PRIVATEER
Privacy-first Security Enablers
for 6G networks

6G SNS

Co-funded by
the European Union

PRIVATEER

Stream D / Stream B joint workshop on KPIs and KVIs, 16/05/2024, Online

Maria Christopoulou (NCSR “Demokritos”)

maria.christopoulou@iit.demokritos.gr

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

Project Mission

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.

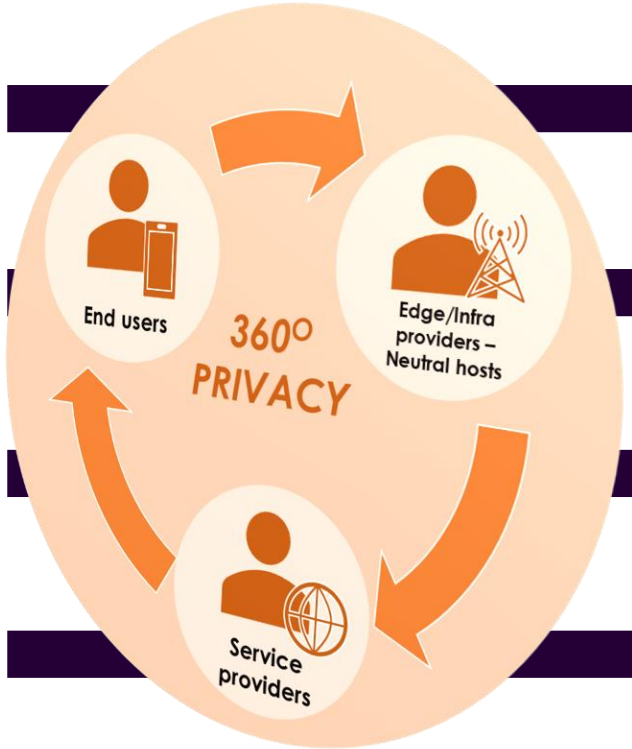
Overall result: PRIVATEER security framework (TRL4/5) integrated and deployed in a 5G+ campus testbed, verified against vertical use cases

Technical Pillars of PRIVATEER

From 5G security…

…to 6G "privacy-first" security

- AI-driven Security Analytics → XAI-driven Decentralized Robust Security Analytics
- Security Service Orchestration → Privacy-aware Security Service Orchestration
- Infrastructure and Service Attestation → Distributed attestation w/ Verifiable Credentials
- CTI sharing → CTI sharing with searchable encryption



High-Level Architecture

Robust Security Analytics

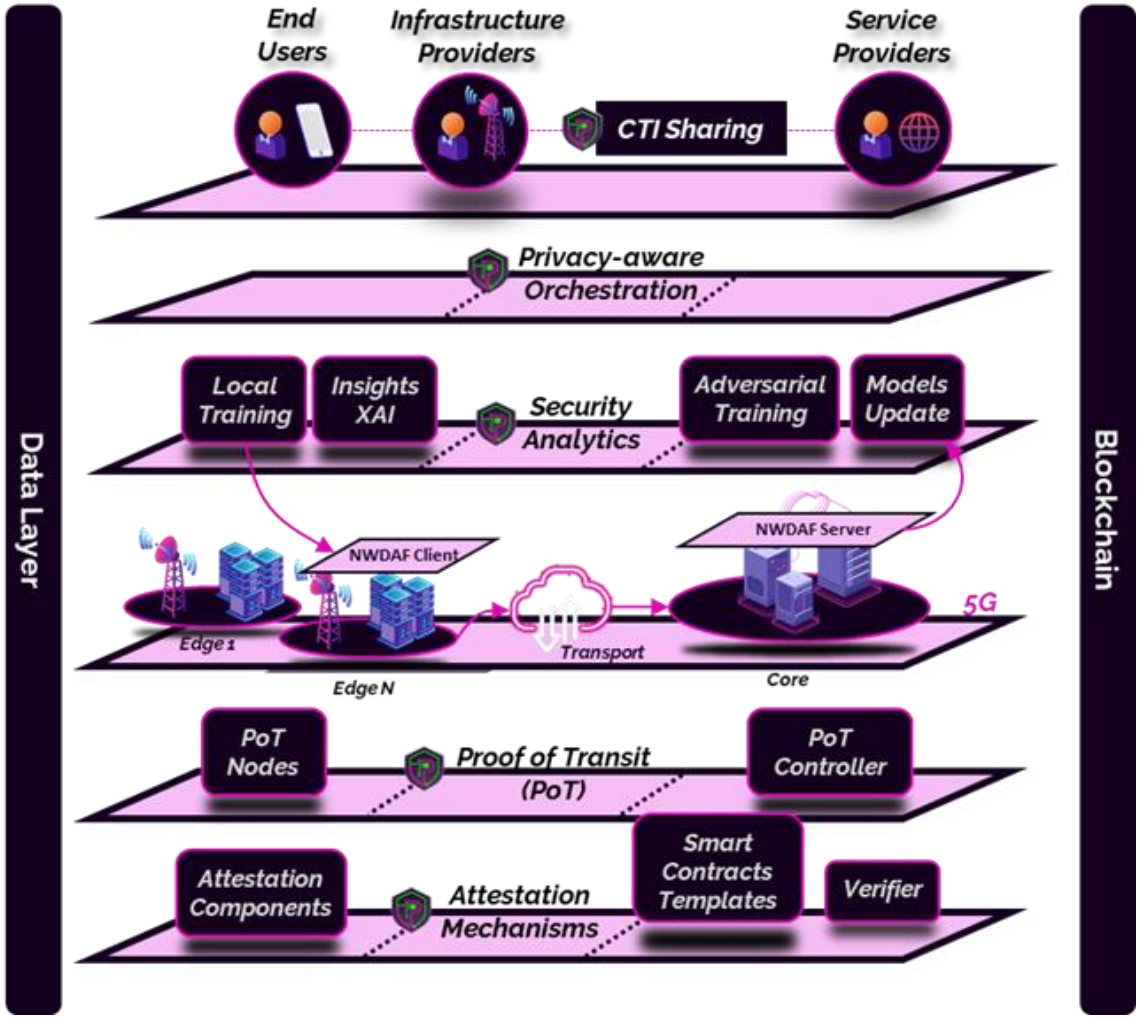
- Federated NWDAF Deployment
- Adversarial Training of AI/ML models
- XAI & FPGA Acceleration
- Data Anonymization Pipelines

Privacy-Aware Orchestration

- Level of Trust Assessment
- Trustworthy Network Topology
- Traceable SLA Verification
- Reinforcement Learning for Orchestration

Attestation & CTI Sharing

- Attestation in virtualized environments and edge FPGA devices
- Verifiable credentials for Identity Mgmt
- Privacy-preserving Threat Sharing with Searchable Encryption



Context

- PRIVATEER Partners have provided a list of KPIs/KVIs in *D2.1* "6G Threat Landscape and Gap Analysis"* and includes relevant references and indicative values (that really depend on the specific use case and system requirements).
- In this presentation, we provide a subset of the KPIs due to space/time limitations.
- We are planning to release a White Paper on 6G Security/Privacy KPIs/KVIs.

**PRIVATEER Consortium, "D2.1 6G Threat Landscape and Gap Analysis", 2023, https://zenodo.org/doi/10.5281/zenodo.7994961*

KPIs/KVIs

Category	KPI	
AI-based Intrusion Detection	Number of False Positives/Negatives	The percentage of incorrect threat identifications by the AI-based detection system.
	Mean Time to Detect a Threat	The average time taken by the system to detect a security threat.
	Accuracy Loss (Federated Model)	The decrease in accuracy of the federated model compared to a centralized model, calculated as $1 - \frac{Accuracy\ of\ federated\ model}{Accuracy\ of\ centralized\ model}$
Privacy Preservation of ML model & Adversarial Protection	Success of Adversarial Privacy Attacks: Inference of Membership	Measures the accuracy of identifying whether a record belongs to the training set by an attacker
	Accuracy Loss (Private Model)	The decrease in accuracy of the private model compared to a non-private model due to privacy mechanisms, calculated as $1 - \frac{Accuracy\ of\ Private\ Model}{Accuracy\ of\ Non\ Private\ Model}$
	Performance Loss/Overhead	The performance impact of introducing adversarial protection mechanisms, measured against metrics such as accuracy, precision, recall, and F1.
	Model Poisoning	The percentage of adversarial workers or agents that can be tolerated without significant performance degradation.

KPIs/KVIs

Category	KPI	
Data Anonymization	Quality Loss	the difference/distance between the anonymized data and the original data/how much quality is lost by reporting anonymized data instead of real data
Orchestration	Time to repair	from the moment a security anomaly breach is detected (or predicted) until relevant intra- or inter-domain adaptation primitives have been triggered and completed, bringing the system back to a stable and privacy-by-default SLA-compliant state
	Time to resource preparation end-to-end	from the moment an order is expressed as intent, until all multi-party resources that comply to corresponding privacy service requirements have been discovered and provisioned
	Decision time	how fast the ML model can process input data, analyze the current network state, and make informed decisions to protect the network
Distributed Ledger	Latency	The time between the receipt of a request and the commitment of the transaction.
	Throughput	The total number of transactions supported by a single blockchain peer.
	Auditability of Data	The ability to trace and verify records within the decentralized ledger.
Trustworthiness	Level of Trust (LoT)	A composite metric calculated from several indicators (e.g., attestation levels, traffic attestation, traceability, security issues) to assess the trustworthiness of 6G services.
	Levels of Assurance (LoA)	Defined by ETSI, these levels range from 0 to 5, representing the scale of relative trust, with higher numbers denoting greater levels of trust.

6GSNS

Co-funded by the European Union

PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096110

Privateer_6GSNS

privateer-6gsns

@Privateer_6GSNS

privateer-contact@spacemaillist.eu