1 Minute Madness

Order of presentations:

1. Preventing EFail Attacks with Client-Side WebAssembly
2. Differential Privacy for Private Pattern Protection
3. SLASH: Serverless Apache Spark Hub (demo)
4. Pattern-Level Privacy in DCEP
5. Goodbye Engineered ANNs, Hello Evolutionary Neural Networks
6. ComDeX Unveiled Demonstrating the Future of IoT-Enhanced …
7. Practical Forecasting of Cryptocoins Timeseries using…
8. Thetacrypt: a distributed service for threshold cryptography…
9. No One Size (PPM) Fits All: Towards Privacy in Stream…
10. Cognitive Cyber Defense - Dynamic, Adaptive Cyber…
11. StreamToxWatch – Detector Architecture for Data Poisoning…
12. Handling Inconsistent Data in Industry 4.0
13. Privacy-preserving Transaction DAG
14. Decentralized Stream Reasoning Agents
15. Agent-based Orchestration on a Swarm of Edge Devices

Université de Neuchâtel

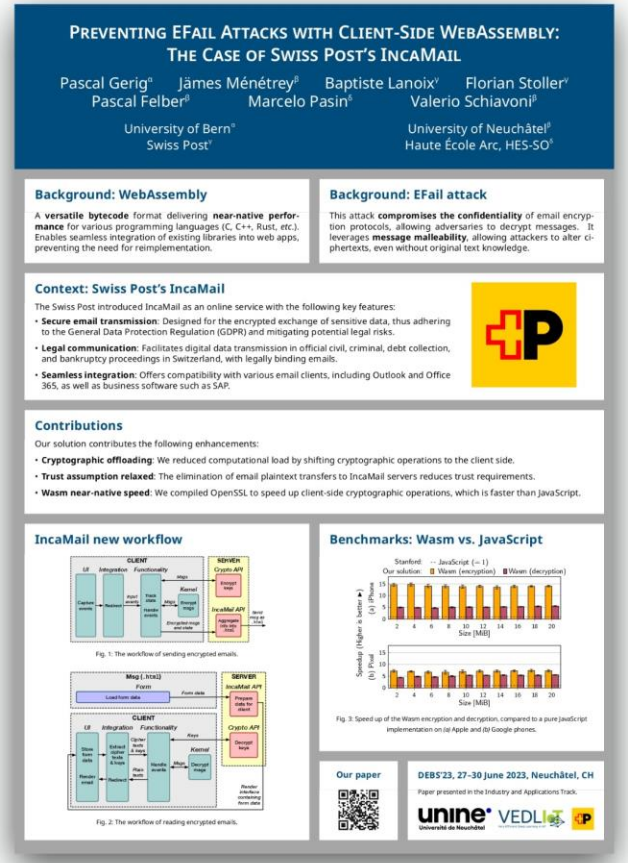
VEDLIoT
Very Efficient Deep Learning in IoT

🇨🇭 Ever wished to send **digitally secure**, **legally-binding** letters in Switzerland?

📪 Worked with **Swiss Post** to design a **better** secure email transmission platform

🚀 **Join us** to: discover how + see our performance results!

#WebAssembly #Cryptography #OpenSSL



PREVENTING EFAIL ATTACKS WITH CLIENT-SIDE WEBASSEMBLY: THE CASE OF SWISS POST'S INCAMAIL

Pascal Gerig[α] Jämes Ménétrey[β] Baptiste Lanoix[γ] Florian Stoller[α]
Pascal Felber[β] Marcelo Pasin[δ] Valerio Schiavoni[β]

University of Bern[α] Swiss Post[γ] University of Neuchâtel[β] Haute École Arc, HES-SO[δ]

Background: WebAssembly

A **versatile bytecode** format delivering **near-native performance** for various programming languages (C, C++, Rust, etc.). Enables seamless integration of existing libraries into web apps, preventing the need for reimplementation.

Background: EFail attack

This attack **compromises the confidentiality** of email encryption protocols, allowing adversaries to decrypt messages. It leverages **message malleability**, allowing attackers to alter ciphertexts, even without original text knowledge.

Context: Swiss Post's IncaMail

The Swiss Post introduced IncaMail as an online service with the following key features:

- **Secure email transmission**: Designed for the encrypted exchange of sensitive data, thus adhering to the General Data Protection Regulation (GDPR) and mitigating potential legal risks.
- **Legal communication**: Facilitates digital data transmission in official civil, criminal, debt collection, and bankruptcy proceedings in Switzerland, with legally binding emails.
- **Seamless integration**: Offers compatibility with various email clients, including Outlook and Office 365, as well as business software such as SAP.

Contributions

Our solution contributes the following enhancements:

- **Cryptographic offloading**: We reduced computational load by shifting cryptographic operations to the client side.
- **Trust assumption relaxed**: The elimination of email plaintext transfers to IncaMail servers reduces trust requirements.
- **Wasm near-native speed**: We compiled OpenSSL to speed up client-side cryptographic operations, which is faster than JavaScript.

IncaMail new workflow

Benchmarks: Wasm vs. JavaScript

Our paper

DEBS'23, 27–30 June 2023, Neuchâtel, CH

Paper presented in the Industry and Applications Track.

The Research Problem

trade-off

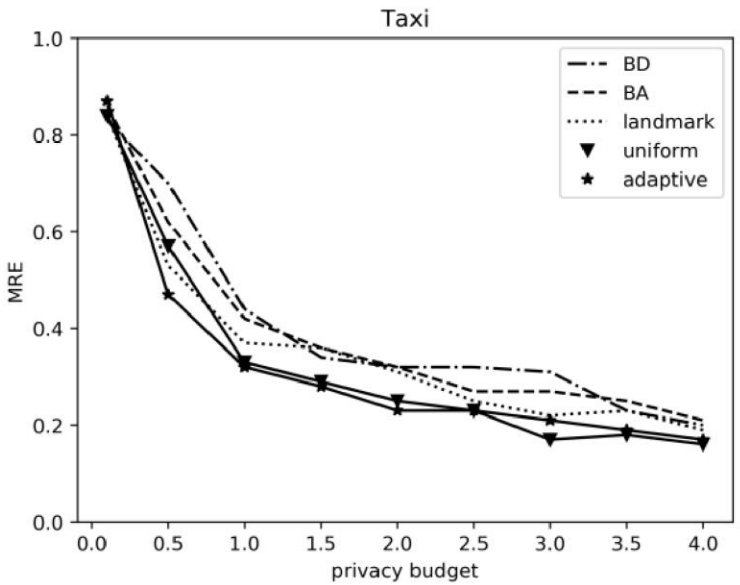
- protect **privacy protection** under a **required data utility** in **data streams**

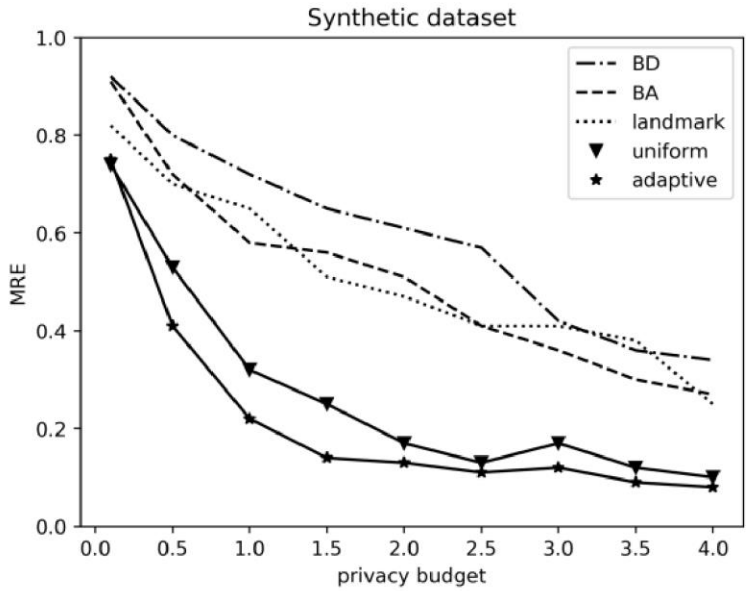
A few people have done something already, but not enough…

Contributions

- **break** the current performance **limitations** and **open up** a novel "level" of DP and PPMs

Early-stage verification results





Demo: SLASH: Serverless Apache Spark Hub

Zurich University of Applied Sciences
School of Engineering
InIT Institute of Applied Information Technology

How do you slash operating expenses (and footprint) of big data infrastructure?

With SLASH!

As easy as '`import slash`'.

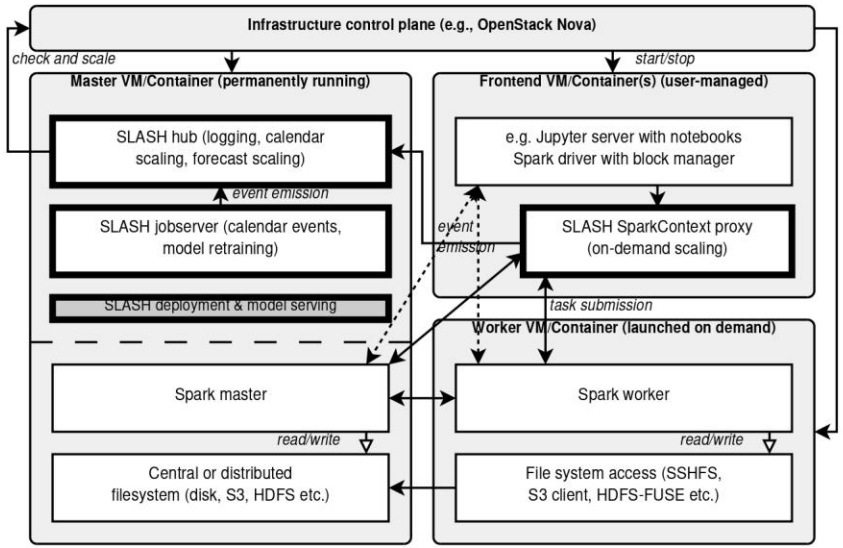
```
import sparky
import pyspark
import pyspark.sql

import slash

sc = sparky.connect("yourbigdatajob", 2)
spark = pyspark.sql.SparkSession.builder.getOrCreate()
```

```
# your custom code here...
#df = spark.createDataFrame([("x",), ("y",), ("z",)], ["reallybigdata"])
#df.show()
```

```
sc.stop()
```

SLASH is

- *Distributed across Spark topology*
- *Event-based from multiple sources*
  - *scheduled usage*
  - *application requests*
  - *forecasting*
- *Adaptive to application needs: local mode, immediate scaling, lazy scaling*



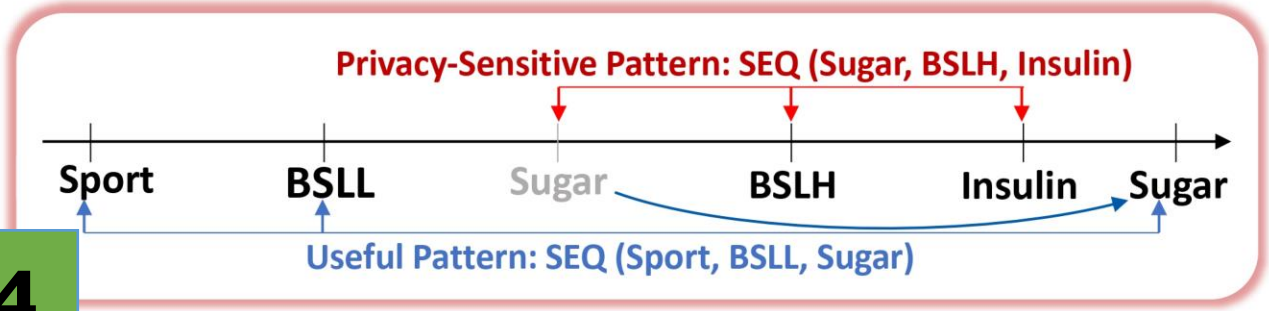
university of groningen

Pattern-Level Privacy in DCEP

Majid Lotfian Delouee

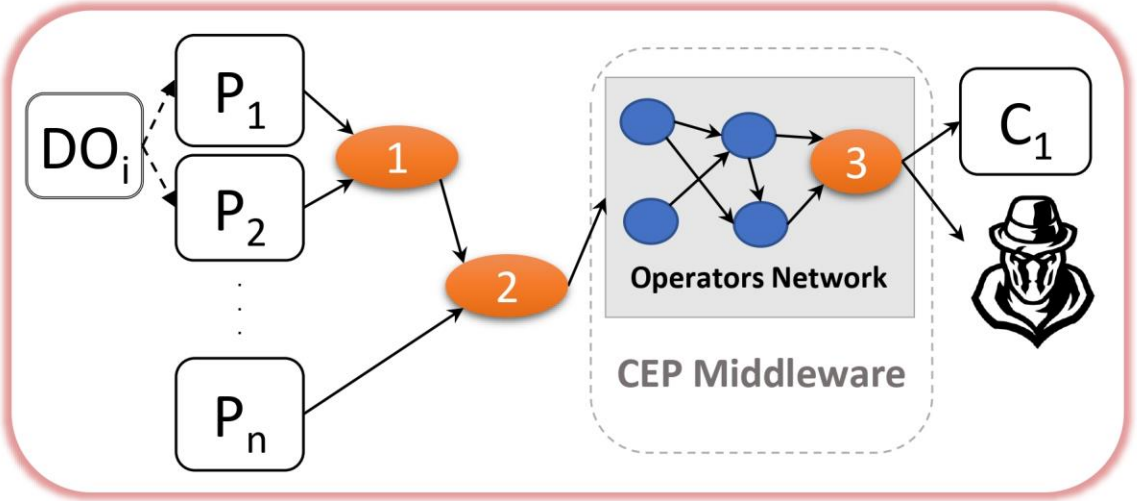
1 Motivation

- From Attributes to Patterns.
- Event Obfuscation Techniques.



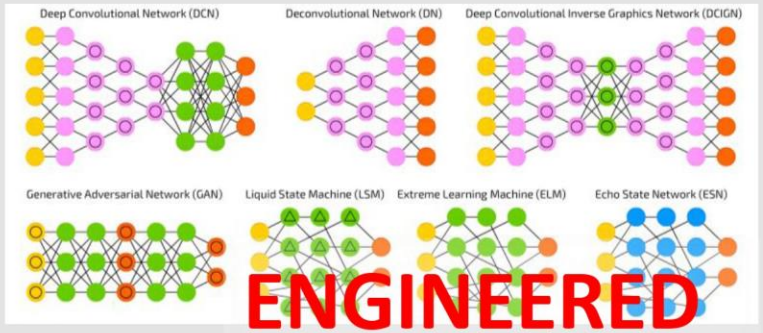
2 Research Questions

- Which obfuscation technique?
- Where to deploy the obfuscation operator?
- How to model adversary's background knowledge?

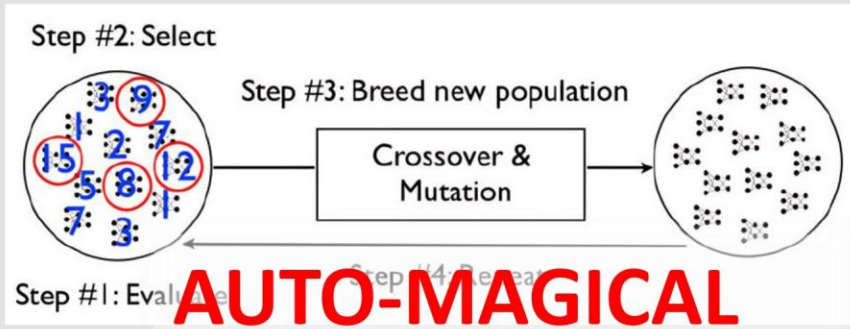


Goodbye Engineered ANNs, Hello Evolutionary Neural Networks

1. **Nature-inspired Machine Learning**:
   - ➢ Artificial Intelligence + Evolution + Neuroscience
2. **Scalable Neuroevolution**:
   - ➢ Collaborating models for emerging new tasks
3. **Universal Representation**:
   - ➢ Data format for different input/output modalities



ENGINEERED



AUTO-MAGICAL

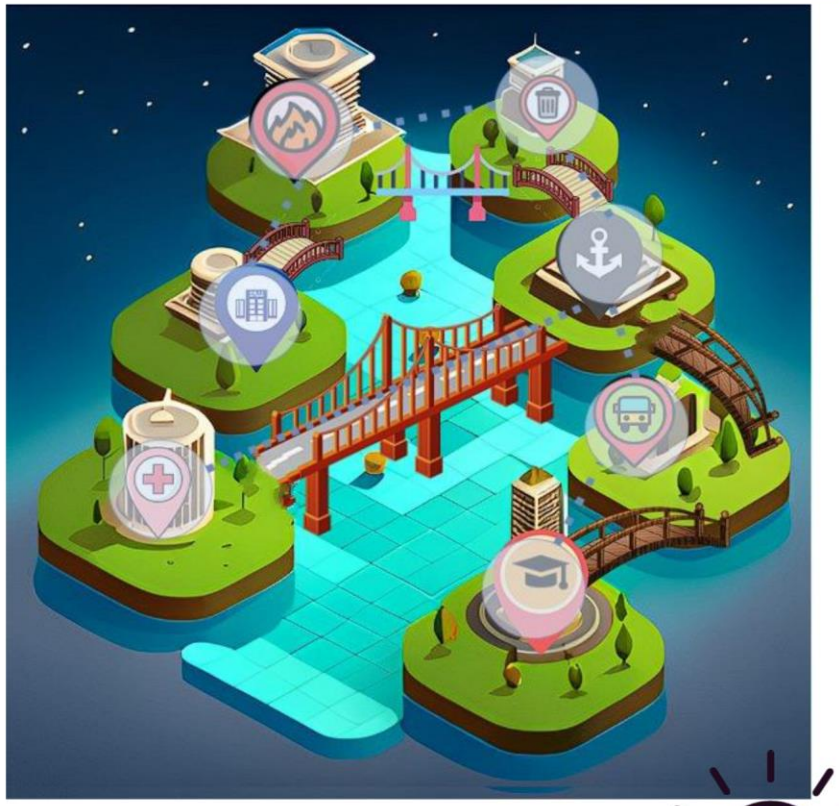
ComDeX: A Context-aware Federated Platform for IoT-enhanced Communities

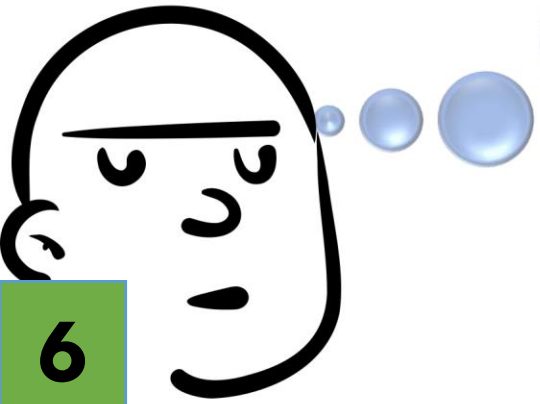
FORTH INSTITUTE OF COMPUTER SCIENCE
TELECOM SudParis

"Breaking the Silos"

How?

"Outperforming Alternatives"





How can stakeholders maintain their data sovereignty while participating in a data-sharing network?

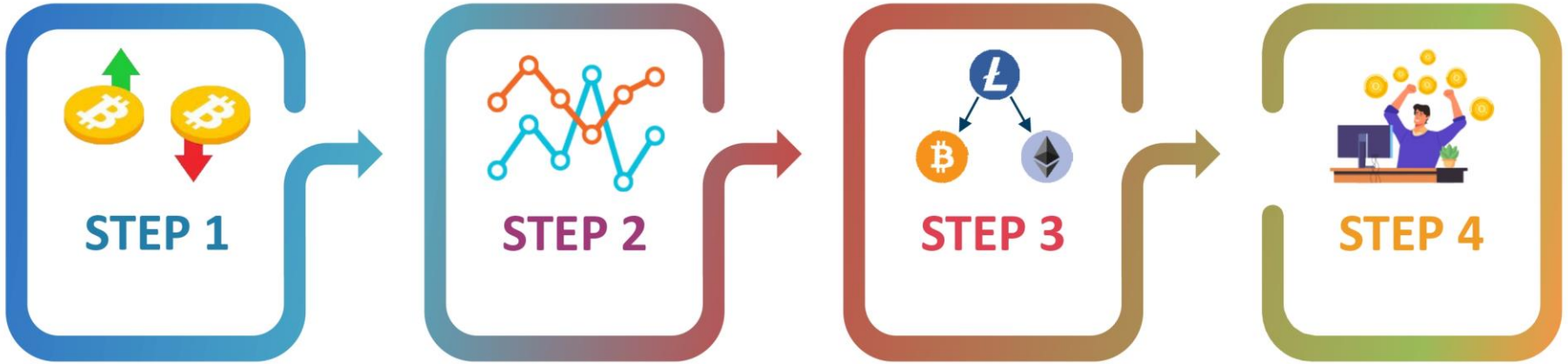
Selective Sharing?
Data Discovery?

How to seamlessly connect diverse stakeholders and enable efficient data exchange?

ComDeX!

Pasquale De Rosa, Pascal Felber and Valerio Schiavoni

unine
Université de Neuchâtel
Institut d'informatique



Problem

Cryptocoins are extremely volatile assets. A real nightmare for potential investors! We propose a solution to predict… the unpredictable.

Correlation

We study correlations between altcoin and main coin (BTC/ETH) prices. Highly correlated altcoins are good predictors for BTC/ETH prices.

Causality

Correlation does not imply causation! We analyze causality between correlated altcoins and main coins to identify the best predictors.

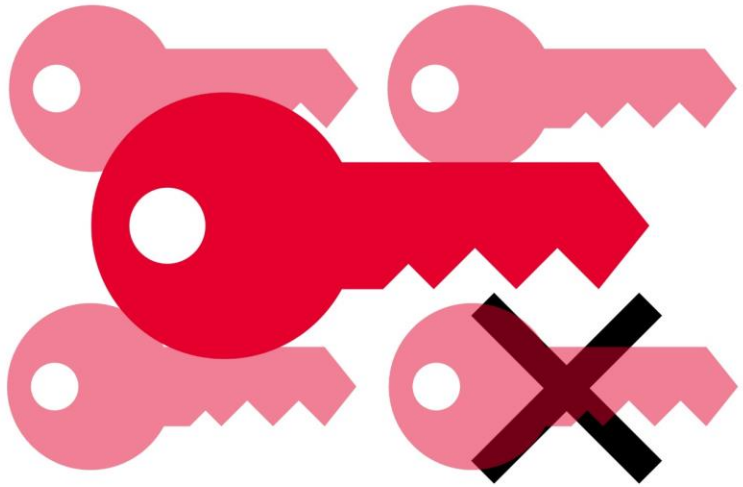
Forecast

We use ML models to forecast BTC/ETH prices basing on these altcoins. Our predictions are highly accurate. Good news for the investors!

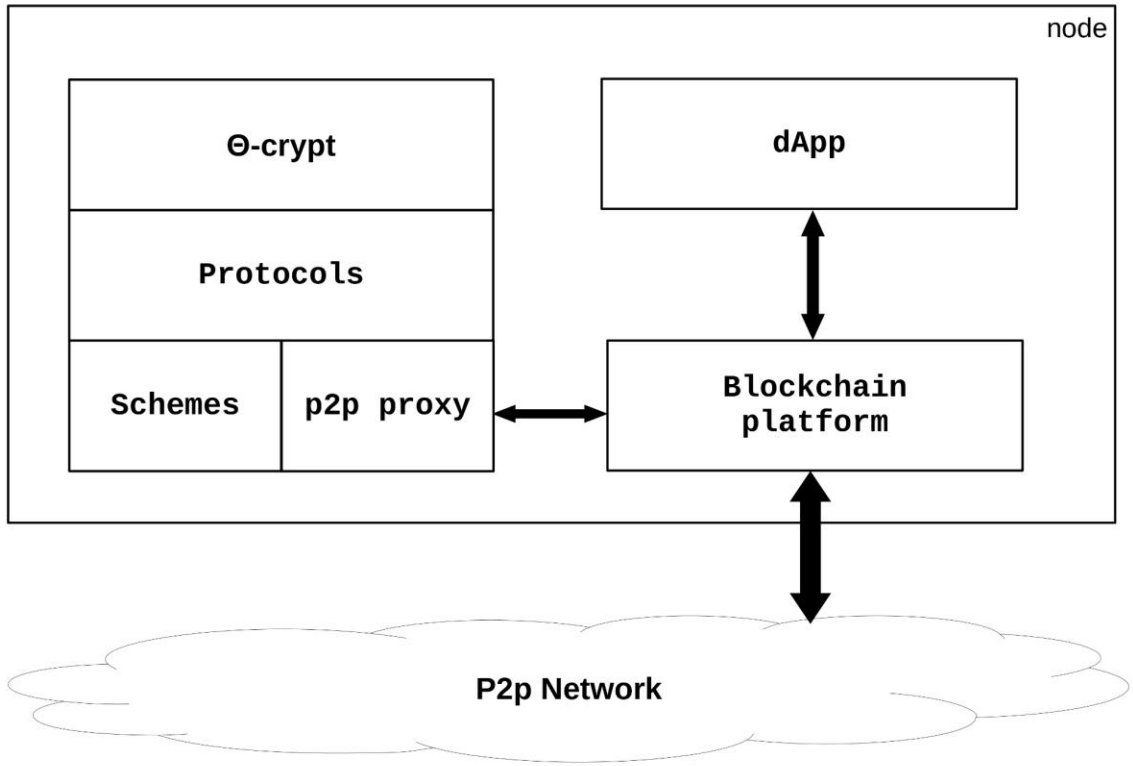
ThetaCrypt: A distributed service for threshold cryptography on chain

Orestis Alpos, **Mariarosaria Barbaraci**, Christian Cachin, Noah Schmid, Micheal Senn, Nathalie Steinhauer
University of Bern

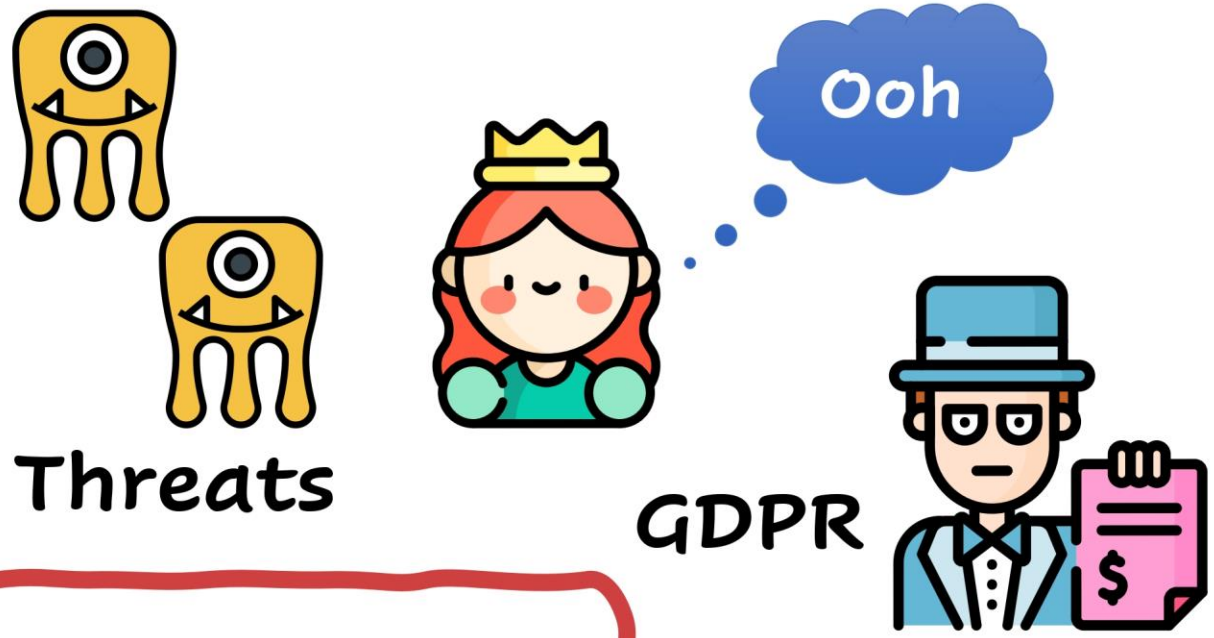
Threshold cryptosystems

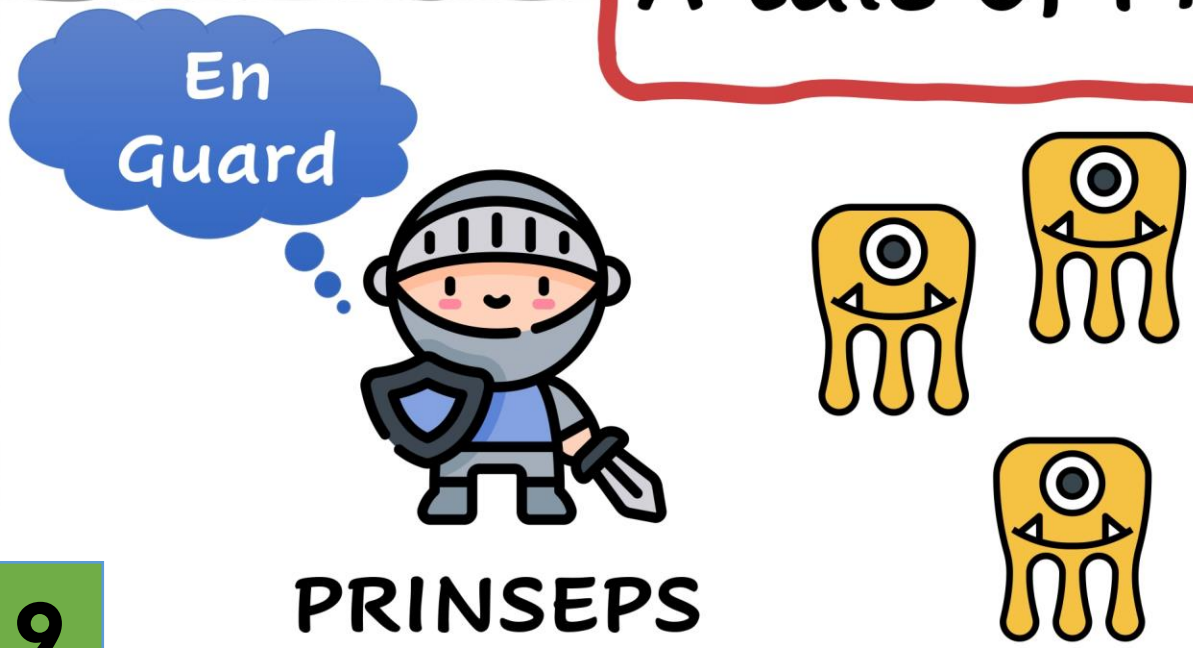


Integration on blockchains



A tale of Privacy in SPSs

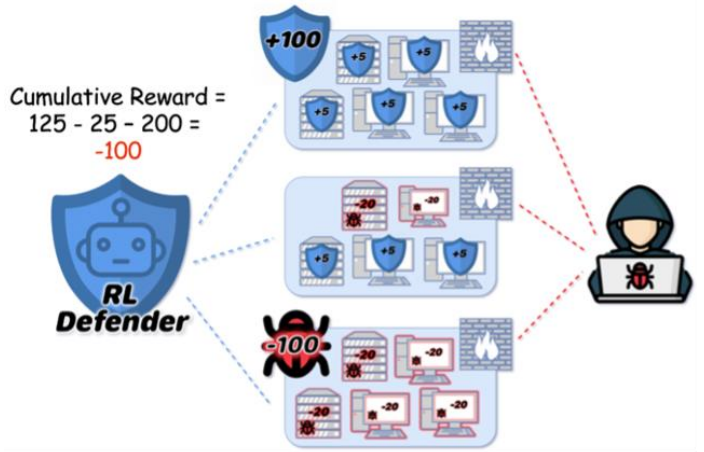




Cognitive Cyber Defense - Dynamic, Adaptive Cyber Defense Systems for Massively Distributed, Autonomous, and Ad-hoc Computing Environments - A New Brand of Cyber.

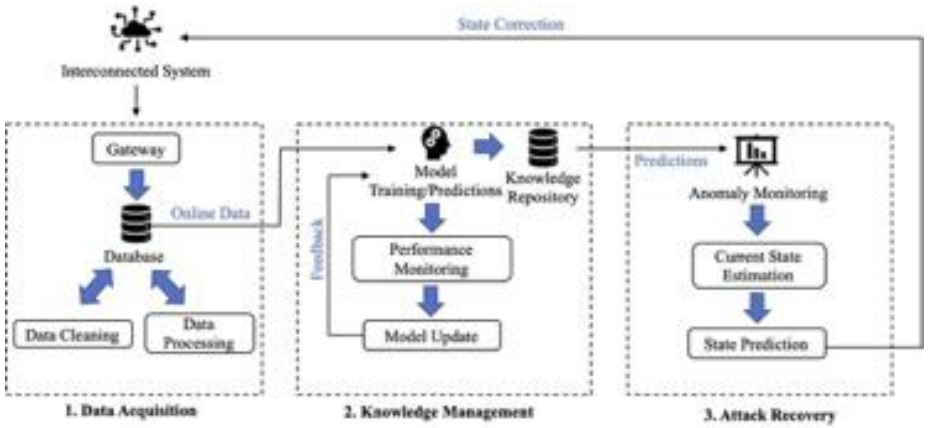
The unprecedented scale, speed, and scope of interconnectivity, ranging from the microsensors on the *edge* to the global networks, will be the prominent characteristics of the emerging computing environments.

Our current cyber defense methods, designed for the computing environments we know, will be mainly rendered inadequate for these future environments. To meet the emerging cyber defense demands, we need a new approach.

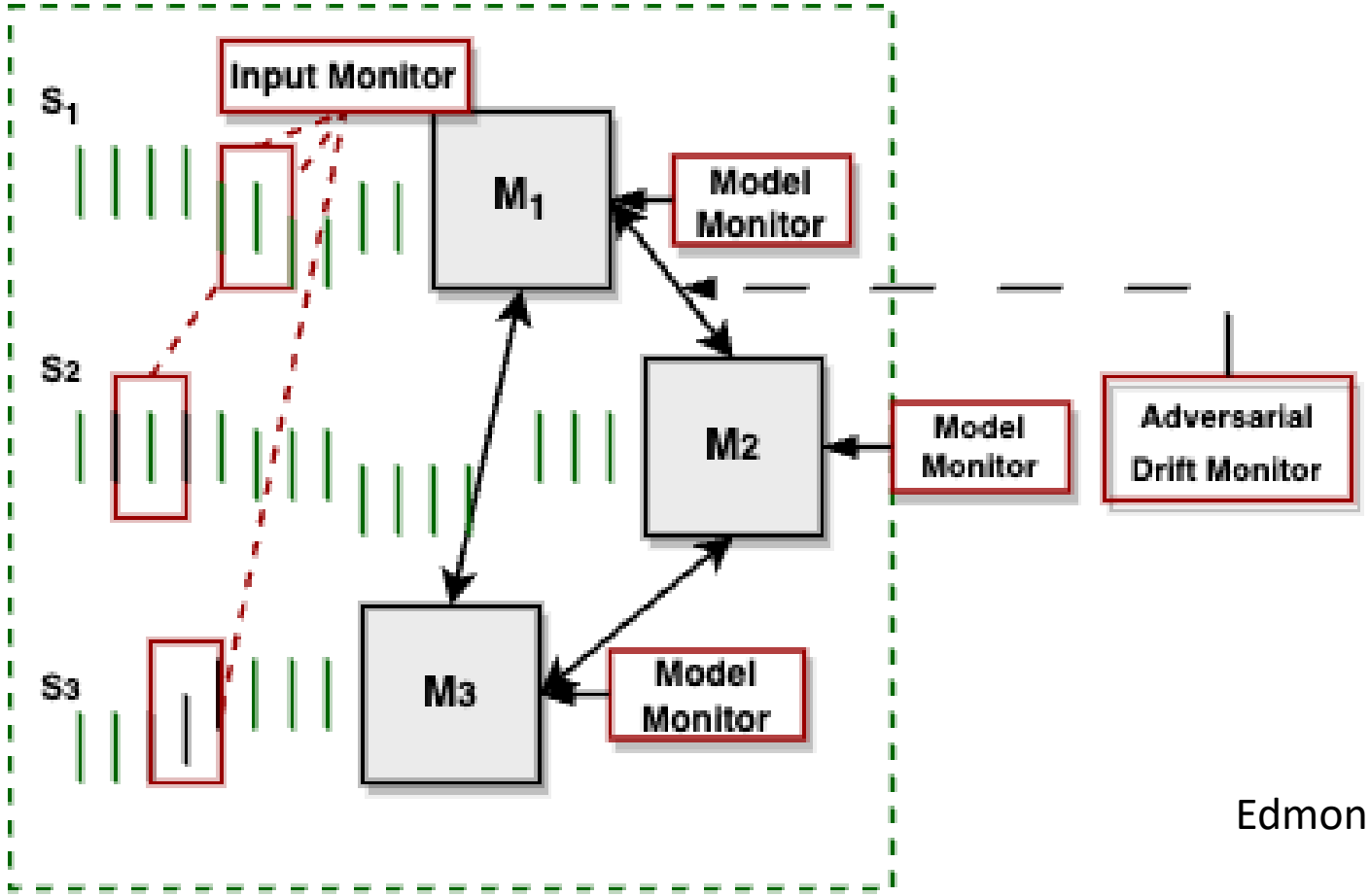


Cognitive Cyber Principles:

(a) Multi-modal and multi-scale cyber defense
(b) Dynamic adaptation
(c) Autonomous responses and operations



StreamToxWatch – Detector Architecture for Data Poisoning in Streams



Functions:

- Input Analysis
- Adversarial Drift Detection
- Model Performance Monitoring

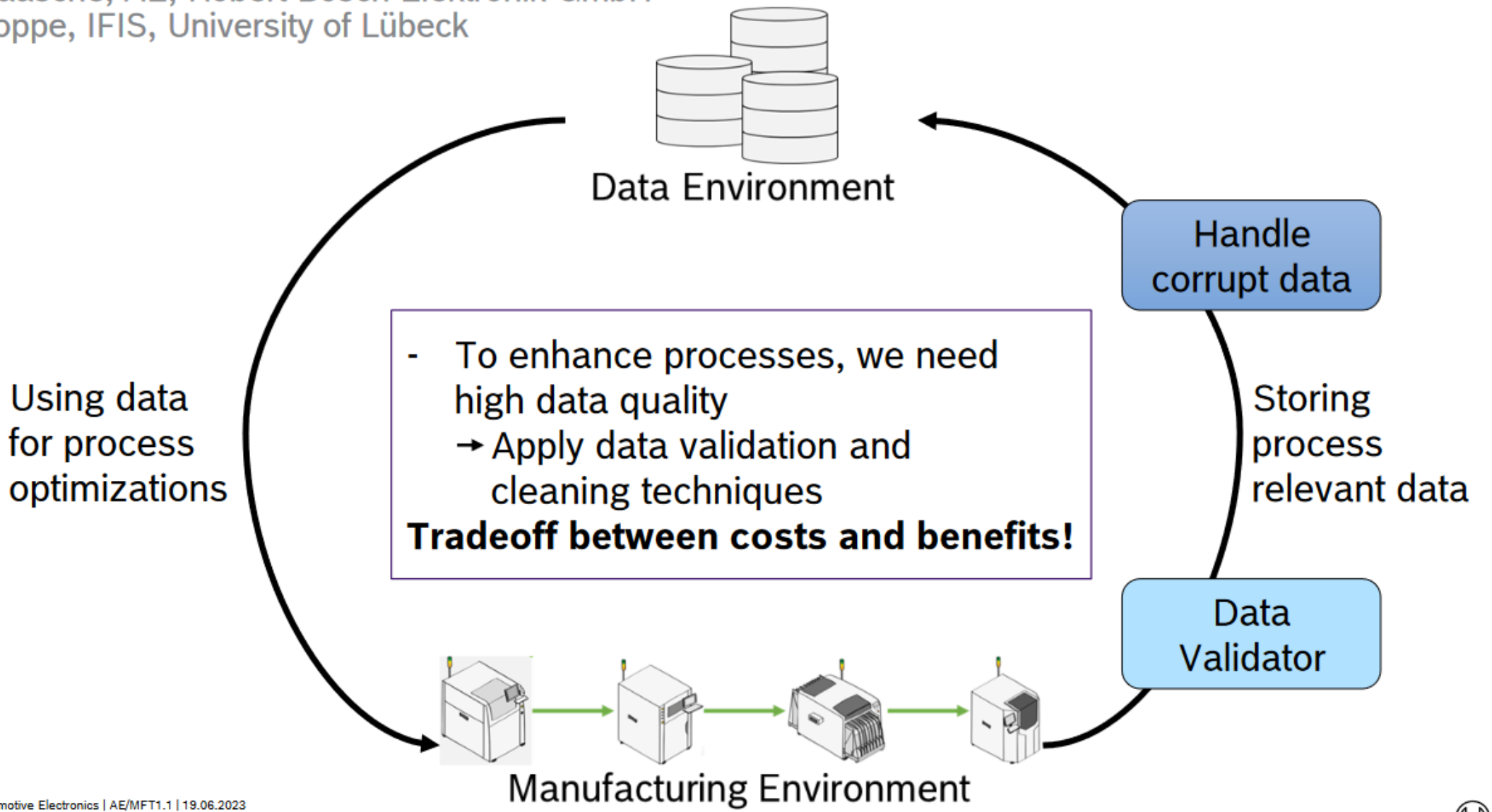
System Protocols and Components:

- ToxWatch Protocol
- Baselining
- Performance and Monitoring Configurations

Edmon Begoli, begolie@ornl.gov, Oak Ridge National Laboratory (ORNL)

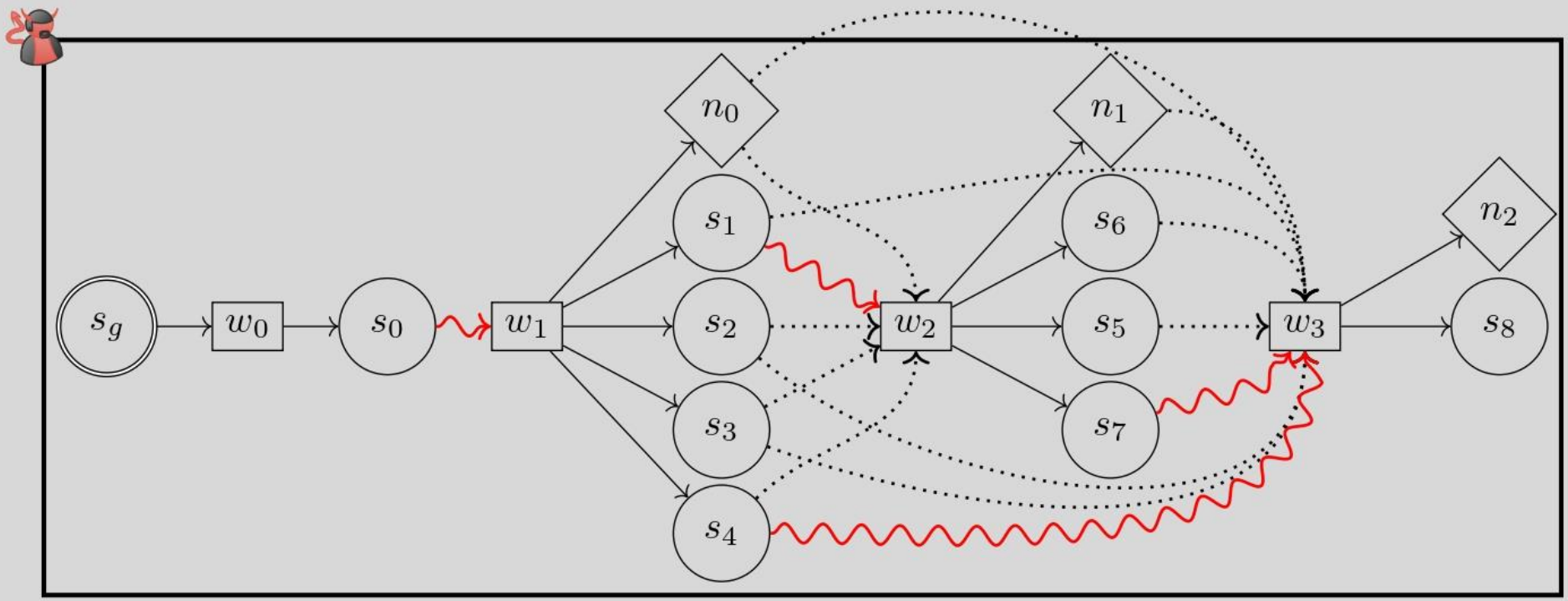
Handling Inconsistent Data in Industry 4.0

Simon Paasche, AE, Robert Bosch Elektronik GmbH
Sven Groppe, IFIS, University of Lübeck

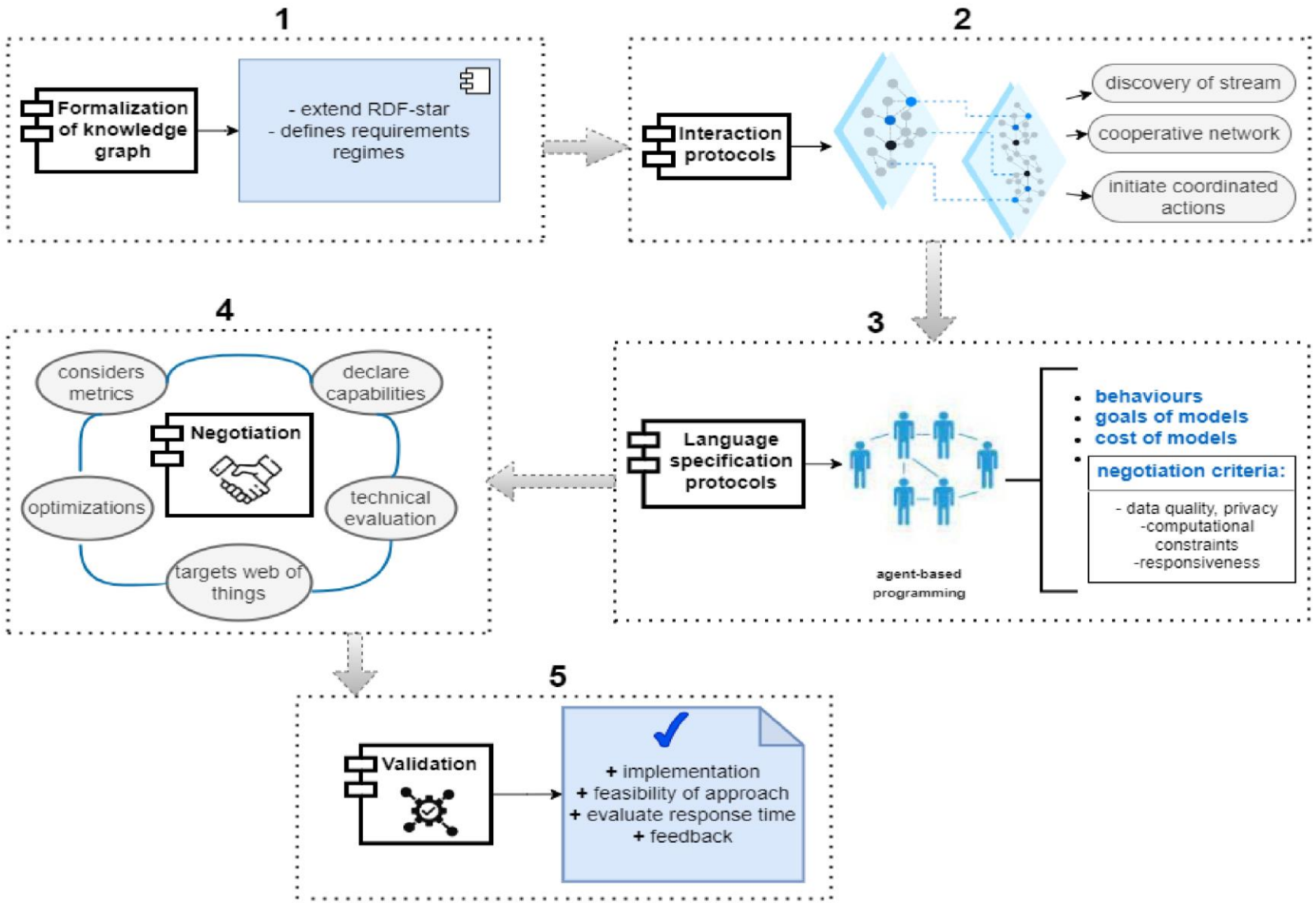


BOSCH

Privacy-Preserving Transaction DAG (PDAG)



Decentralized Stream Reasoning Agents

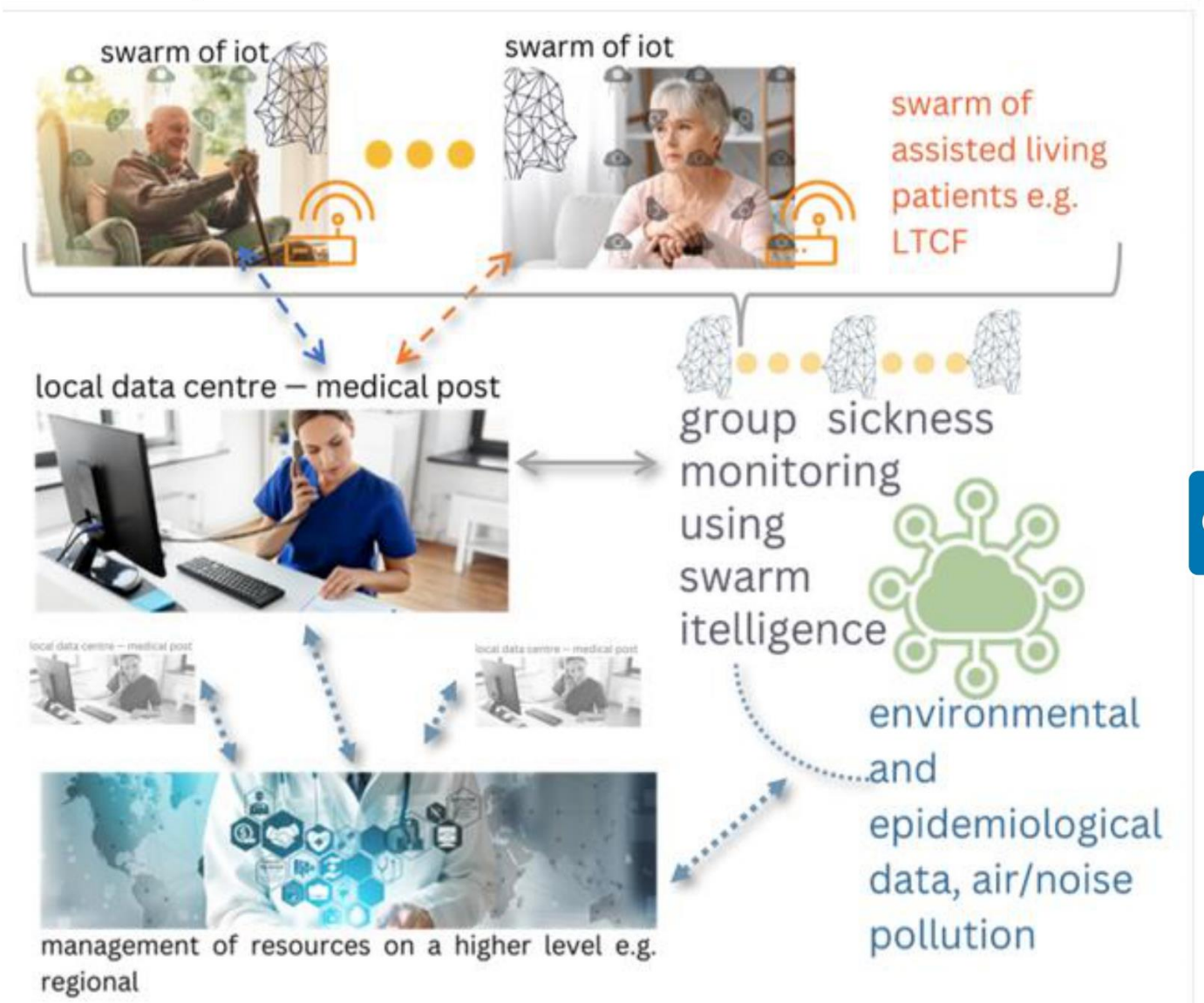


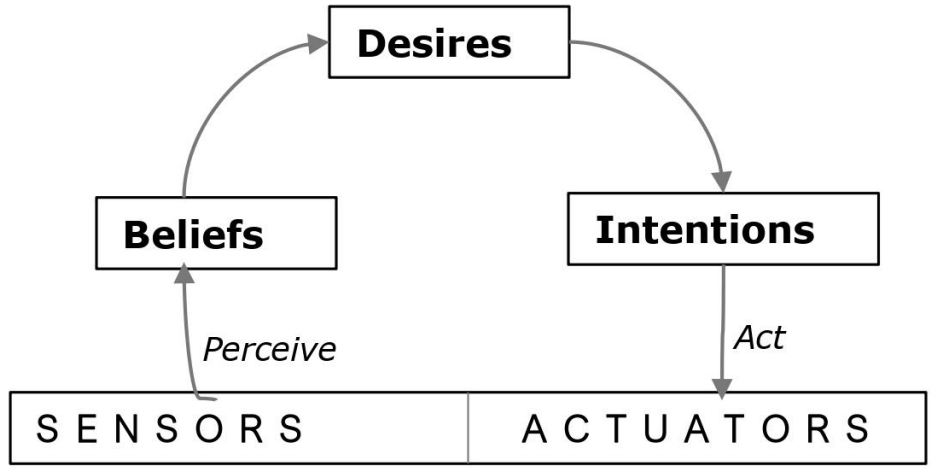
Gozde A. Tataroglu Ozbulak

University of Applied Sciences and Arts
Western Switzerland HES-SO

DEBS 2023

Agent-Based Orchestration on a Swarm of Edge Devices





- Orchestrator
- Tasks/goals/skills defined
- Participation of smart edge nodes
- Find and discover which nodes comply with these requirements

By Banani Anuraj (Supervised by Jean-Paul Calbimonte)

Ref: SmartEdge Deliverable D2.1 Documentation