PRIVATEER
Privacy-first Security Enablers
for 6G networks

6G SNS

Co-funded by
the European Union

PRIVATEER

Privacy-first Security Enablers for 6G Networks

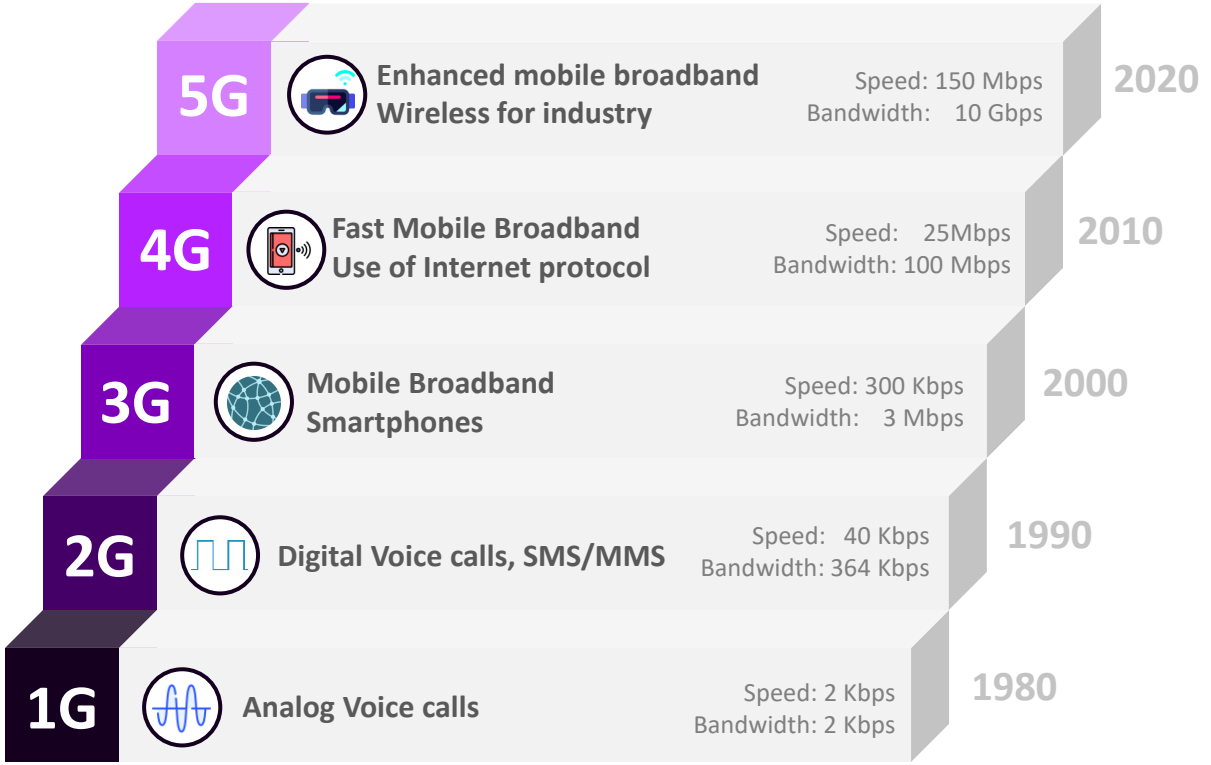
Project Overview

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

Adoption of 5G Nowadays

Widespread adoption of 5G today

- Faster speeds (150 Mpbs)
- Lower Latency (<5ms)
- Increased Bandwidth (10 Gbps)



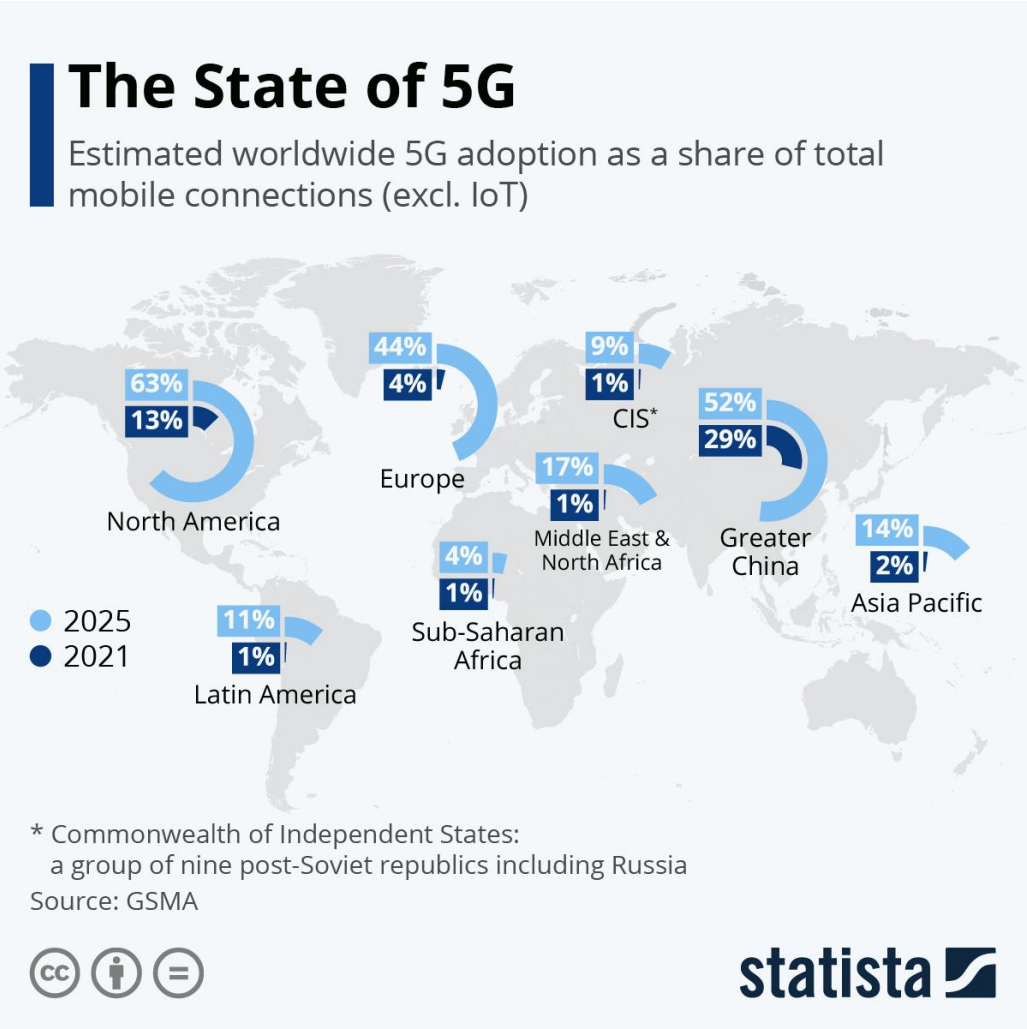
Inspired by
https://prc.chapters.comsoc.org/2019/04/01/5g-evolution-wireless-communications/
https://drawingcapital.substack.com/p/5g-the-revolution-begins

Adoption of 5G Nowadays

Widespread adoption of 5G today

- Faster speeds (150 Mpbs)
- Lower Latency (<5ms)
- Increased Bandwidth (10 Gbps)

40% increment from 2021 to 2025 in Europe

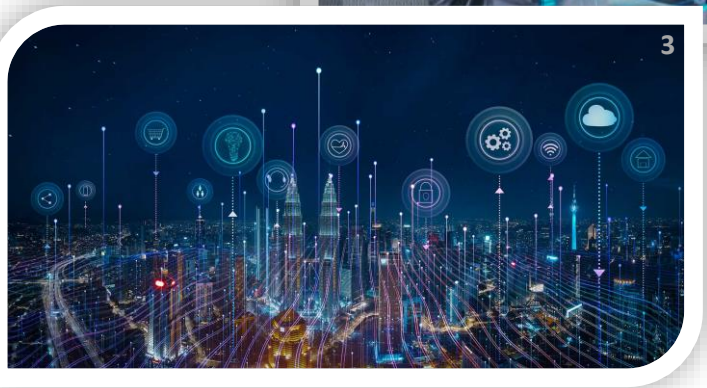


https://www.statista.com/chart/26954/5g-adoption-by-world-region/

Towards B5G and 6G

5G still poses limitations for next-gen applications

- Need for faster speeds (e.g., XR)
- Need for ultra-low latency (e.g., autonomous transportation)
- Need for increased bandwidth (e.g., IoT at scale)



➔ Beyond 5G (B5G) and 6G networks as a solution!

6G to be realized by 2030 in Europe[4]

[1] https://cmte.ieee.org/futuredirections/2020/10/25/6g-does-not-exist-yet-it-is-already-here-xiv/
[2] https://device-insight.com/en/2022/12/14/from-1g-to-6g-how-5g-is-fueling-the-iot-and-what-comes-next/
[3] https://metrology.news/6g-to-deliver-hyper-connected-digital-twins/
[4] https://5g-ppp.eu/european-vision-for-the-6g-network-ecosystem/

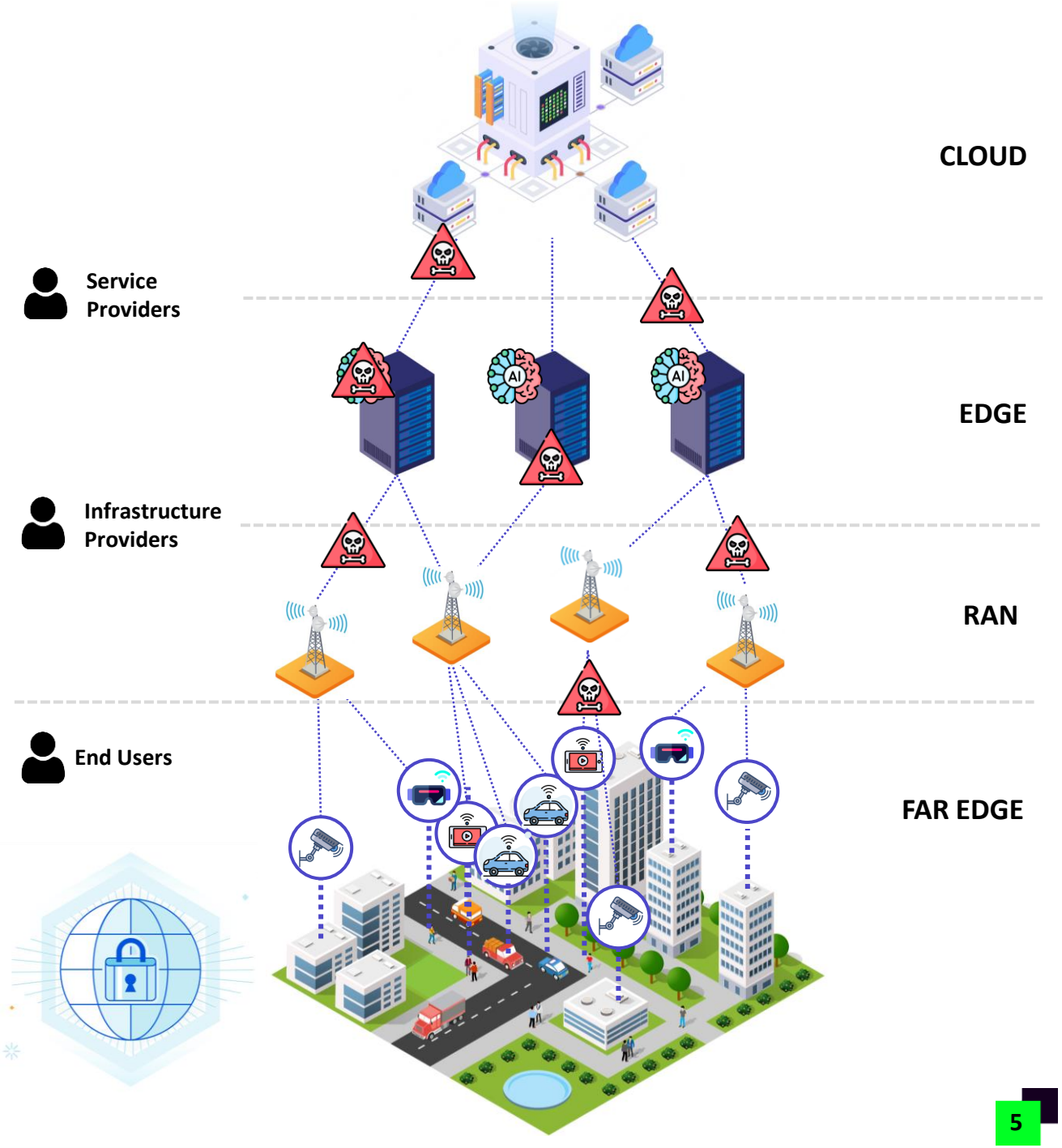
Security & Privacy: Major challenges of 6G

6G networks will be characterized by [1,2]:

- Heterogeneous radio & RAN softwarization
- Multiple stakeholders across the service chain
- AI-driven analytics & network management
- Computation spread across the entire continuum

➔ New security vulnerabilities and threats introduced!

➔ Privacy as a fundamental societal concern within EU's vision for 6G[3]



[1] Jiang, Wei, et al. "The road towards 6G: A comprehensive survey." IEEE Open Journal of the Communications Society 2 (2021): 334-366.
[2] Lee, Ying Loong, et al. "Dynamic network slicing for multitenant heterogeneous cloud radio access networks." IEEE Transactions on Wireless Communications 17.4 (2018): 2146-2161.
[3] https://5g-ppp.eu/european-vision-for-the-6g-network-ecosystem/

Security & Privacy: Major challenges of 6G

6G networks will be characterized by [1,2]:

- Heterogeneous radio & RAN softwarization
- Multiple stakeholders across the service chain
- AI-driven analytics & network management
- Computation spread across the entire continuum

➔ New security vulnerabilities and threats introduced!

➔ Privacy as a fundamental societal concern within EU's vision for 6G[3]

Need of ***novel frameworks*** to tackle this multi-level ***security and privacy requirements*** imposed by end-users and societal factors

PRIVATEER

“ PRIVATEER aims to provide privacy-centric security enablers specifically designed for future 6G networks ”

[1] Jiang, Wei, et al. "The road towards 6G: A comprehensive survey." IEEE Open Journal of the Communications Society 2 (2021): 334-366.
[2] Lee, Ying Loong, et al. "Dynamic network slicing for multitenant heterogeneous cloud radio access networks." IEEE Transactions on Wireless Communications 17.4 (2018): 2146-2161.
[3] https://5g-ppp.eu/european-vision-for-the-6g-network-ecosystem/

The PRIVATEER Project

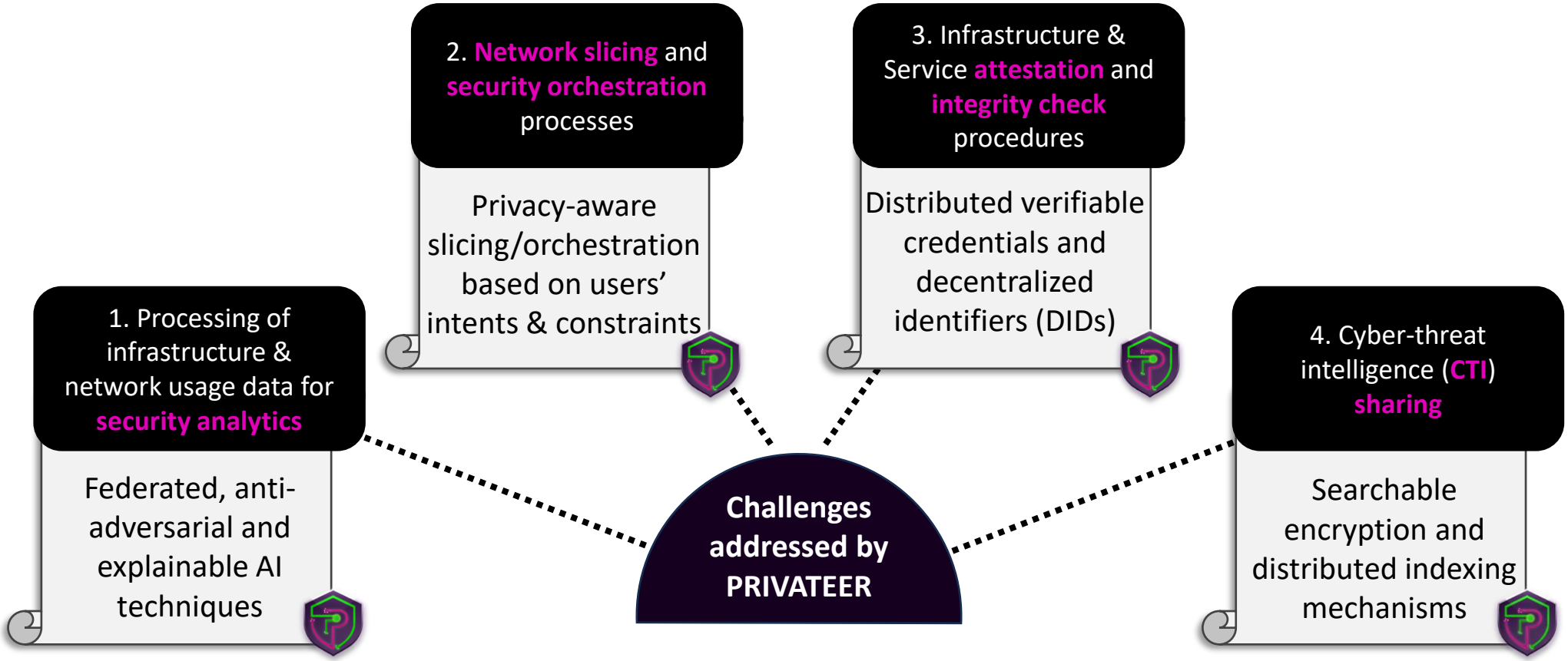
Proposal Title	**PRIVATEER** Privacy-first Security Enablers for 6G Networks
Topic Identifier	**HORIZON-JU-SNS-2022-STREAM-B-01-04** Secure Service development and Smart Security
Coordinator	**Space Hellas S.A.**
Consortium	**13 organizations, 6 countries** 6 RTOs, 3 Industries, 3 SMEs, 1 Association
Total Budget	**5.05 M€**
Duration	**36 months (January 2023 – December 2025)**

The PRIVATEER Consortium

- Space Hellas S.A. (Coordinator)
- NCSR “Demokritos” (Tech Mgr)
- Telefonica I+D
- RHEA System BV
- INESC TEC
- Infili Technologies S.A.
- Ubitech Limited
- U. Computense de Madrid
- Inst. Comm. & Comp. Systems
- Forsvarets Forksninginstitutt
- Iquadrat Informatica SL
- Instituto Politecnico do Porto
- ERTICO ITS Europe

PRIVATEER's Goals & Addressed Challenges

"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"



PRIVATEER's Technical Pillars

From 5G Security…

… to 6G "privacy-first" Security

AI-driven Security Analytics

Security Service Management

CTI Sharing

Infrastructure & Service Attestation

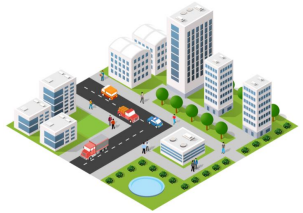
XAI-driven Federated & Robust Security Analytics

Privacy-aware Security Service Orchestration

CTI sharing with Searchable Encryption

Distributed Attestation with Verifiable Credentials

PRIVATEER's High-Level Architecture




USER | RAN | EDGE/FOG | CLOUD




Distributed Security Analytics Engines

Attestation services & Credentials wallets

Verifier service

Proof-of-Transit verification services

NETWORK SLICE

User edge function | 6GC edge function | User core function | 6GC core function

Monitoring & Analytics Agents

Privacy-aware intent-based Orchestrator

Distributed Remote Index Identifiers

Edge Acceleration

Slice Manager | Service Orchestrator

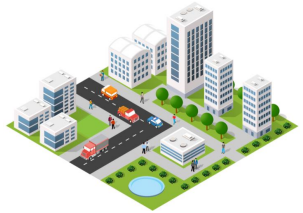
RLC/MAC/PHY | Fog/Edge VIM & NFVI | Core VIM & NFVI

End User | Infra Provider | Service Provider

DLT Distributed storage

Threat Sharing | Threat Sharing | Threat Sharing

PRIVATEER's High-Level Architecture



USER

RAN

EDGE/FOG

CLOUD

Distributed Security Analytics Engines

Attestation services & Credentials wallets

Verifier service

Proof-of-Transit verification services

NETWORK SLICE

User edge function

6GC edge function

User core function

6GC core function

Monitoring & Analytics Agents

Privacy-aware intent-based Orchestrator

Distributed Remote Index Identifiers

Edge Acceleration

Slice Manager

Service Orchestrator

RLC/MAC/PHY

Fog/Edge VIM & NFVI

Core VIM & NFVI

End User

Threat Sharing

DLT Distributed storage

Infra Provider

Threat Sharing

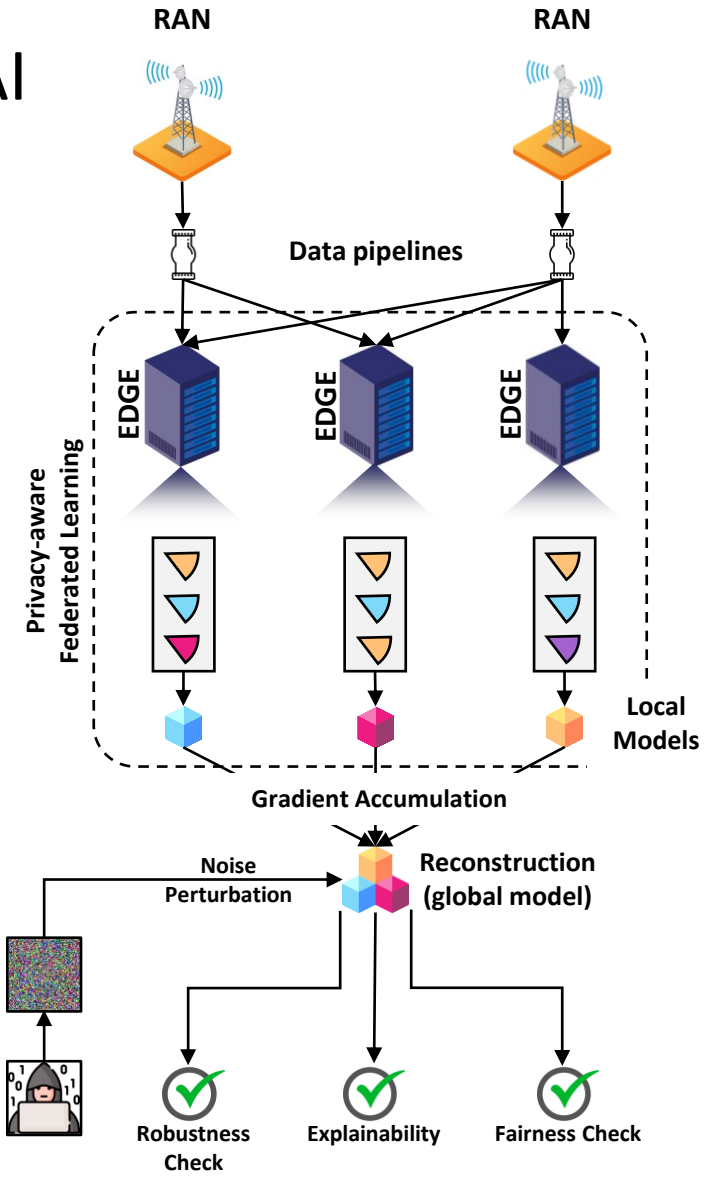
Service Provider

Threat Sharing

Decentralized Robust Security Analytics

Purpose: Detect and classify network threats through AI

- ***Privacy & Fairness***
  - Federated Learning at the edge
  - Private and fair learners (e.g., FairOD[1], FairLOF[2])
- ***Adversarial AI robustness***
  - Multiparty computation & differential privacy
  - GAN-based techniques for FL
- ***AI model Explainability***
  - Adoption of “explainable by design” models (e.g., trees)
  - Development of explanation models for deep networks

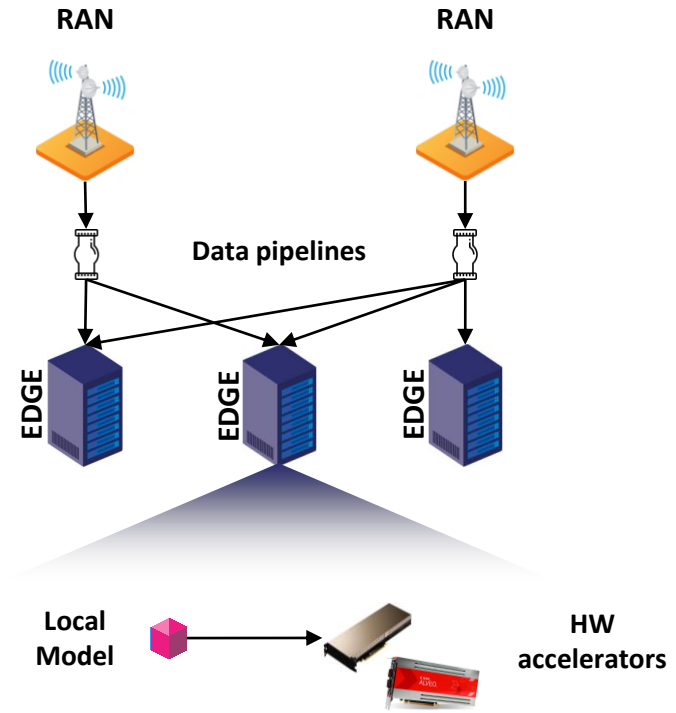


[1] Shekhar, Shubhranshu, Neil Shah, and Leman Akoglu. "Fairod: Fairness-aware outlier detection." Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. 2021.
[2] Abraham, Savitha Sam. "Fairlof: fairness in outlier detection." Data Science and Engineering 6 (2021): 485-499.

Decentralized Robust Security Analytics

Purpose: Detect and classify network threats through AI

- ***Edge analytics acceleration***
  - Employment of HW accelerators (e.g., FPGAs/GPUs)
  - Accelerate inference tasks
    - Enhance performance & reduce energy consumption
  - Approximation techniques
    - Tradeoff between accuracy loss (if any) and performance
    - Enabler towards <1ms latency required by 6G



PRIVATEER's High-Level Architecture

USER

RAN

EDGE/FOG

CLOUD

Distributed Security Analytics Engines

Attestation services & Credentials wallets

Verifier service

Proof-of-Transit verification services

NETWORK SLICE

User edge function

6GC edge function

User core function

6GC core function

Monitoring & Analytics Agents

Privacy-aware intent-based Orchestrator

Distributed Remote Index Identifiers

Edge Acceleration

Slice Manager

Service Orchestrator

RLC/MAC/PHY

Fog/Edge VIM & NFVI

Core VIM & NFVI

End User

DLT Distributed storage

Infra Provider

Service Provider

Threat Sharing

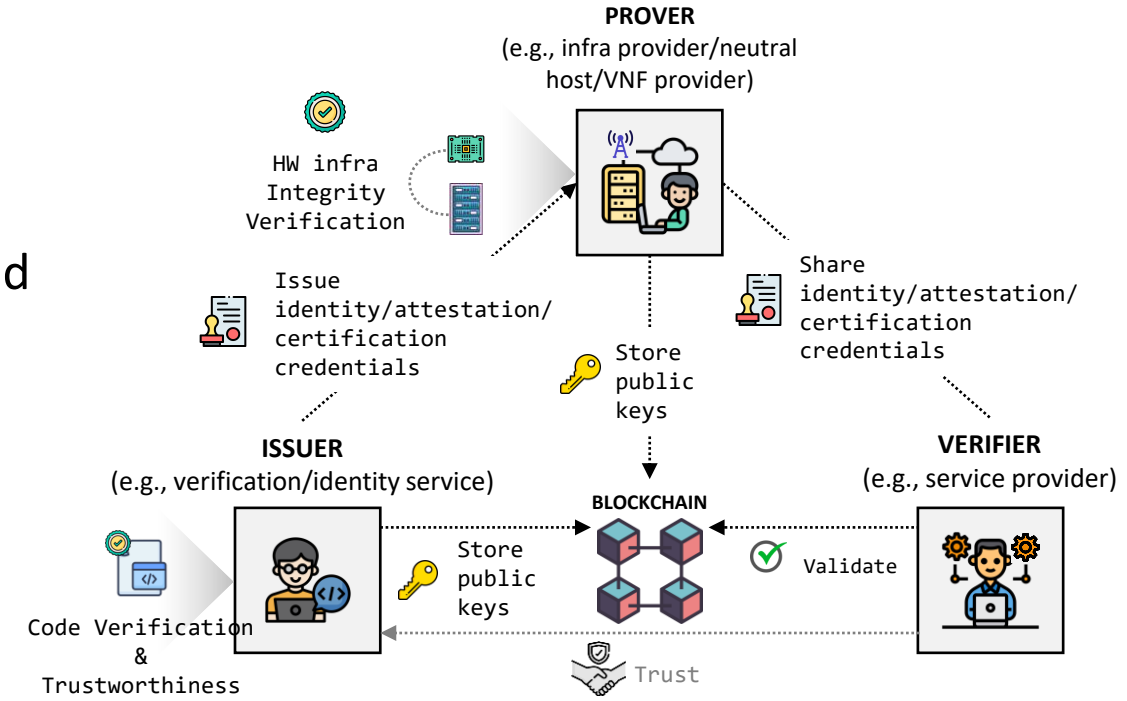
Threat Sharing

Threat Sharing

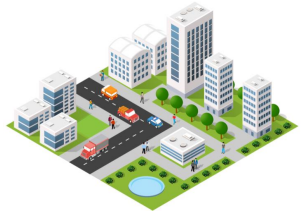
Distributed Attestation

Purpose: Privacy-preserving attestation and identification in a distributed manner

- ***Service & Infrastructure attestation***
  - Real-time supervision and verification of the operational assurance of applications
  - Integrity, authenticity and secure execution of accelerated applications
- ***Decentralized identifiers (DIDs):*** Store attestation results as Verifiable Credentials (VCs)
- ***Distributed Ledger Technology (DLT):*** Reliable attestation log and messaging platform



PRIVATEER's High-Level Architecture



USER | **RAN** | **EDGE/FOG** | **CLOUD**

Distributed Security Analytics Engines

Attestation services & Credentials wallets

Verifier service

Proof-of-Transit verification services

NETWORK SLICE

User edge function

6GC edge function

User core function

6GC core function

Monitoring & Analytics Agents

Privacy-aware intent-based Orchestrator

Distributed Remote Index Identifiers

Edge Acceleration

Slice Manager

Service Orchestrator

RLC/MAC/PHY

Fog/Edge VIM & NFVI

Core VIM & NFVI

End User

Threat Sharing

DLT Distributed storage

Infra Provider

Threat Sharing

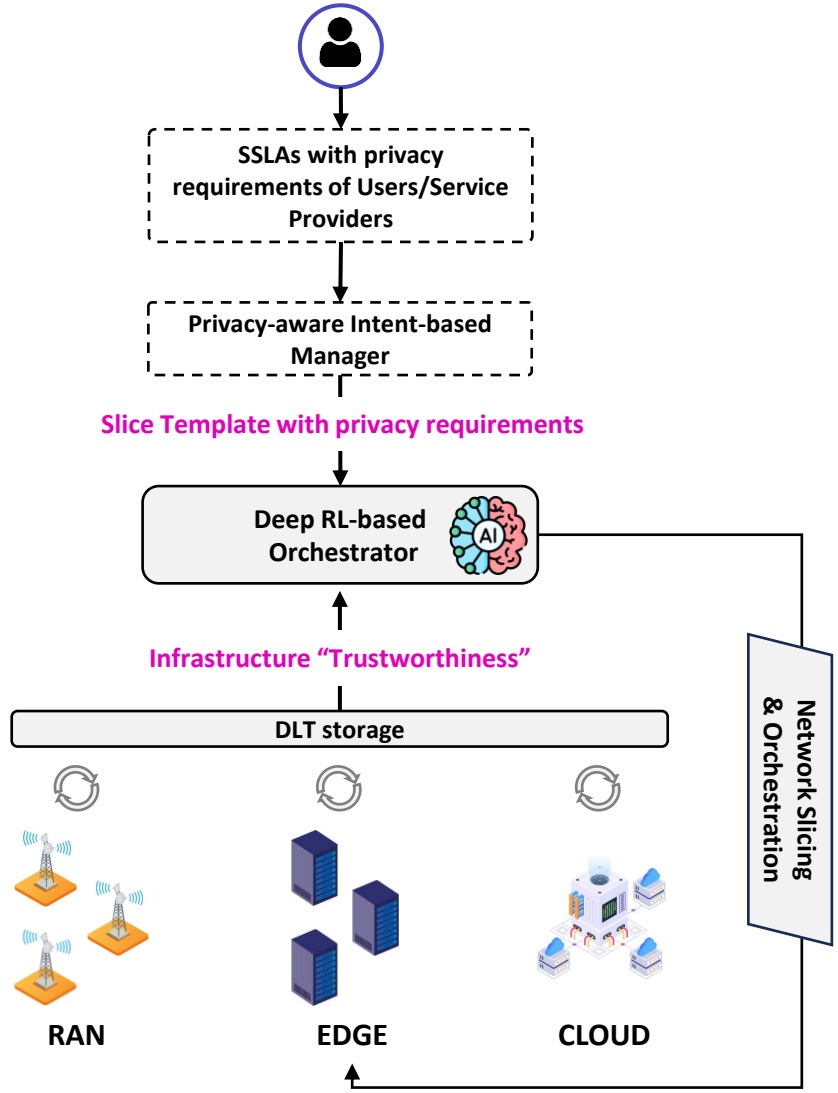
Service Provider

Threat Sharing

Privacy-aware Slicing & Orchestrator

Purpose: Orchestrate services across the continuum in a privacy- and intent-aware manner

- ***Privacy-aware, intent-based manager*:** Translates end-users' Security SLAs (SSLAs) to data model formats
- ***DLT storage*:** Stores and propagates "infrastructure's trustworthiness" evaluated from the attestation mechanisms
- ***Deep RL-based Orchestrator*:** Receives the above and performs autonomous network slicing & orchestrator
  - Privacy-aware rewards
  - FL to decentralize control loop without exchanging privacy-sensitive data



PRIVATEER's Use-Cases

PRIVATEER demonstrated through 5 use-case scenarios on two vertical domains

Key Milestones

March 2023

Threat Landscape Analysis

September 2023

PRIVATEER Framework Design

June 2024

PRIVATEER Beta Release

December 2025

PRIVATEER Final Release & UC demos

All technical deliverables will be public and most components will be open-sourced!

Conclusion

- 6G to play a key role in the evolution of the society towards the 2030's
  - Billions of devices connected to the Internet
- Security and Privacy as a fundamental concerns within EU's vision for 6G
- PRIVATEER HORIZON EUROPE project tackles security and privacy challenges
  - By developing **innovative security enablers** for 6G networks
  - Following a **privacy-by-design approach**
- PRIVATEER addresses 4 major challenges of future 6G networks
  - Security Analytics
  - Network Slicing & Orchestration
  - Infrastructure & Service Attestation and Verification
  - Cyber-threat intelligence sharing

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

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS JU. Neither the European Union nor the granting authority can be held responsible for them

Privateer_6GSNS

privateer-6gsns

@Privateer_6GSNS

privateer-contact@spacemaillist.eu