iapp



Proactive AI Privacy – Leveraging PETs throughout the AI life cycle

Monday, 9 November
08:00-09:00 PST
11:00-12:00 EST
16:00-17:00 CET

iapp LIVE WEB CONFERENCE

Proactive AI privacy

Leveraging PETs throughout the AI lifecycle

WEDNESDAY
9 NOVEMBER
11:00–12:00 EST
08:00–09:00 PST
16:00–17:00 CET

FEATURED SPEAKERS



Dylan Gilbert
Senior Fellow for Privacy Engineering
IAPP



David Buckley
Head of Partnerships
OpenMined



Julien Freudiger
Senior Staff Privacy
Google



Khaled El Emam
Director
Electronic Health Information Laboratory,
CHEO Research Institute

Session Outline

I. Why use PETs for AI?
II. How are PETs used in the AI lifecycle?
III. Deployment strategies and considerations
IV. What's next for PETs and AI?
V. Q&A

Why use PETs for AI?

Why Use PETs in the AI life cycle? Key PETs

Federated Learning

Decentralized Training | Computation goes to the data rather than data doing to a central server

Global Model Updates | Local model updates are combined into a single global model. Training continues iteratively

Synthetic Data

Statistical Fidelity | Data is generated with fidelity to the real data's patterns, correlations, and distributions

Scalability | Data can be generated at scale quickly and cheaply

Trusted Execution Environment

Confidentiality | Data processing in cordoned off memory region; even privileged software can't read or modify

Integrity | Attempts to tamper with data fail or are detectable

Remote Attestation | Cryptographically signed evidence of hardware and software integrity

Differential Privacy

Output Privacy | Rigorous output privacy guarantees through addition of random noise to the process of output data generation

How are PETs used in the AI life cycle?

Deployment strategies and considerations

What's next for PETs and AI?

Audience Q&A