



Privacy to a “TEE” – Secure data collaboration and confidential computing

Tuesday, 13 October

08:00-09:00 PST

11:00-12:00 EST

17:00-18:00 CET





Privacy to a “TEE” – Secure data collaboration and confidential computing

Tuesday, 13 October

08:00-09:00 PDT 11:00-12:00 EDT 17:00-18:00 CEST



Dylan Gilbert

Senior Fellow for
Privacy Engineering

IAPP



Lynne Penberthy

Director, Surveillance
Research Program

National Cancer Institute



Rina Shainski

Co-Founder and
Chairwoman

Duality Technologies



Timon Van Overveldt

Senior Staff Software
Engineer

Google

Session Outline

- I. What is secure computation?**
- II. Why secure computation now?**
- III. How is secure computation being used?**
- IV. What does the future hold?**
- V. Q&A**

What is secure computation?

Key PETs for Data Collaboration and Secure Computation

Trusted Execution Environment

Confidentiality

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

Trust in Hardware | Hardware enclave is trusted to isolate workloads and data; data is decrypted inside the enclave only during compute

Secure Multiparty Computation

Input Privacy | No party learns about another's inputs beyond what can be inferred from output

Collaborative Computation | Multiple parties jointly compute to get a shared result without pooling raw data

Distributed Trust | No single party is trusted with sensitive data; but all parties are trusted to perform the compute correctly

Constraints | All collaborating parties must be online during compute

Homomorphic Encryption

Computation on Encrypted Data | Privacy and security for data in use; information is never decrypted while being processed

Outsourcing Trust | A third party is not entrusted with sensitive data but is trusted to perform the compute correctly

Why secure computation now?

How is secure computation being used?

How is secure computation being used?

Use case	Examples	Privacy-enhancing technologies
User data analysis	Generating provably private insights into AI use	TEE Differential Privacy Federated Analytics/Learning
Data analysis across departments	Public health cost analysis Welfare and housing policy optimization Skill development and workforce readiness	TEE Fully Homomorphic Encryption
Collaborative data analysis across borders	International cancer research collaboration	TEE Federated Query Differential Privacy

What does the future hold?

Audience Q&A

Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: <https://iappwf.questionpro.com/t/AbBPvZ913S>

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

**For questions on this or other IAPP Web Conferences
or recordings please contact:**

livewebconteam@iapp.org