cyberwatching.eu

The European watch on cybersecurity & privacy

Protecting privacy in the context of third party analytical services

Dr. Bridget Kane PhD
Karlstad University Sweden

Funded by the European Commission
Horizon 2020 – Grant # 740129

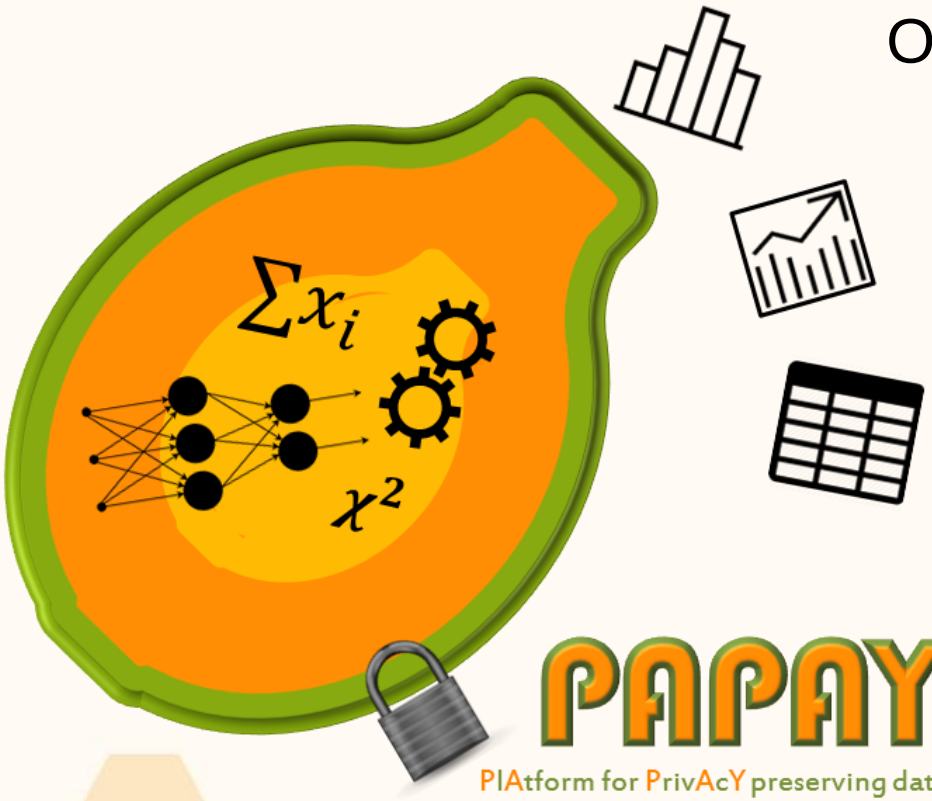
Data Analytics

- Data analytics can leverage collected data and derive relevant information that provides valuable knowledge to companies
- Processed data are often highly sensitive
- Disclosure may harm individual privacy
- GDPR obligates companies to protect individuals' data privacy while processing

Solution

- Privacy preserving data analytics modules that can extract analytics on protected data using artificial intelligence
- Protects individual privacy
- Cost-effective
- Accurate

PAPAYA



Objectives

- Privacy by design
  - PP analytics: processing over protected data
- Different settings
  - Single vs multiple DOs
  - Third party queriers
- Integrated platform
  - Common framework
- User control
  - Transparency, usability & auditability

5

GDPR

- Explicit Consent
  Data subjects can give or withdraw consent

- Security measures
  PETs used to extract analytics from Data

- Transparency
  Data subjects can visualise their disclosed data and their rights

- Auditability
  Data controllers can visualise audit logs and manage DPIA

Use Case examples

PAPAYA

- *Cloud service providing analysis of data*
- *Through third party*

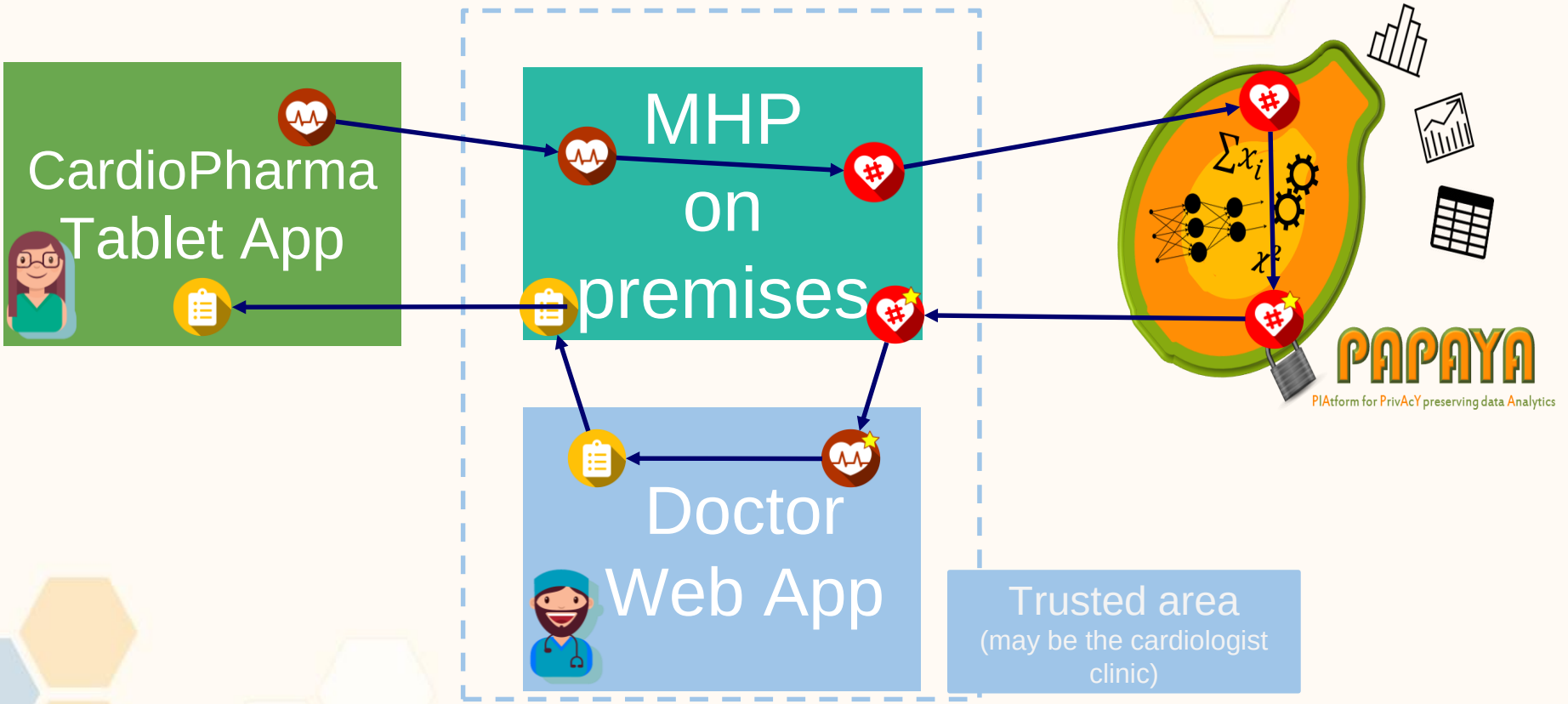
- *Example:*

Doctor provides patient with device to gather data

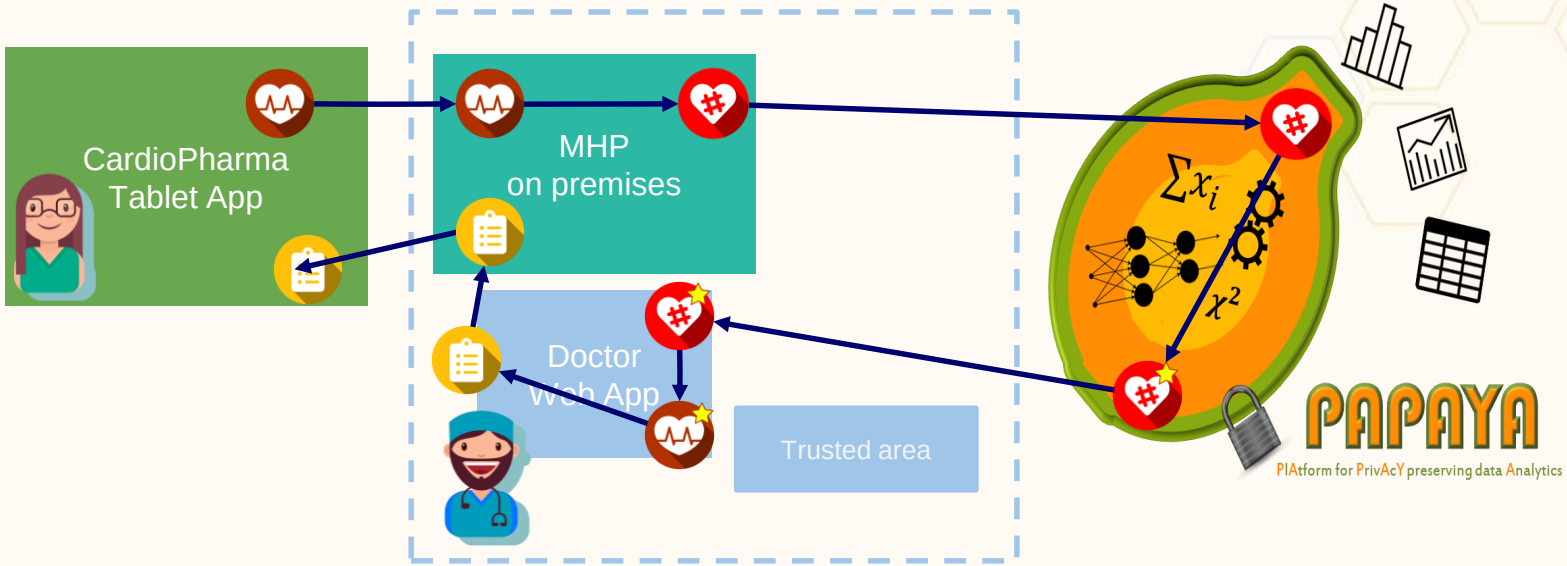
Data sent to Cloud service for analysis

Report sent back to Doctor (+/- patient)

Arrhythmia detection with Neural Networks



Arrhythmia detection with Neural Networks



Advantages:

- Data subject's privacy is preserved
- Computational burden is with Data Processors

PAPAYA

- *Cloud service providing analysis of data*
- *Through third party*

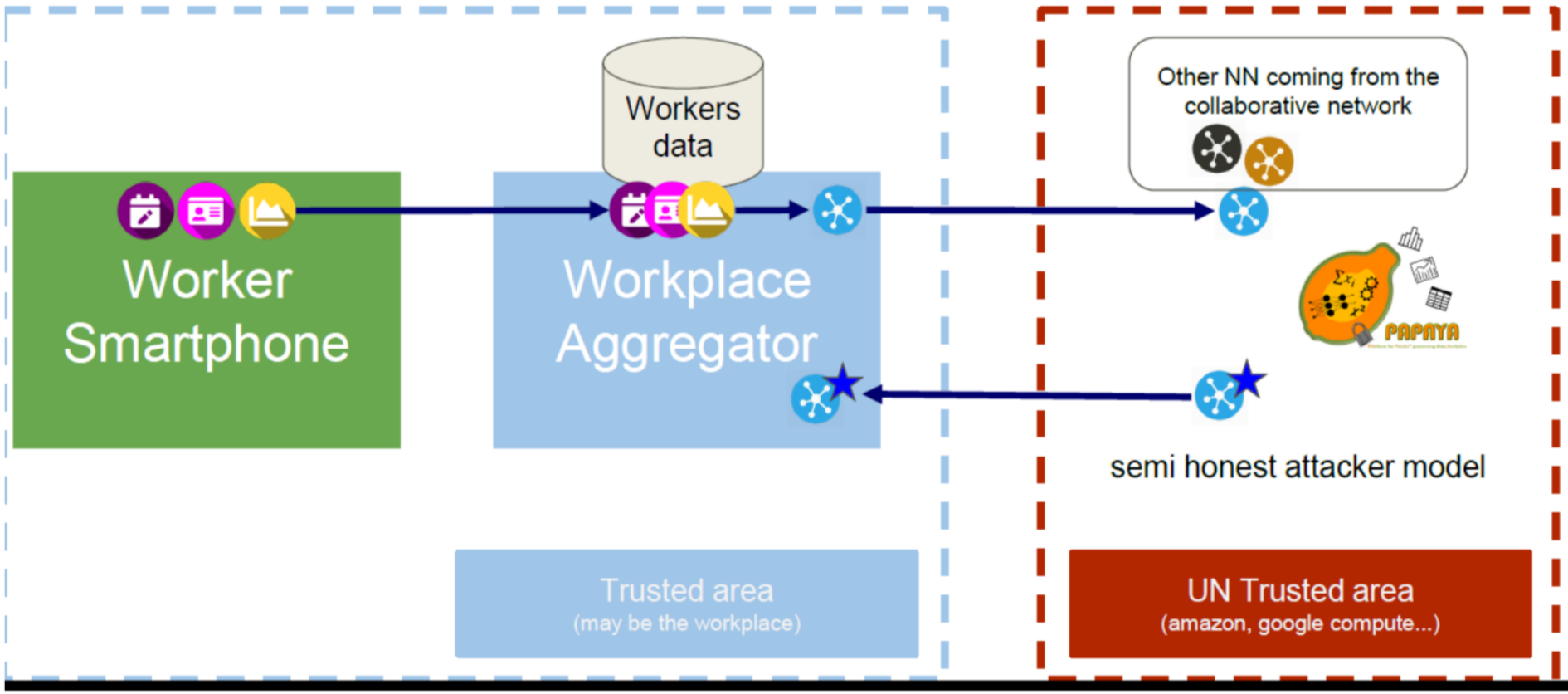
- *Example:*

Company provides staff with wearable device to gather data about stress

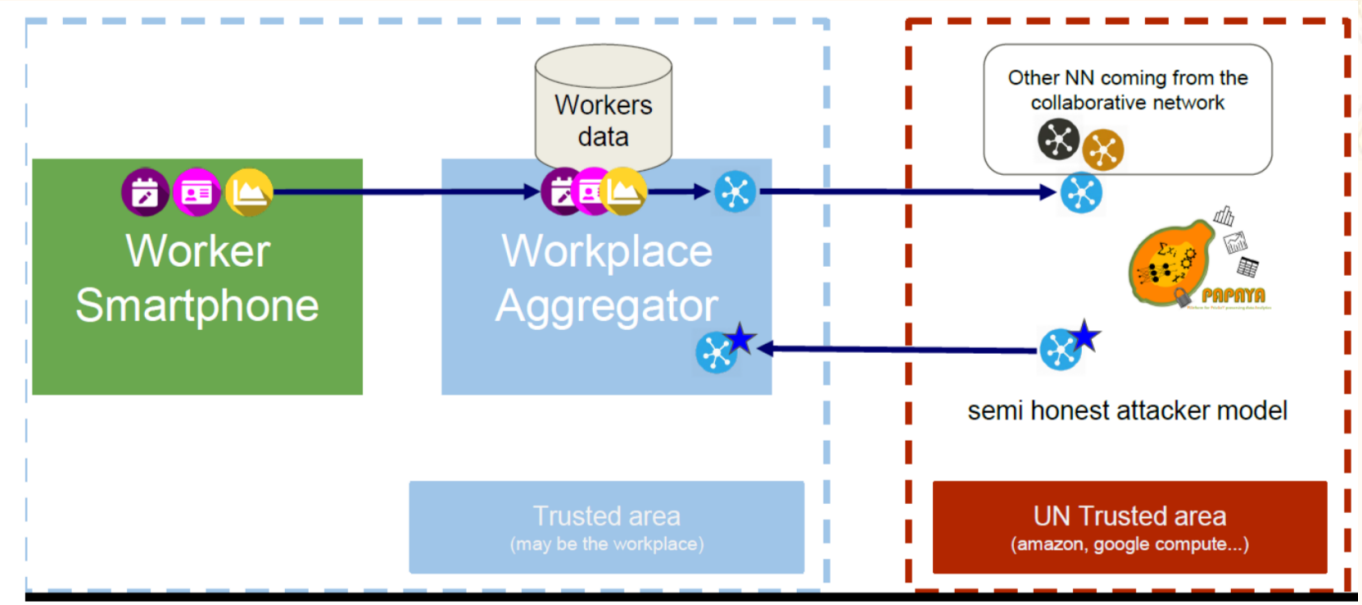
Data sent to Cloud service for analysis

Report sent back to Company (+/- staff)

Stress - Multiple Data Owners



Stress - Multiple Data Owners



<u>Advantages</u>:

- Data subject's privacy is preserved
- Better models are built on large datasets

Papaya

- *Healthcare has experience of protecting patient privacy and ethics*
- *Experience is largely paper based*
- *Privacy (in the past) protected by physical boundaries & local authentication*
- *Medical staff are not so knowledgeable about risks to patient data online*
- *Assume trust in service*
- *Assume accuracy of services*
- *Patients trust their doctors, & Organisations*

Papaya

Who is responsible for protecting patient data?

- *Doctor has professional responsibility*
- *Healthcare organisation has legal responsibility to ensure systems are in place*
  - *Various interpretations and practices*

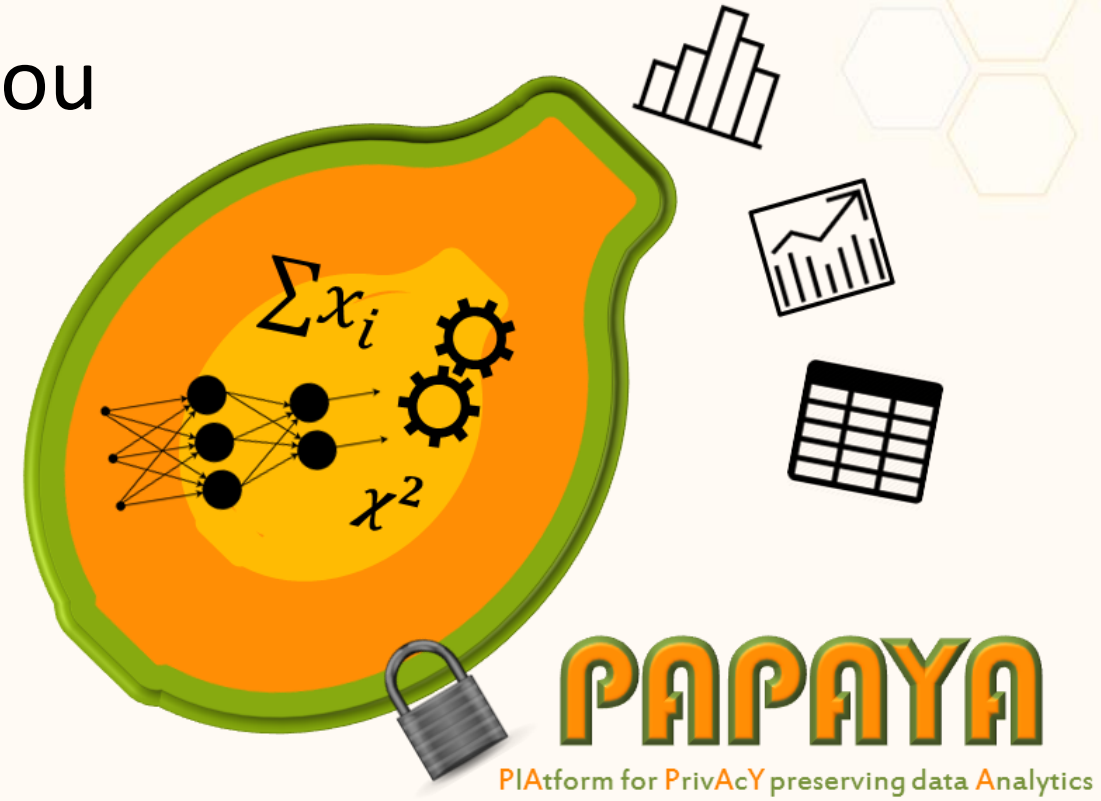
    Some use Cloud services; others don't
- *Doctors rely on organisation*
- *Patients rely on the HC professional*

  Often 'personal' relationship between Dr and patient

Papaya

- *Third party Service provider (SP) must deliver accurate service*
- *SP must provide security & protect privacy*
- ***TRUST and Integrity** is essential*
- *Informed Consent is concern for designers*

- Thank you


$\sum x_i$
x^2
PAPAYA
PlAtform for PrivAcY preserving data Analytics