Mayar Elfares
Contact: mayar.elfares@vis.uni-stuttgart.de

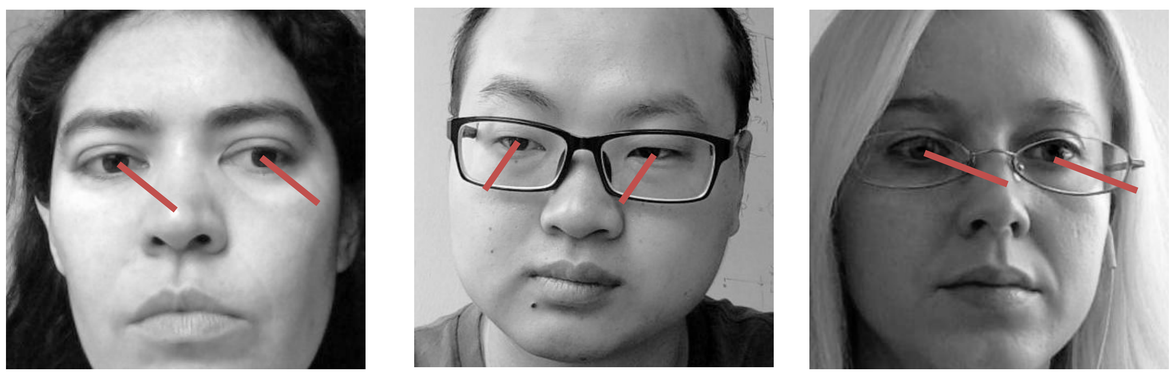
Privacy-preserving Attentive User Interfaces

Motivation

Computer vision and machine learning methods for gaze estimation, eye contact detection, and attention analysis have significantly matured and so have the capabilities of attentive user interfaces (AUI). This paves the way to develop robust collaborative model training while alleviating data-sharing concerns and providing security and privacy guarantees.

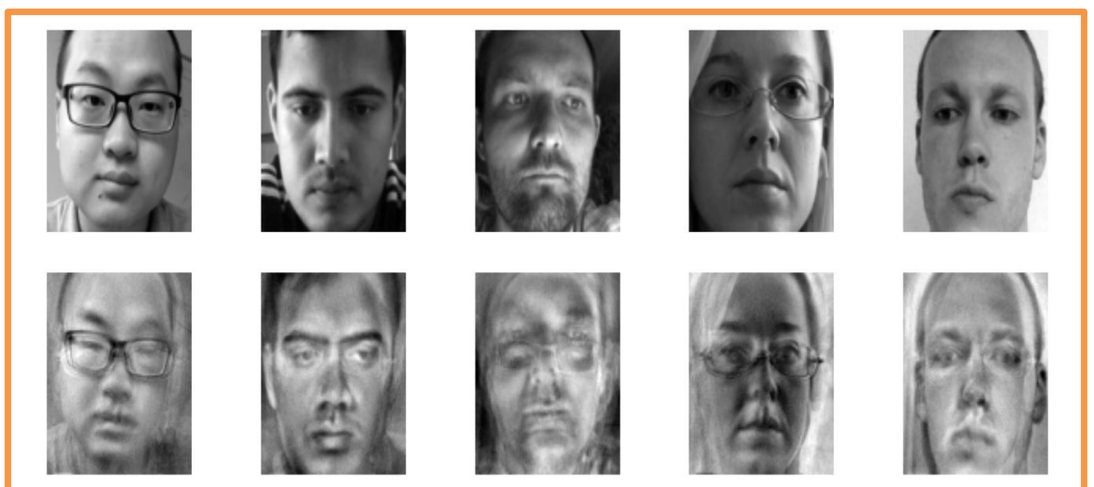
Gaze Estimation

Appearance-based gaze estimation [1] is a computer vision task that aims to predict either the 2D point of regard or the 3D gaze direction.



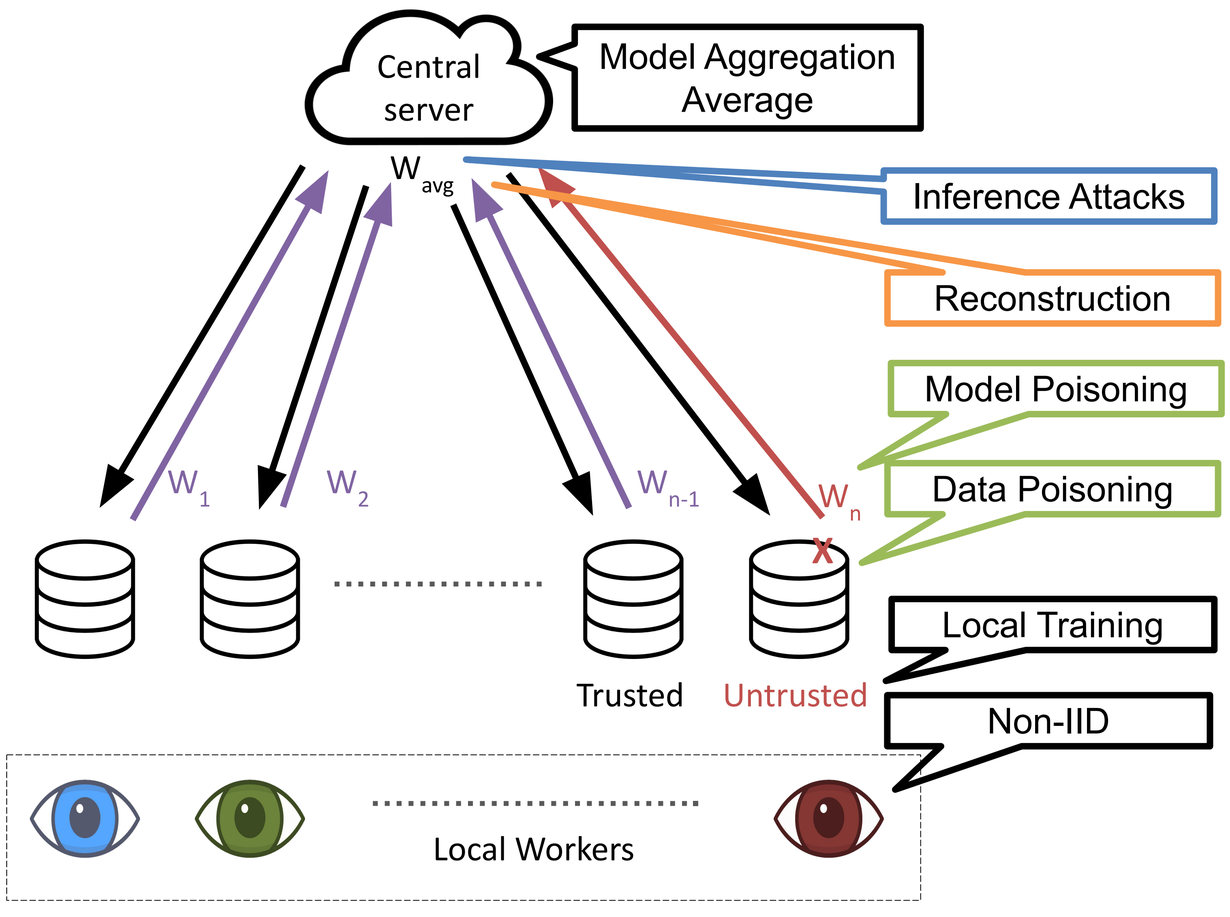
Attacks

Gaze data present several challenges. They are characterized by Non-IID (Non-Independent and Identically Distributed) features and are legally protected by different regulatory organizations.
Furthermore, the collection and exchange of gaze data over private and public networks introduce confidentiality, integrity, and availability problems, and dissipate the user's sovereignty over his/her data.
Moreover, by involving a large number of participants, the attackers' capabilities of poisoning the data, manipulating the updates, and influencing the model performance increase.



Privacy-Preserving Techniques

- **Federated Learning** [2]**:** To develop a **robust** gaze estimation algorithm with high generalization performance, a large dataset that handles the different real-life variations is required.
  - Client-server, horizontal, cross-device setup
- **Meta-Learning:** For **personalization**, meta-learning enables model adaptation.
  - non-IID (Non-Independent and Identically Distributed) data
- **SPDZ** [3]**:** To alleviate concerns of data sharing, **secure multi-Party computation** is used to train a **collaborative** model without compromising the user's privacy.
  - Dishonest majority, active security, pre-processing vs online phase



References

[1] Zhang, Xucong, et al. 2015. "Appearance-based gaze estimation in the wild."
[2] Konečný, Jakub, et al. 2016. "Federated learning: Strategies for improving communication efficiency."
[3] Damgård, Ivan, et al. 2012. "Multiparty computation from somewhat homomorphic encryption."

PUI Perceptual User Interfaces SEC AISA