NGI

Partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet

Webinar, 26 March 2021

NGI TRUST

Webinar – Agenda

Timing	Topic
10:30 – 10:40	Welcome *Jean-Luc Dorel, DG Connect, European Commission*
10:40 – 10:50	Introduction *Alasdair Reid, NGI Trust coordinator, EFIS Centre*
10:50 – 11:40	NGI_Trust Funded projects results *NGI_Trust Project managers*
11:40 – 11:55	Round table discussion and exchange - Q&A *All*
11:55 – 12:00	Wrap-up and close

NGI TRUST

Welcome and Introduction: NGI TRUST in a snapshot

Jean-Luc Dorel, DG Connect & Alasdair Reid, EFIS Centre

Project partners

EFIS

Fraunhofer IAO

GÉANT Networks • Services • People

tecnalia Inspiring Business

ebn innovation network

kantara INITIATIVE EUROPE

Key facts & figures

- Duration: December 2018 - November 2021
- 3 open calls :
  - 300 applications;
  - 448 applicants;
  - 36 countries.
- 3rd party funding: €5.6m:
  - 57 funded projects;
  - 84 funded third parties;
  - 20 countries.

NGI TRUST

NGI TRUST objectives

1. Reinforce, structure and develop the community of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies
2. Build on the state of the art in privacy and trust enhancing technologies by focusing support for third-party projects in a limited number of priority topics
3. Improve user trust and acceptance of emerging technologies by focusing on applications and solutions that develop a more open, robust and dependable Internet and strengthen Internet Governance
4. Foster the exploitation and commercialisation of the results of selected third-party projects through a tailored process of coaching and mentoring

NGI TRUST

NGI TRUST

57 PROJECTS FUNDED
12 THEMATIC AREAS

BEYOND PASSWORDS

BETTER PRIVACY

SAFER BROWSING

USER CONTROL

IMPACT OF AI

HUMAN-CENTRIC INTERNET

STRONGER TOOLS

EFFECTIVE IDENTITY

PERSONAL DATA MANAGEMENT

DATA ETHICS

SECURING THE INTERNET OF THINGS

ADVANCING IDENTITY

NGI TRUST Funded projects results

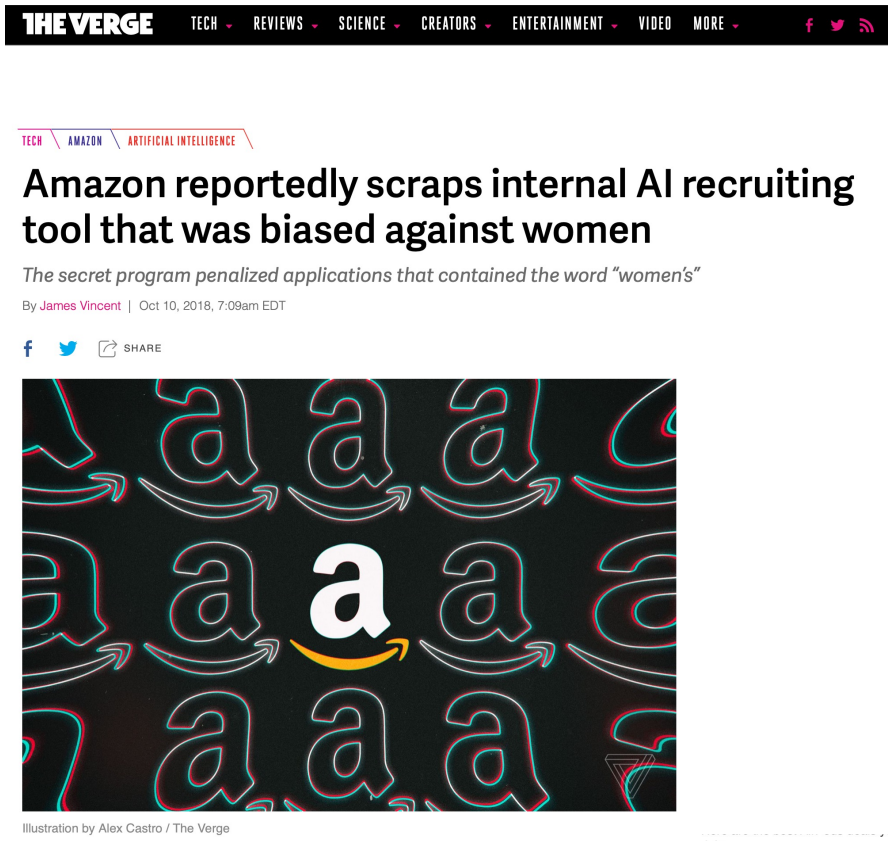
Project	Third party
AMNESIA [Impact of AI]	ZenaByte *Carlo Dambra*
COSCA [Impact of AI]	Università degli Studi di Catania *Giampaolo Bella*
FAIR AI [Impact of AI]	University of Cambridge *Ahmed Izzidien*
IZI [Impact of AI]	University of Jyväskylä *Mikhail Zolotukhin*
SePriCe [Impact of AI]	University of Jyväskylä *Andrei Costin*
TRUSTRULES [Impact of AI]	KAI SYNERGATES IKE (ASN) *Grigoris Nikolaou*

NGI TRUST

AMNESIA

ZenaByte – Carlo Dambra

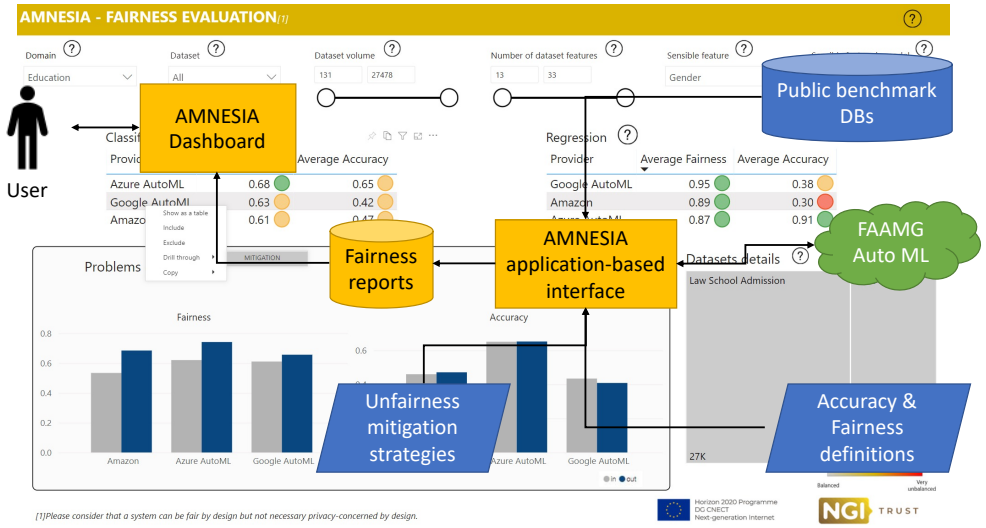
AMNESIA objectives & contributions

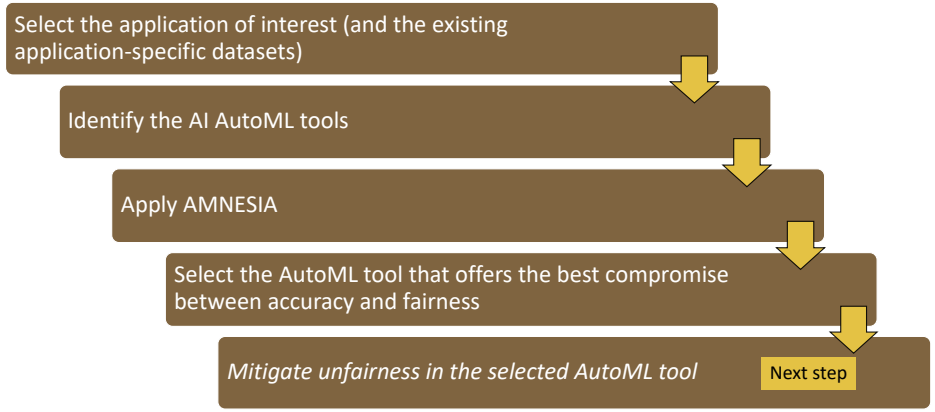


- AMNESIA objectives
  - to assess the fairness of AI-based AutoML tools and models available from FAAMG
  - to suggest mitigating actions of detected unfair behaviours
- AMNESIA target
  - individuals and companies with little to no AI skills that are looking to employ the AI technology in their decision-making processes

AMNESIA results & next steps

AMNESIA





- AMNESIA has implemented at TRL 4
  - the tool to assess the fairness of AutoML tools
  - a dashboard to visualise results
  - the mitigation options
- AMNESIA next steps
  - to reach TRL 7 with the current tool
  - to design & implement the mitigation tool
  - to disseminate the results
  - to start trials with clients

COSCA

University of Catania/CNR - Giampaolo Bella

COSCA project – Conceptualising Secure CArs

Modern cars treat a lot of data

1. Crowd-source drivers' privacy concerns and trust perceptions
2. Study manufacturers' privacy policies
3. Risk-assess car security and drivers' privacy
4. Conceptualise socio-technical measures up to UX

Main findings

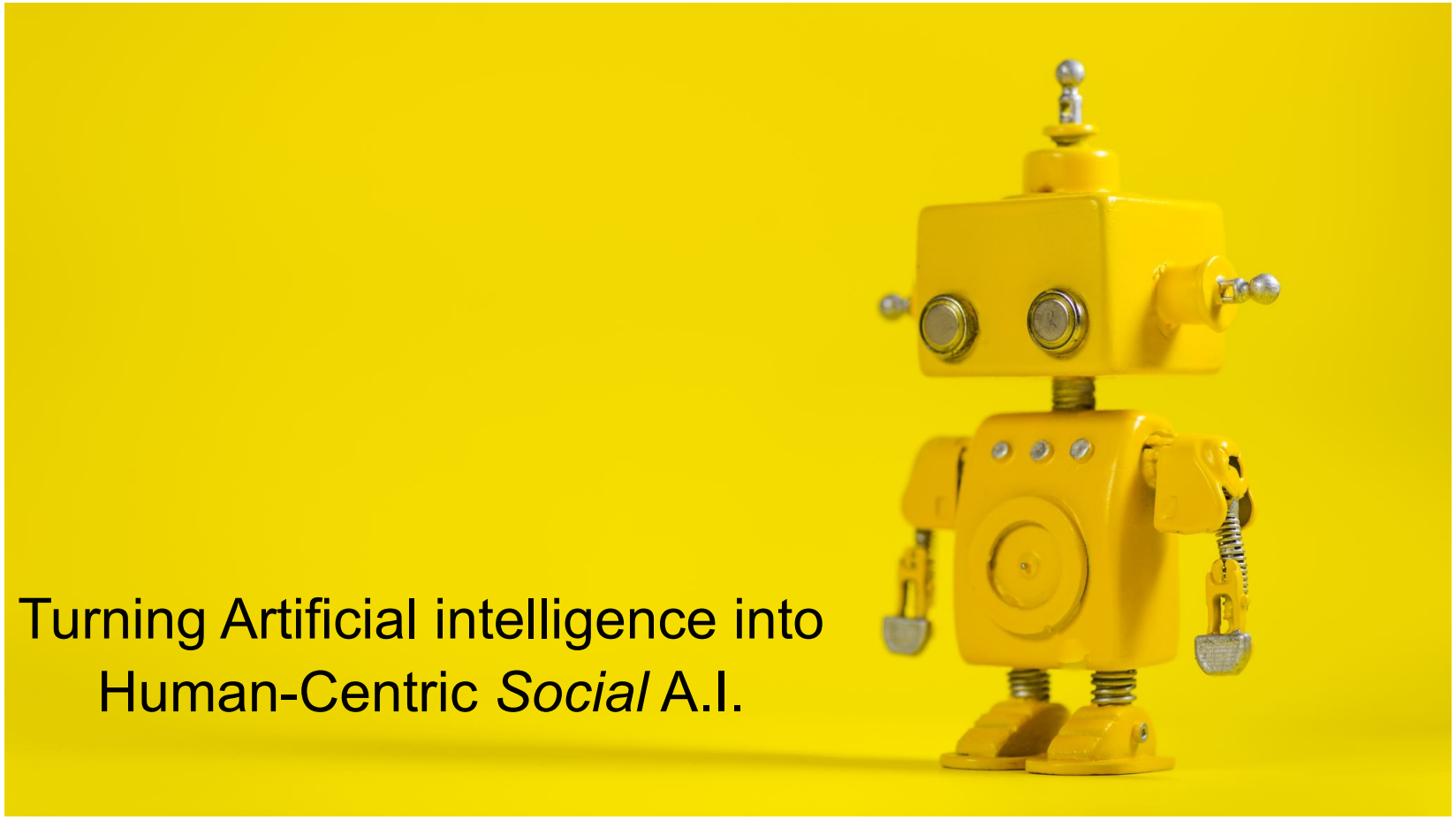
1. Low privacy concerns yet low trust perceptions: need awareness
2. Scant policies, underspecified measures, data inference untouched
3. User profiling is a risk, Tesla most data hungry
4. User groups into UX seem promising

AI 4 COSCA

- Adversarial driver profiling
- Ethical driver profiling to undestand errors and faults hence improve technical measures
- Ethical driver profiling to offer better-tailored UX
- Cue optimisation to transmit privacy policy
- Information and immersiveness increase to increase trust

FAIR AI

University of Cambridge – Ahmed Izzidien / David Stillwell



NGI TRUST

Research objectives

1. To allow AI to recognise principle components of social fairness in texts.

2. To use a cross-cultural definition of fairness.

3. To program an AI with this interface without the limitations of traditional methods (e.g., A.I. Deontic logic).

Results

Instead of programming **rules**, or a list of **Do's and Don'ts**, the research developed **a new theory** to capture human perception:

Allowing an **AI to reach explainable fairness conclusions by itself** using Word Embeddings, and a novel **Fairness Vector**

This research was accepted in a peer-review journal as a unique and successfully implemented method *Journal of Artificial Intelligence & Society Vol. 36, no. 2, Jun. 2021 (Springer Nature Publication)*

Impact

- This has now presented academia and industry with a new approach to analyse texts using social ontology concept triangulation. To develop flexible and context sensitive human-centric AI.
- A second paper was sent to the AAAI/ACM. Conference on AI, Ethics and Society, New York, NY, USA, 2021. The code for the research output is accessible through Github.

TEACHING AN AI FAIRNESS THROUGH CONCEPT RECOGNITION IN WORD EMBEDDINGS

Applications

Stage 1: Detecting harms in online texts.
Stage 2: Assigning legal Rights and Duties to individuals, institutions and states in texts (e.g., legislation & legal contracts).
Stage 3: Providing a new measure for industry.

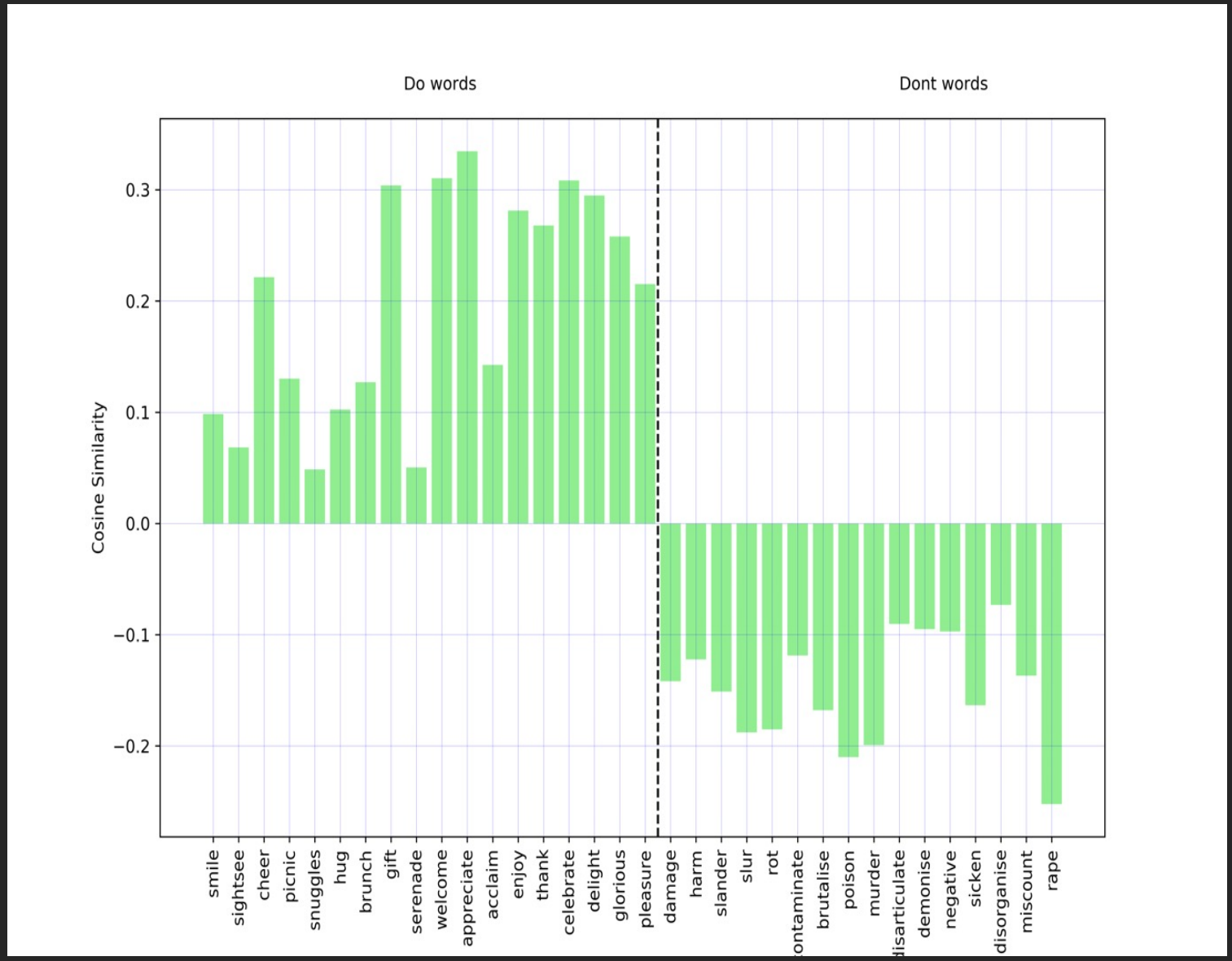


Fig. 1. Implementation of FairVec, without rules (Code available on Github)

IZI

University of Jyväskylä - Mikhail Zolotukhin

NGI TRUST

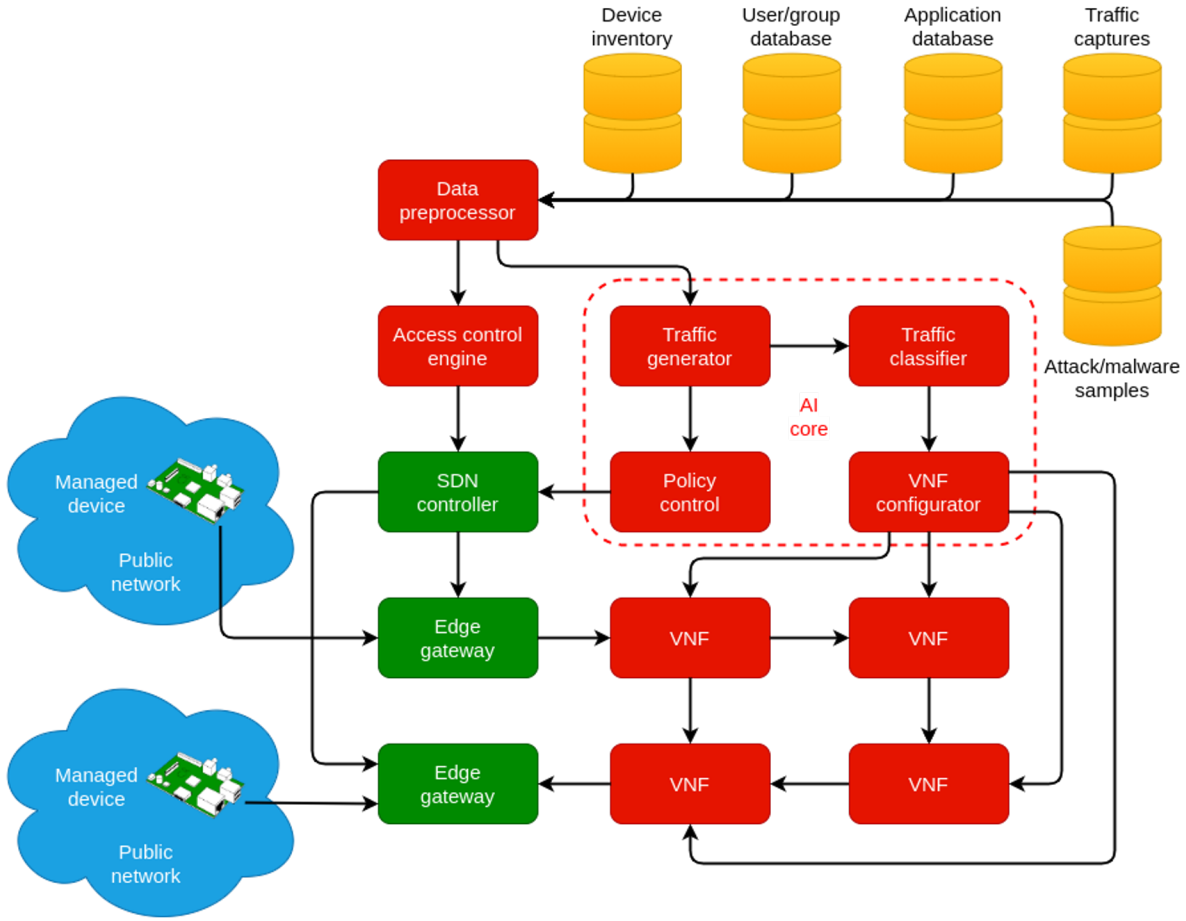
IZI: Intelligent Zero-Trust Network for IoT

Abstract:

The aim of this project is to develop a network defense system which relies on SDN and NFV technologies and state-of-art AI algorithms

Objectives:

- Investigate how recent advances in reinforcement machine learning can be employed in order to enhance network security mechanisms
- Implement a prototype of AI-driven IoT defense framework that satisfies zero-trust requirements
- Integrate and evaluate the prototype developed in a real production network environment



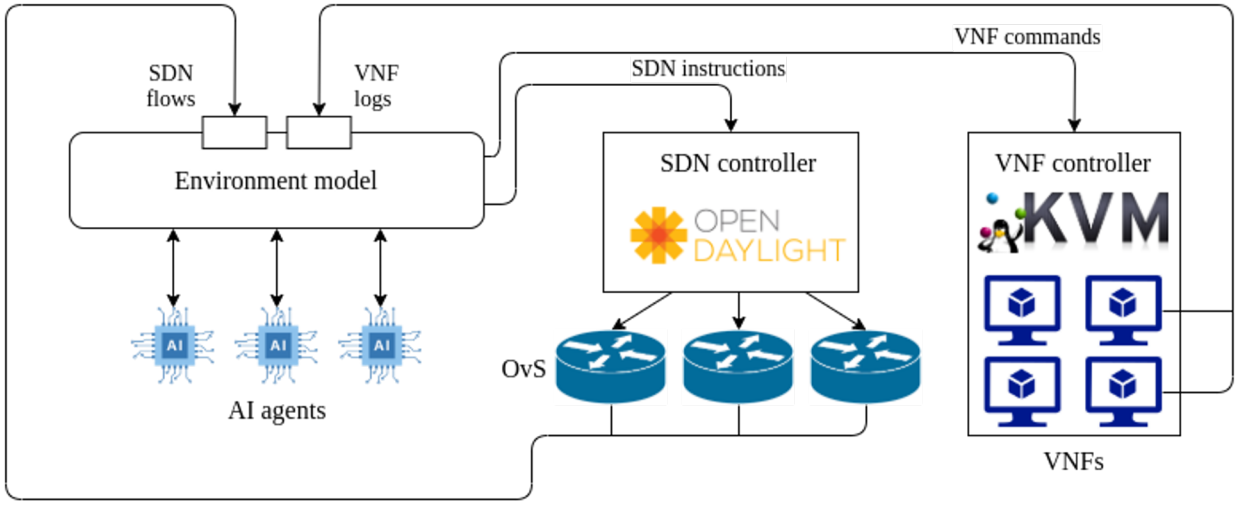
IZI: Intelligent Zero-Trust Network for IoT

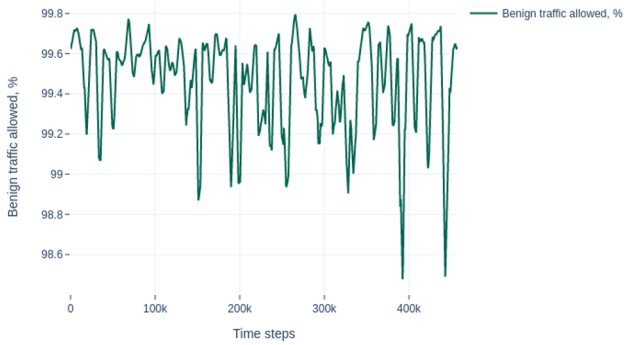
Results:

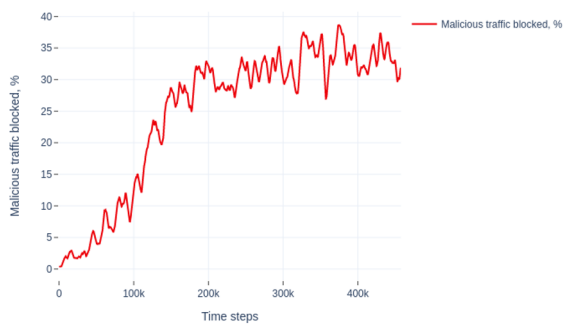
- A PoC of an intelligent network defense system which relies on SDN and NFV technologies and allows for detection and mitigation of attacks performed against their devices by letting an AI agent control network security policy

Future work:

- Train AI agents and test the prototype using IoT specific traffic
- Evaluate the prototype in our university lab network environment







SePriCe - Security, Privacy, Certification

University of Jyväskylä (Finland) - Andrei Costin

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Andrei Costin – ancostin@jyu.fi

IoT-SePriCe:
IoT Security, Privacy, Certification

NGI TRUST Open Call #2

University of Jyvaskyla (Finland)

Andrei Costin – ancostin@jyu.fi

Objectives and Contributions

- Objectives
  - Explore feasibility and challenges of automating IoT certifications (security)
  - Explore feasibility and challenges of automating IoT device decommissiong checks (privacy)
- Contributions
  - Advance R&D and technology state of the art
  - Proof-of-Concept (PoC) implementations demonstrating approaches and findings
  - Comprehensive analysis and reporting on state-of-play limitations

Horizon 2020 Programme
DG CNECT
Next-generation Internet

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

NGI TRUST

IoT-SePriCe:
IoT Security, Privacy, Certification

NGI TRUST Open Call #2

University of Jyvaskyla (Finland)

Andrei Costin – ancostin@jyu.fi

Results and Next Steps

- Now: Results
  - PoC certification automation
    - **ETSI 303 645, UL 2900, IoXt Alliance, IMDA TS RG-SEC, BSI TR-03148**
  - PoC decommissioning privacy automation
    - Multiple vulnerabilities discovered, e.g., PII & secrets leakage
- Next: Explore
  - Peer-review publication draft in-preparation
  - Implementation of new certification and decommisioning schemes/automations
  - Technology partnerships with www.binare.io / www.linkedin.com/company/binare/

Horizon 2020 Programme
DG CNECT
Next-generation Internet

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

NGI TRUST

Trusted AI for B2B services

NGI TRUST

Privacy by Design concept and Accountability

Motivation: demonstrate the benefits of AI for trade fair management, while preserving privacy

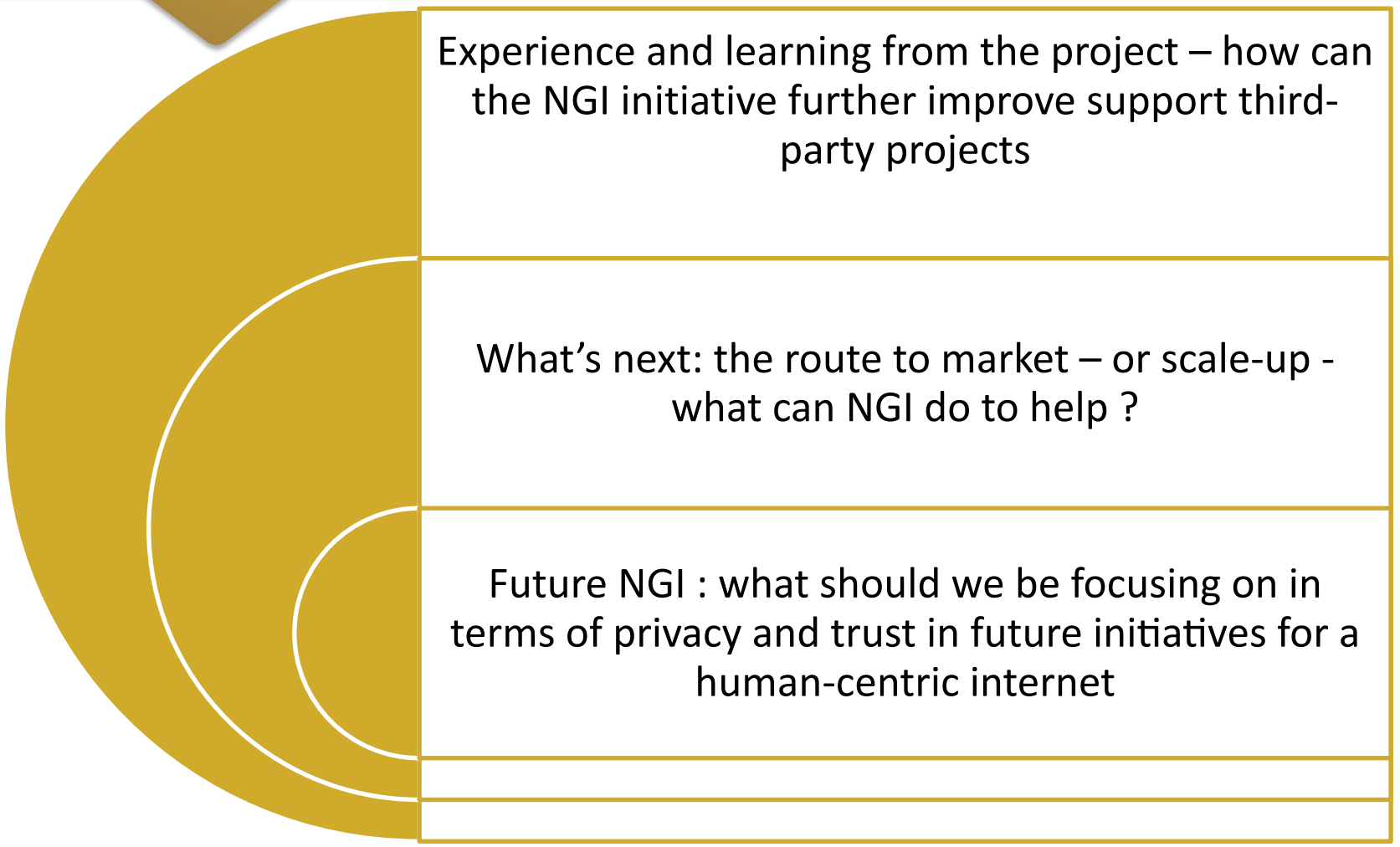
Results

- **Differential privacy**
  - Decentralized collaborative filtering and data obfuscation
  - Local differential privacy = noise is added to each individual data point in the dataset
  - Global differential privacy = noise is added at the output

- **Accountability through Explainable AI-based Matchmaking system**

  Techniques that were evaluated aiming to enhance AI system transparency and data privacy:
  - Local Interpretable Model agnostic Explanations (LIME)
  - Layerwise Relevance Propagation (LRP)
  - Deep Learning Important FeaTures (DeepLIFT)

Round table discussion and exchange - Q&A



NGI TRUST

More information/contact us

- Project coordinator : Mr Alasdair Reid @ EFIS Centre - www.efiscentre.eu
- Email : NGI-Trust-support@lists.geant.org
- Twitter: @NgiTrust
- NGI_TRUST wiki : https://wiki.geant.org/display/NGITrust
- NGI.eu website : https://www.ngi.eu/about/

The NGI_TRUST project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 825618