TRUstworthy Multi-site Privacy Enhancing Technologies

TRUMPET partners organize Special Session on security and privacy challenges in Federated Learning at IH&MMSec'24

In June next year, from the 24th to the 26th, a gathering for researchers involved in Artificial Intelligence studies will take place

The TRUMPET project is thrilled to announce a Special Session on "Security and Privacy Challenges towards Trustworthy Federated Learning" at the **12th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'24**), scheduled to take place from **June 24-26, 2024, in Baiona, Spain**. The special session aims to foster collaborations among researchers working on distributed machine learning and information security. It addresses the escalating security and privacy challenges in Federated Learning, where accessing and collecting data from diverse sources poses logistical and legal hurdles.

TRUMPET project invites all researchers interested in the field to submit conference papers

The special session opens the possibility **to submit conference papers**, an opportunity for all those researchers and institution that are contributing to the innovation **in artificial intelligence field.** The organizers invite **submissions that explore robust architectures for federated learning**, tools to measure and mitigate risks, and privacy-preserving techniques for training and inference across multiple parties. Topics include privacy and security attacks against machine learning, estimation of privacy leakage and security risks, novel defenses in machine learning against privacy attacks, privacy-preserving techniques, defense mechanisms for robust federated learning, tradeoffs between privacy, security, and efficiency, fairness, accountability, transparency, and ethics, challenges of federated learning deployment, hardware support, and case studies.

How to participate to IH&MMSec'24

Papers will undergo the standard review procedure of IH&MMSec'24 and must adhere to the formatting instructions specified in the workshop Call for Papers. Submission will be handled through EasyChair, where authors must select the corresponding track - "Special Session on Security and Privacy Challenges towards Trustworthy Federated Learning."

Important Dates:

- January 12, 2024: Submission system (EasyChair) opens.
- February 16, 2024: Paper submission deadline.
- April 12, 2024: Acceptance notification.
- May 3, 2024: Camera-ready submission is due.
- June 24-26, 2024: In-person workshop meeting in Baiona.

For more information and updates, please visit the conference website https://www.ihmmsec.org/

Funded by the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038