EUCNC | 6G Summit
Antwerp, Belgium • 3-6 June 2024

Privacy-Aware Decentralized Security Analytics for 6G Networks

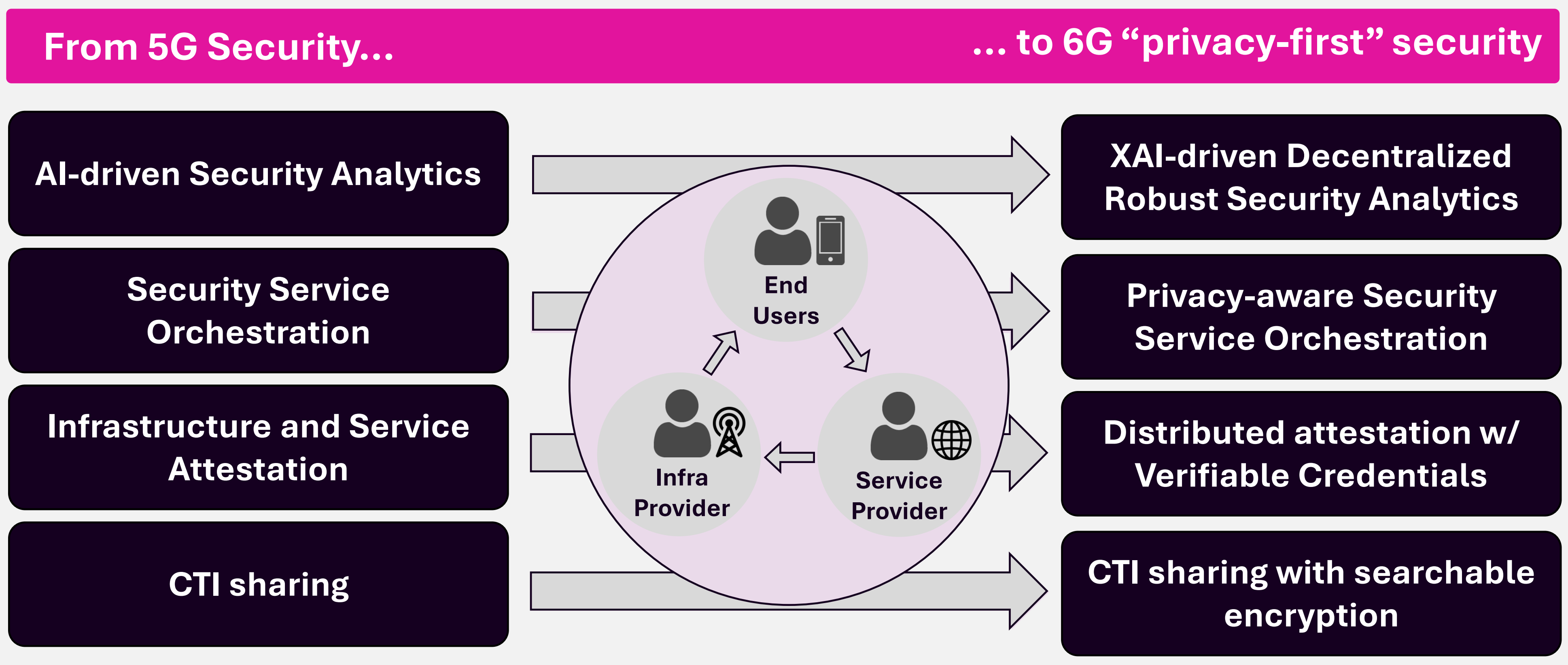
Mariana Cunha[1], João P. Vilela[1], Lampros Argyriou[2], Antonia Karamatskou[2], and Nikolaos Papadakis[2]

[1]CRACS/INESC TEC, CISUC, and Department of Computer Science, University of Porto, Portugal
[2]Infili Technologies S.A., Greece

PRIVATEER'S VISION

> *The mission of PRIVATEER is to **pave the way for 6G "privacy-first security"** by studying, designing and developing innovative security enablers for 6G networks, following a privacy-by-design approach.*

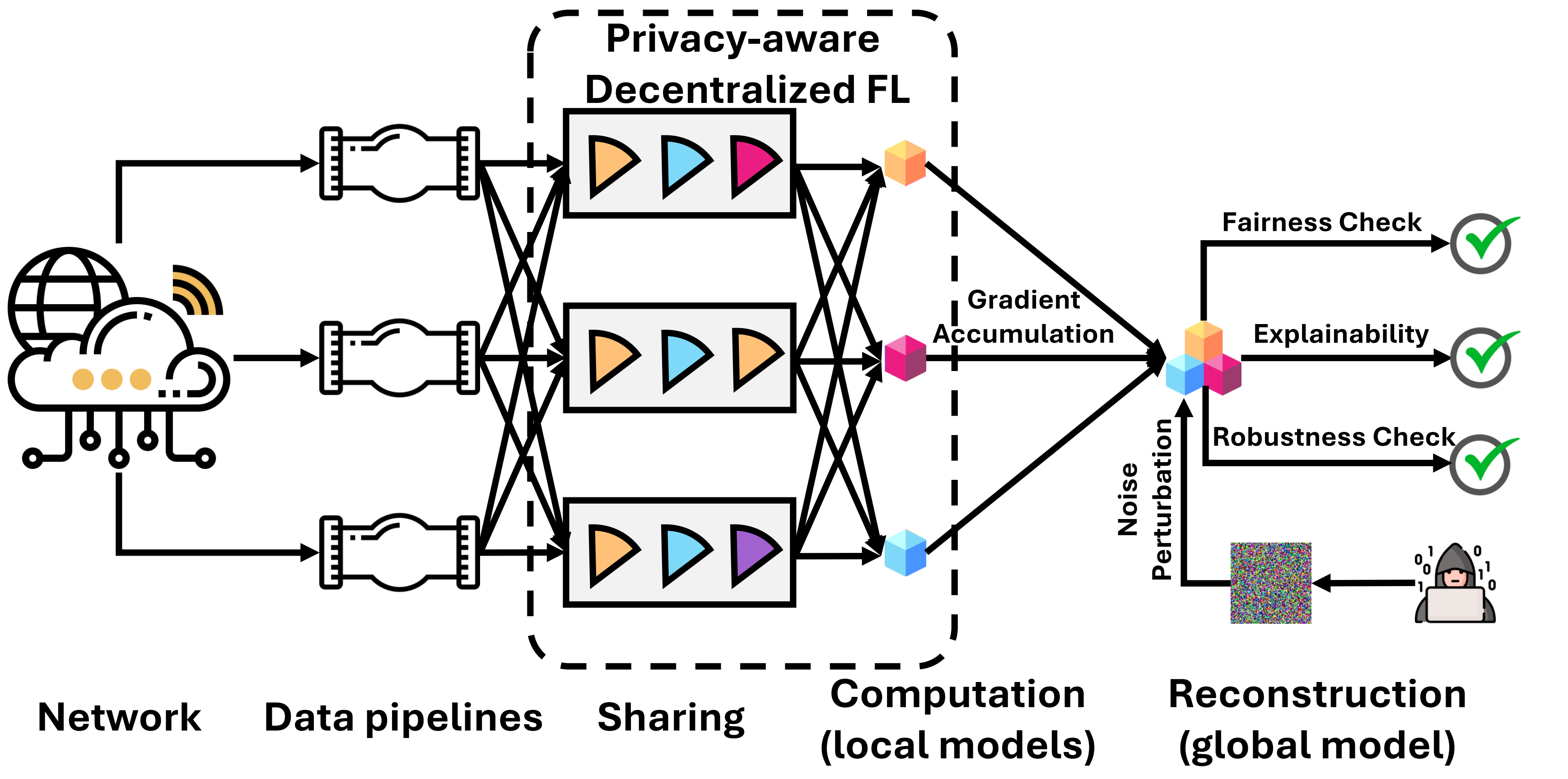
www.privateer-project.eu


From 5G Security...
... to 6G "privacy-first" security
AI-driven Security Analytics
Security Service Orchestration
Infrastructure and Service Attestation
CTI sharing
End Users
Infra Provider
Service Provider
XAI-driven Decentralized Robust Security Analytics
Privacy-aware Security Service Orchestration
Distributed attestation w/ Verifiable Credentials
CTI sharing with searchable encryption

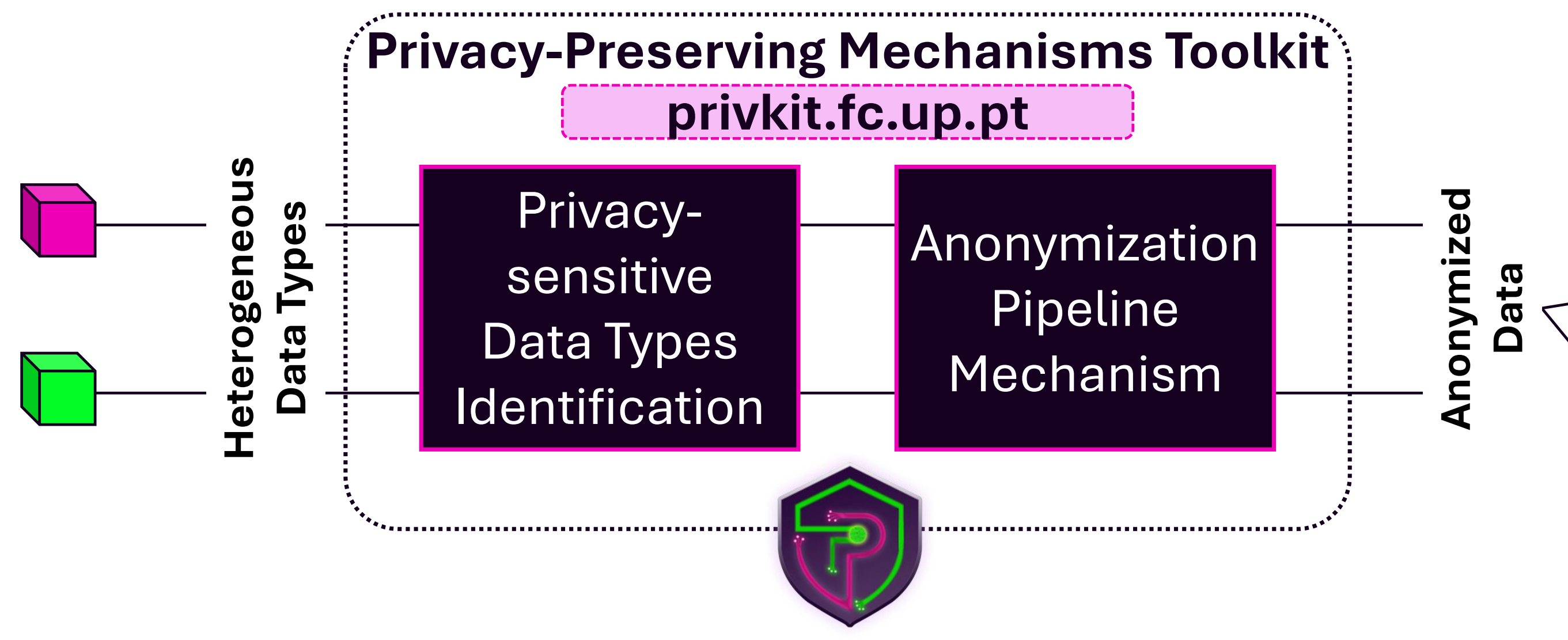
INTRODUCTION

- **Privacy** and **security** are main concerns in **6G networks**.
- Enormous **amounts of data** are continuously **collected**.
- **6G** has a **heterogeneous** and **distributed** nature that challenges the **processing of infrastructure and network data** with **privacy guarantees**.
- A **PRIVATEER's objective** is to enable **explainable** and **decentralized AI-driven security** analytics for **6G**.
- **PRIVATEER's proposal:** **privacy-aware decentralized security analytics** enriched with **data pipelines**.

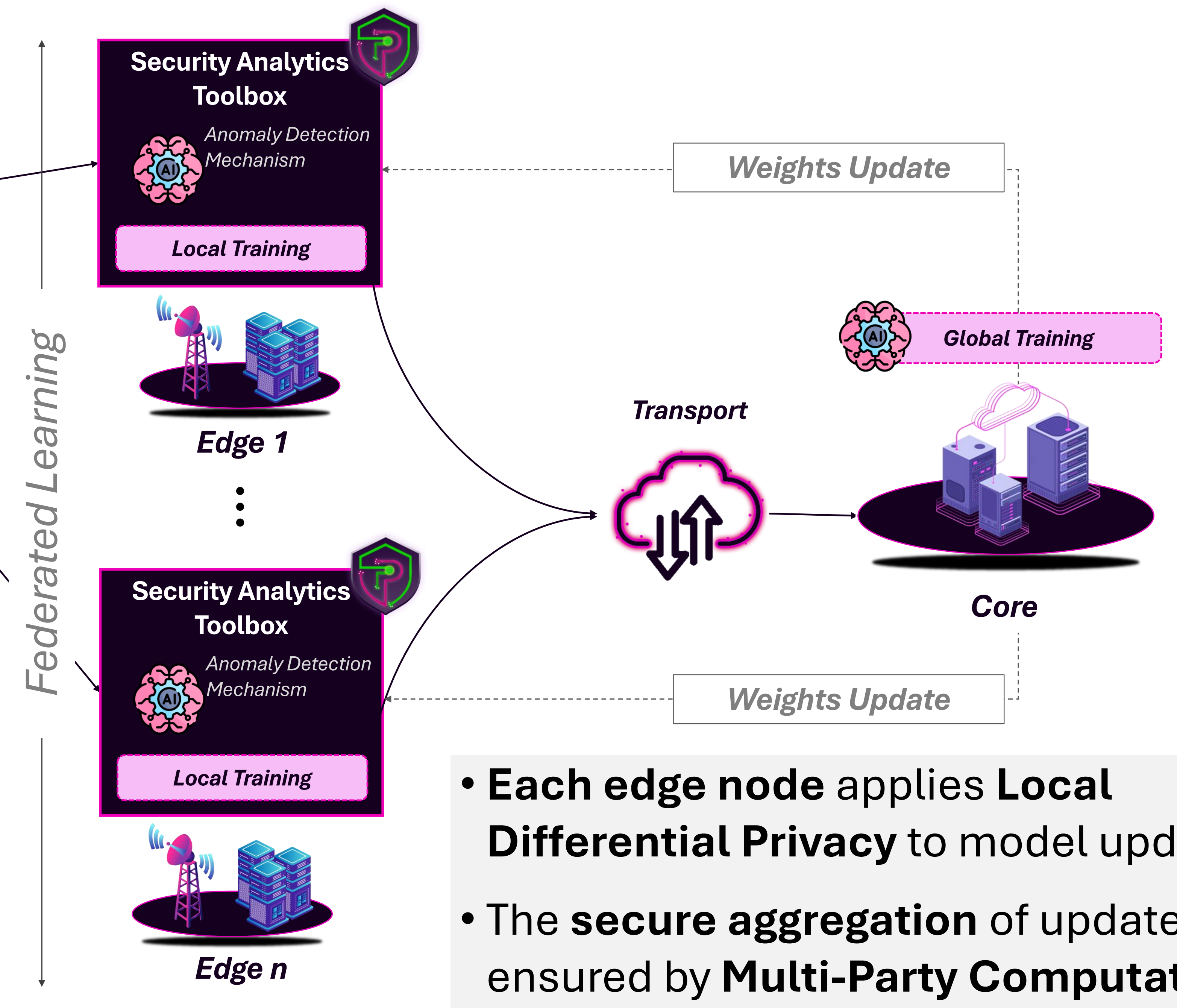
PRIVATEER'S DECENTRALIZED ROBUST SECURITY ANALYTICS



APPROACH AND ARCHITECTURE


Privacy-Preserving Mechanisms Toolkit
privkit.fc.up.pt
Heterogeneous Data Types
Privacy-sensitive Data Types Identification
Anonymization Pipeline Mechanism
Anonymized Data

- The **data anonymization pipeline** is available as a **toolkit** that acts as a **privacy-aware pre-processing stage [1]**.
- Given the **anonymous data**, the **security analytics** provide **anomaly detection capabilities** through **Privacy-Preserving Machine-Learning Techniques**.
- **Federated Learning (FL)** is leveraged at **edge nodes** to warrant **privacy-aware decentralized security analytics**.



- **Each edge node** applies **Local Differential Privacy** to model updates.
- The **secure aggregation** of updates is ensured by **Multi-Party Computation**.

PRIVATEER'S PARTNERS

SPACE
DEMOKRITOS
Telefónica
RHEA GROUP
INESCTEC
UBITECH ubiquitous solutions
FFI Norwegian Defence Research Establishment
iquadrat
P.PORTO
ERTICO ITS EUROPE

REFERENCES

[1] M. Cunha, G. Duarte, R. Andrade, R. Mendes, and João P. Vilela, "Privkit: A Toolkit of Privacy-Preserving Mechanisms for Heterogeneous Data Types," in Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy, ser. CODASPY '24. ACM, 2024

INESCTEC
CISUC
fct Fundação para a Ciência e a Tecnologia
PRIVATEER Privacy-first Security Enablers for 6G networks
6GSNS
Co-funded by the European Union