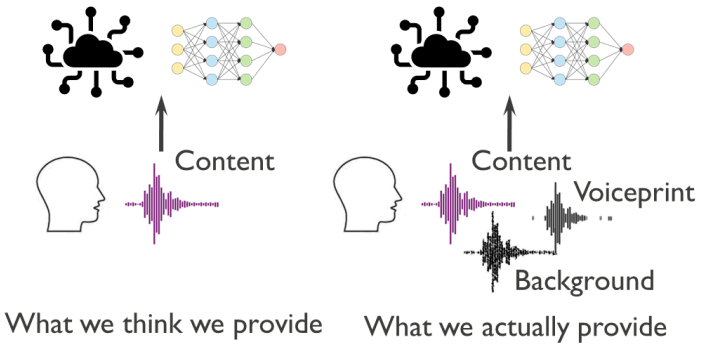
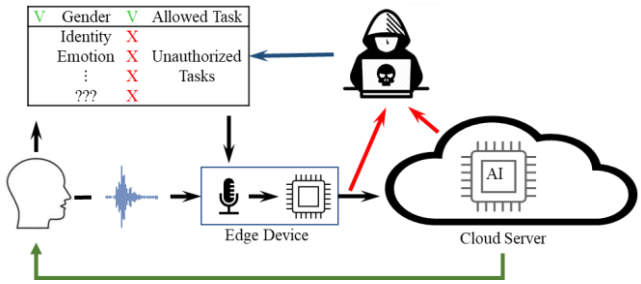
Privacy-Aware Audio Recognition

Wei-Cheng Wang, Pieter Simoens, Sam Leroux,
UGent, WeiCheng.Wang@UGent.be

We are giving away more data than we expected.

- Data may contain sensitive information.
- Data may be misused without authorization.



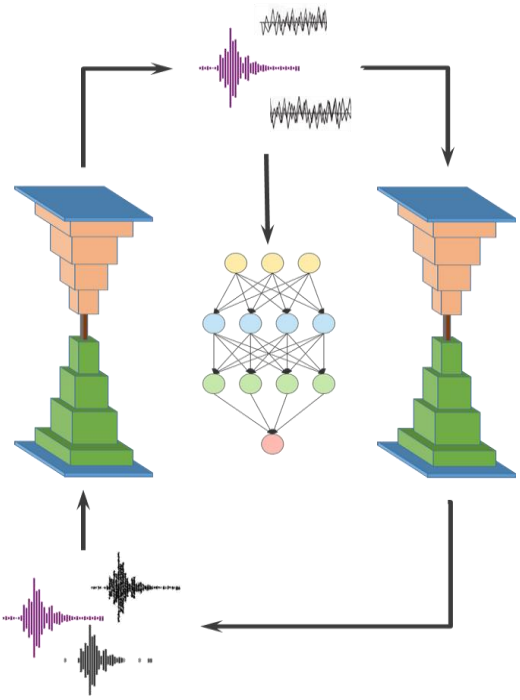


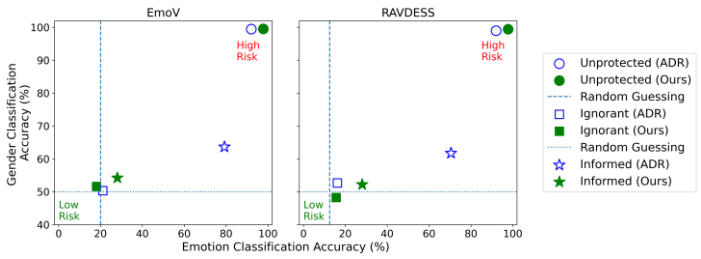
What can we do about it?

- Preprocess the data to constrain its usage on the target task.
- Ensure the preprocessed data can still do its work.

How can we do that?

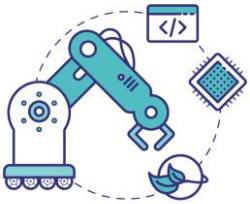
- An obfuscator that
  - Real-time processing on resources-constraint edge devices.
  - Obfuscates the data but maintain its performance on target task.
- A deobfuscator that
  - Serves as adversarial attack during training.
  - Ensures the obfuscated data has no extra information can be retrieved.





To make it even better

- Lighter, faster, more robust
- One model, customized privacy



AI FLANDERS
BUILDING OUR DIGITAL FUTURE
WWW.FLANDERSAIRESEARCH.BE
GHENT UNIVERSITY