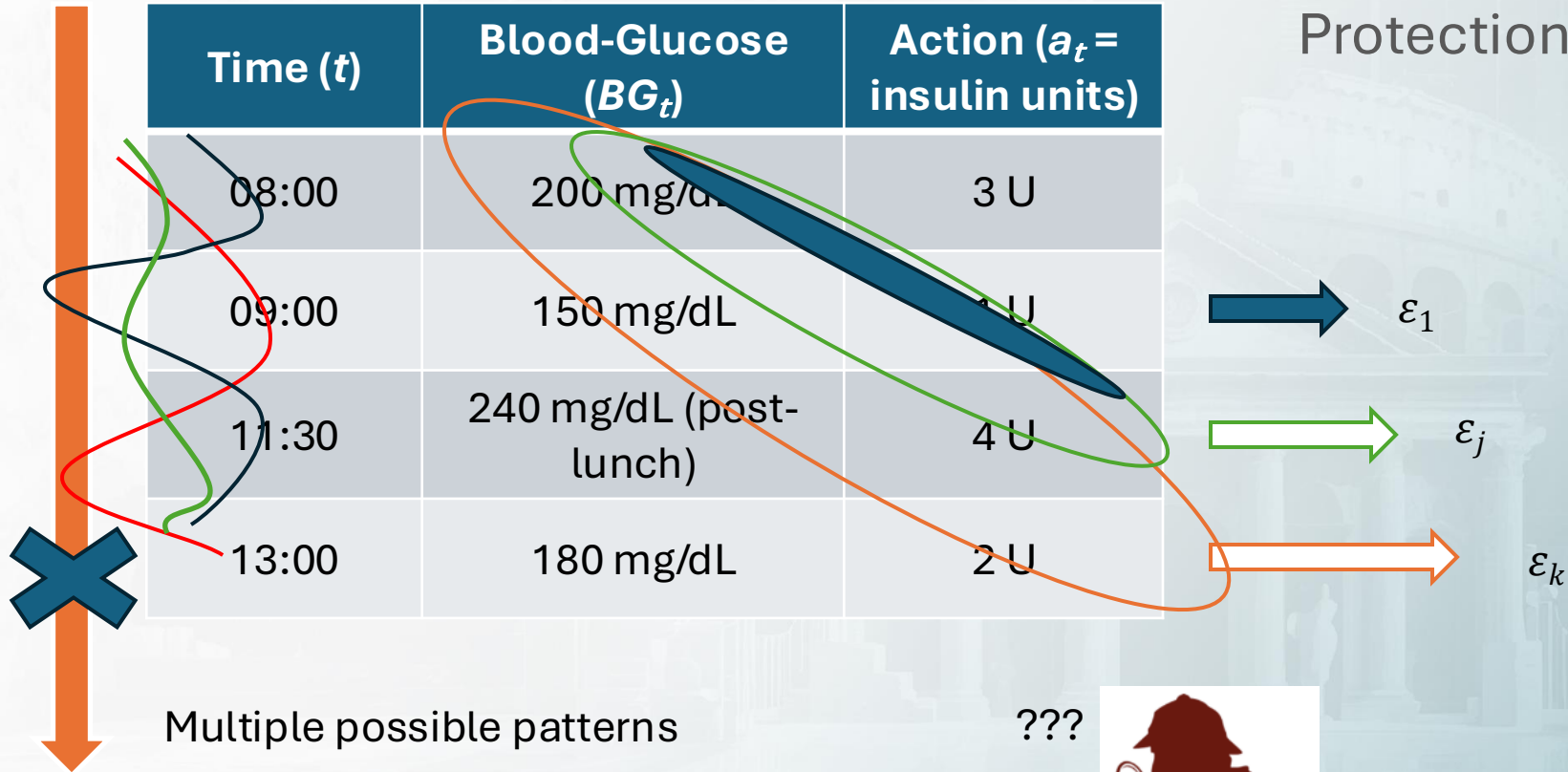
[44] X. Zhang, M. M. Khalili, and M. Liu, "Differentially private real-time release of sequential data," *ACM Transactions on Privacy and Security*, 2022.

[48]. I. Mironov, "R Lenyi Differential Privacy," in *IEEE Computer Security Foundations Symposium (CSF)*, 2017.



INTERNATIONAL JOINT CONFERENCE ON NEURAL NETWORKS
IJCNN2025
30 JUNE - 5 JULY 2025 | ROME, ITALY
INTERNATIONAL NEURAL NETWORK SOCIETY

Multi-scale Protection

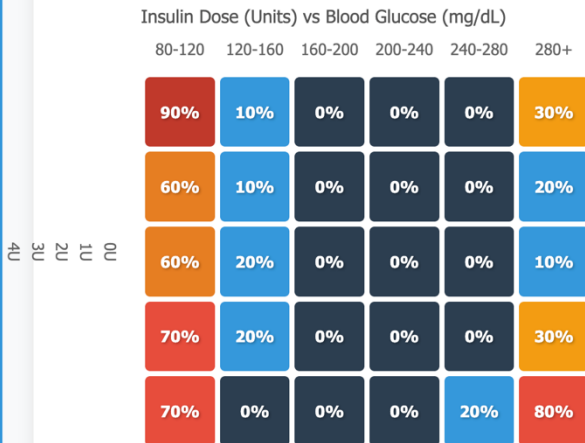


???

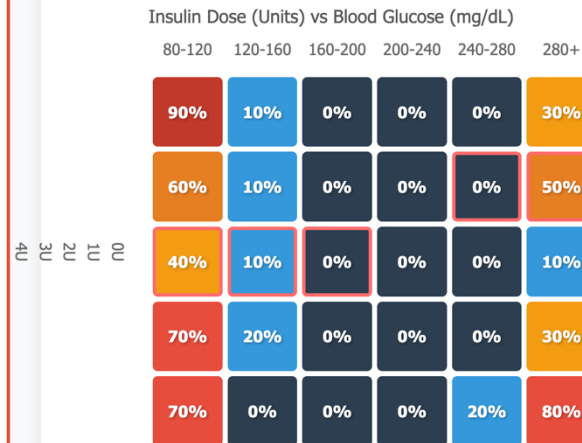


Behavioral Privacy

Policy Trained WITHOUT Patient A



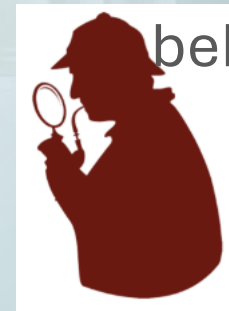
Policy Trained WITH Patient A



Privacy itself is a privacy vulnerability

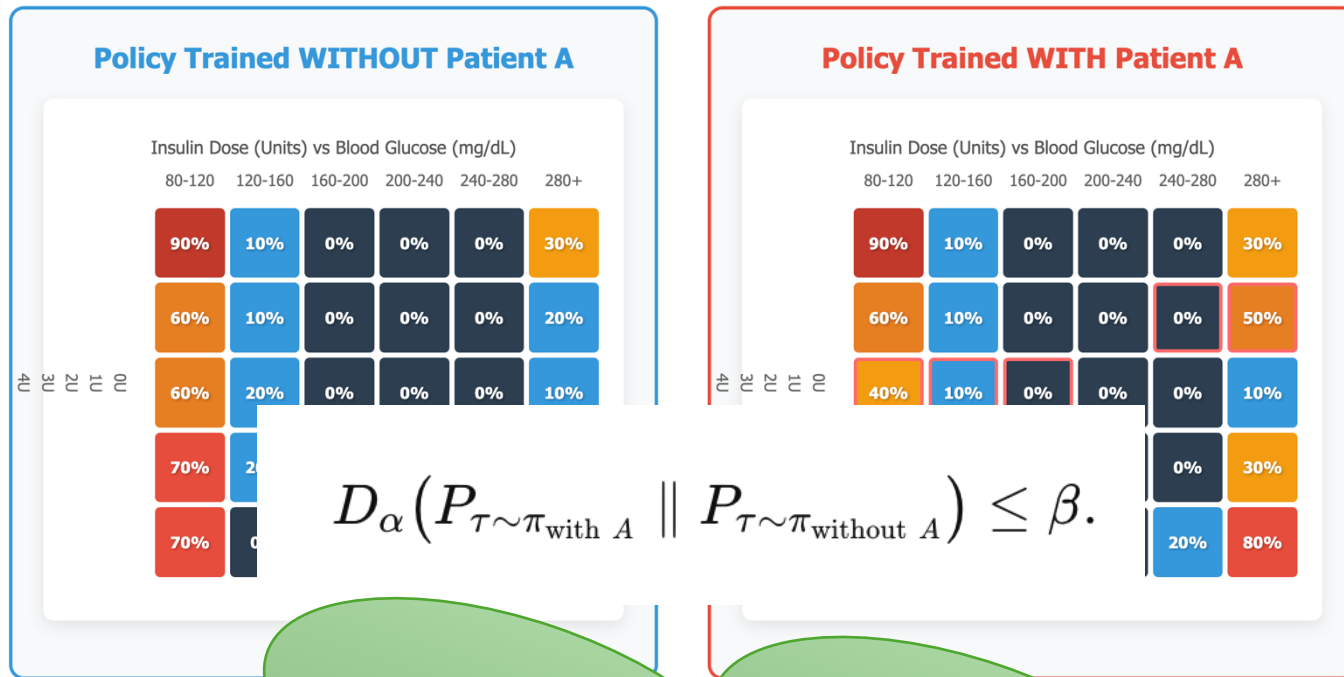
- Treatment protocols
- Physiological response
- Patient demographics

Privacy leakage through policy's behavioral pattern [11]



[11] C. J. Cundy, R. Desai, and S. Ermon, "Privacy-constrained policies via mutual information regularized policy gradients," in AISTATS, 2024

Behavioral Pattern Protection



Similar distributions

???



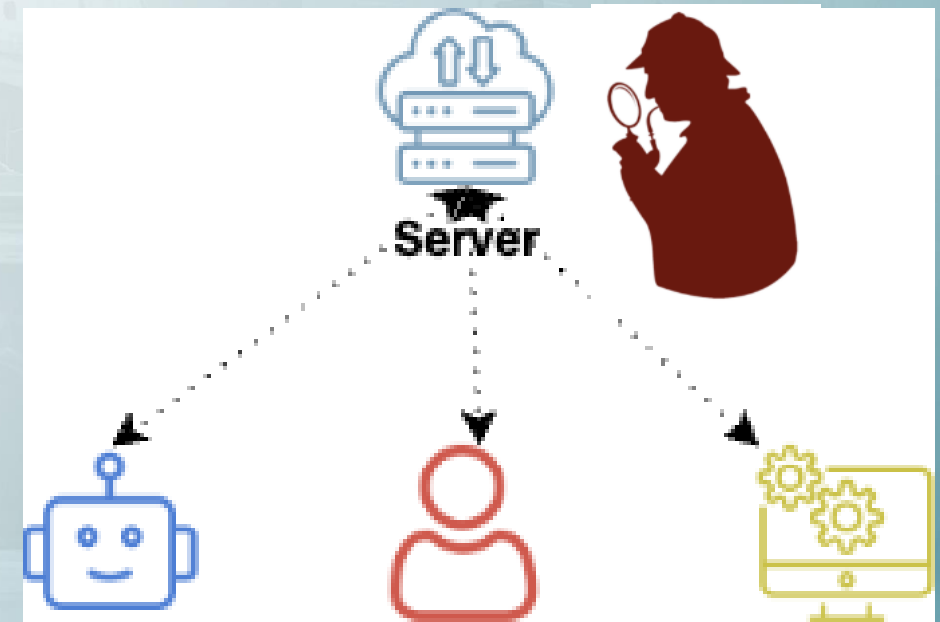
Collaborative Learning

Multi-agent systems are being deployed

Current solution:

Federated RL: Collaborative learning without transmitting RL trajectories

Global updates reveal sensitive information about individuals or institutions [42]

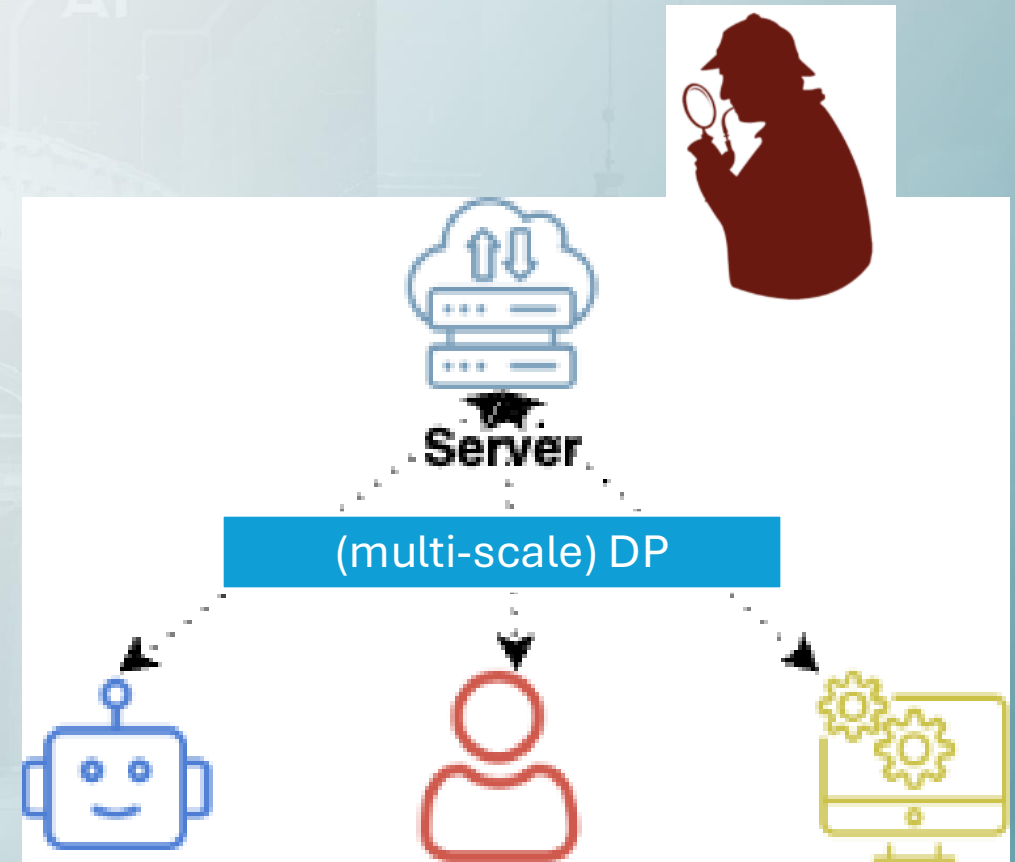


Collaborative Privacy protection

Potential directions:

- Apply multi-scale DP on the gradients
 - Prevent adversaries from identifying individual agents
- Construct mutual-information bound
 - Ensure shared updates reveal minimal information about individual agents

Prevents from reverse-engineering individuals when observing global patterns



Context-Dependent Privacy Requirements



Healthcare Domain

HIPAA Compliance Requirements

- Strict privacy protection



Autonomous Vehicle Domain

Transportation Safety Standards

- Vehicle performance optimization
- Route efficiency requirements



Privacy in decision-making is not “one size fits all”.



Context-Aware Adaptation



Healthcare Domain

HIPAA Compliance Requirements

- Strict privacy protection

Privacy Requirement:  $\epsilon \leq 0.1$



Autonomous Vehicle Domain

Transportation Safety Standards

- Vehicle performance optimization
- Route efficiency requirements

Privacy Requirement:  $\epsilon \leq 2.0$



Rethinking Privacy in RL

Challenges in Sequential Decision-making

- Temporal Correlation
- Behavioral Policy
- Collaborative Learning
- Domain Dependence

Sequential Privacy Framework

- Multi-scale Privacy Protection
- Behavioral Pattern Protection
- Collaborative Privacy Preservation
- Context-Aware Adaptation

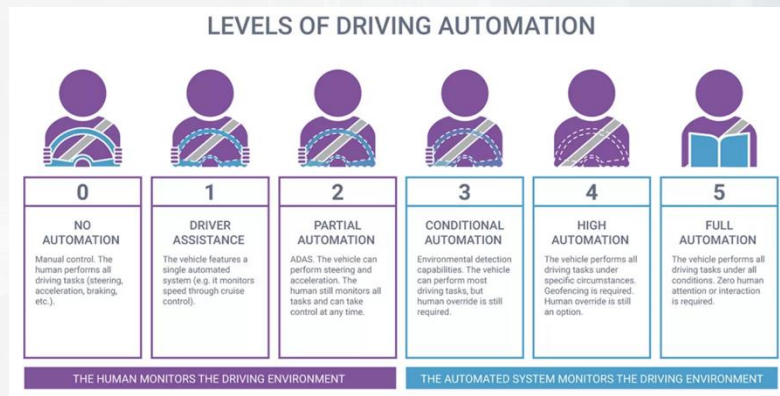


Image source: Synopsys blog

Analogy to Levels of Driving Automation

Principles for defining privacy protection in RL

Research Agenda – What We Need

Sequential Privacy

Theoretical Foundations

Mechanism Design

Implementation
& Deployment

Privacy
notions w.r.t
temporal
sequence

Privacy-utility
tradeoff
metrics

Adaptive
noise
injection

Policy-level
regularization

Benchmarks
& Tools





INTERNATIONAL JOINT CONFERENCE ON NEURAL NETWORKS

IJCNN2025

30 JUNE - 5 JULY 2025 | ROME, ITALY



INTERNATIONAL NEURAL NETWORK SOCIETY

Thank you

fxf@u.nus.edu

LET'S CONNECT



<https://flint-xf-fan.github.io/>