CONFIDENTIAL6G Newsletter - Latest Updates from the Project

CONFIDENTIAL6G is a Horizon Europe research and innovation project (Grant Agreement No. **101096435**) launched in January 2023. The project brings together **15 partners from 8 countries** to build the foundations for **confidentiality and privacy in future 6G networks**.

By combining advances in **confidential computing**, **privacy-preserving AI**, and **quantum-safe cryptography**, the project develops innovative mechanisms to ensure **data remains secure across the entire 6G cloud-edge continuum**—even while it is being processed.

Events and News

Open Source Summit Europe 2024
(Vienna, Sept 2024)

Partners Dušan Borovčanin (Ultraviolet) and Draško Drasković (Abstract Machines) represented CONFIDENTIAL6G at the Open Source Summit Europe 2024. They delivered a talk at the ***Confidential Computing Mini Summit*** on how confidential computing enhances security and privacy in next-generation 6G networks. Key points included **data security improvements, deployment challenges**, and future applications like secure edge processing and privacy-preserving AI.

Read more

New Partner: TU Wien
(Dec 2024)

Technische Universität Wien has joined the CONFIDENTIAL6G project as a partner. With a legacy of excellence since 1815, TU Wien is Austria's largest science and technology university, known globally for research and education.
This partnership strengthens the project's research capabilities in cryptography and security.

Read more

Secure Automotive Updates Seminar
(Belgrade, Feb 18, 2025)

Ana Kovačević (Zentrix Lab) presented her **research on secure automotive over-the-air (OTA) firmware updates** at a seminar hosted by the Mathematical Institute of the Serbian Academy of Sciences. She introduced a blockchain-based approach using Decentralized Identifiers (DIDs) to enhance the security of automotive software updates, a solution developed within CONFIDENTIAL6G.

Read more

FHE.org Conference 2025
(Sofia, Mar 25, 2025)

Antonio Guimarães (IMDEA Software Institute) was a **featured speaker at the FHE.org 2025** conference in Sofia. During his talk, held on March 25, 2025, Antonio shared valuable insights on secure computation and fully homomorphic encryption, showcasing CONFIDENTIAL6G's advances in these domains.

Read more

WSSS 2025 Workshop
(Tarragona, May 14, 2025)

The project took part in the ***Workshop on Secret Sharing Schemes (WSSS 2025)***, organized by the HERMES project and INCIBE. CONFIDENTIAL6G researchers joined this event to discuss state-of-the-art secret sharing techniques and how they can protect data confidentiality in 6G networks.

Read more

Use Case Highlights

Use Case 1 – Aviation Maintenance: This use case enables **secure data sharing** for predictive maintenance in aviation. Using **federated AI** and **blockchain**, airlines and manufacturers can collaborate without exposing sensitive data—improving safety, reducing downtime, and protecting data ownership.

Read more

Use Case 2 – Telecom Cloud Security: As telecom operators move to virtualized infrastructure, this use case applies **confidential computing** and **quantum-safe encryption** to secure cloud-native 5G/6G networks. The solution simplifies secure deployment and enhances trust in telecom services.

Read more

Use Case 3 – Connected Vehicles & OTA Updates: This use case secures **Vehicle-to-Infrastructure communication**, **OTA software updates**, and **federated learning** in real vehicles. With blockchain, digital IDs, and privacy-preserving AI, it ensures safe updates and smarter, more secure driving experiences.

Read more

Key Achievements from CONFIDENTIAL6G

CONFIDENTIAL6G is advancing secure, privacy-preserving, and intelligent connectivity for future 6G systems. Below are major achievements recently reported to the SNS.

Confidential Computing Toolkit

A comprehensive set of cryptographic libraries, SDKs, and tools for confidential computing and networking. **Key highlights:**

- Post-quantum threat analysis and migration strategy toward quantum-safe infrastructures
- Privacy-preserving technologies including Fully Homomorphic Encryption (FHE), Zero-Knowledge Proofs (ZKP), and Multi-party Computations (MPC)
- Hardware-accelerated cryptographic primitives and novel schemes for secret sharing

📄 **D2.1 Post-Quantum Analysis Report**
📄 **D2.2 Confidential Networking Toolkit**

Confidential Computing & Networking Elements
Design and implementation of secure architectures supporting both hardware-assisted and software-only privacy-preserving computation. **Key contributions:**

- Open, vendor-neutral software abstractions for secure enclaves and containers
- Decentralized data sharing framework combining Distributed Ledger Technologies, MPC, and TEEs
- Confidential AI workflow orchestration and enhanced resilience to side-channel threats

📄 **D3.1 Requirements and Architecture for Confidential Computing**
📄 **D4.2 Secure Decentralized Data Sharing**

Federated Learning in Connected Vehicles
A proof-of-concept showcasing federated learning in connected vehicles for traffic management and driving insights. **Highlights:**

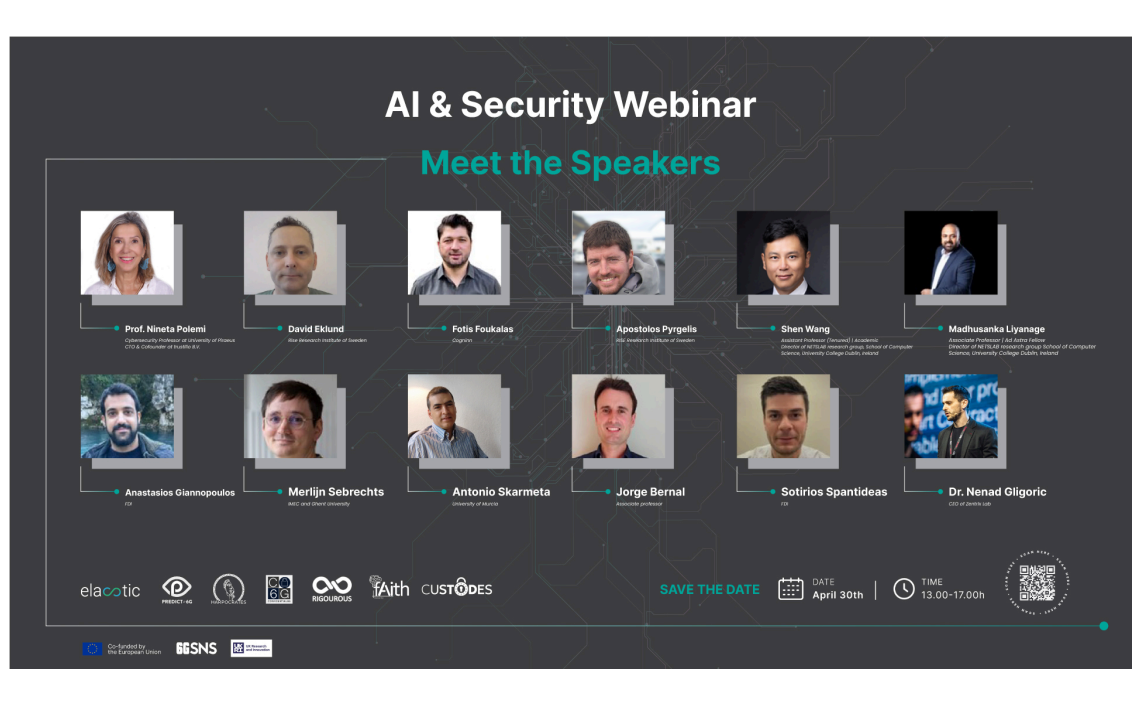
- Predicting congestion and cellular handovers using real-time data and recurrent neural networks
- Classifying driving behavior for safer, adaptive traffic systems
- Detecting road faults with on-board camera analysis

📄 **D5.1 Pilot Requirements and Integration Report**

Open-Source Contributions
One of CONFIDENTIAL6G's core strengths is its strong commitment to open-source. The project has released multiple tools supporting confidential computation and privacy-preserving technologies, enabling broader community adoption and collaboration.

Tool/Library	Link
ElGamal homomorphic encryption scheme	GitHub
BGV homomorphic encryption scheme (additive version only)	GitHub
Template library for (compressed) sigma protocols (ZKPs)	GitHub
Hybrid Homomorphic Encryption Benchmarking Library	GitHub
Aloha-HE: Hardware Accelerator implementation	GitHub
Accelerating Multiparty Noise Generation Using Lookups	GitHub
Multi-Party Homomorphic Encryption Library	GitHub
Two-party Computational Differential Privacy implementation	GitHub

AI & Security Webinar (April 30, 2025)



CONFIDENTIAL6G co-organized an **"AI & Security" webinar** on April 30, 2025, in collaboration with four other EU projects ELASTIC, PREDICT-6G, HARPOCRATES, RIGOUROUS with support from FAITH, CUSTODES, and 6G-Cloud. This online event focused on the intersection of artificial intelligence and cybersecurity for next-generation mobile networks (6G). Experts from each project presented recent research and solutions addressing emerging security challenges in AI-driven 6G systems. Key topics included privacy-preserving AI techniques, AI-based network resilience, and the use of blockchain for network management. **Notably, two University College Dublin researchers from CONFIDENTIAL6G** spoke at the webinar: **Dr. Shen Wang** presented on privacy-enhanced federated learning in 6G networks, and **Dr. Madhusanka Liyanage** discussed blockchain-enabled decentralized spectrum access for 6G. Their contributions showcased how CONFIDENTIAL6G technologies can secure AI operations and network functions in future wireless networks.

Watch the webinar

EuCNC & 6G Summit 2025 Highlights

CONFIDENTIAL6G had a strong presence at the **2025 EuCNC & 6G Summit** (June 3–6, 2025 in Poznań, Poland). The team showcased the project's latest innovations for secure and private 6G networking, demonstrating how our cryptographic enablers and frameworks protect data across the cloud-edge continuum. CONFIDENTIAL6G joined over 70 SNS JU projects in exhibiting demos and results, contributing to workshops and sessions focused on 6G security and trust technologies. In addition, the project was featured in the **SNS JU Journal 2025**, which was released at EuCNC. This annual journal highlights progress across Europe's 6G research projects; the 2025 edition included an article on CONFIDENTIAL6G's approach to confidentiality and privacy in 6G. Attendees at EuCNC could pick up the journal and visit the CONFIDENTIAL6G booth to learn how the project is paving the way for quantum-resistant, privacy-preserving 6G infrastructures.

Read SNS Journal 2025

Technical Articles

Protecting Privacy in the 6G Era

This March 2025 article explores the growing privacy risks in 6G networks, which will handle massive volumes of sensitive data. It highlights solutions like encryption, differential privacy, and secure multi-party computation to ensure data remains protected in highly connected environments.

Read more

Processing Without Exposure

Published in May 2025, this post explains how CONFIDENTIAL6G uses **confidential computing**—including TEEs and homomorphic encryption—to process encrypted data without exposing it. This approach supports privacy-preserving AI and secure analytics across the cloud-edge continuum.

Read more

Contributing to the Scientific Community

The CONFIDENTIAL6G consortium continued to advance scientific research, publishing several papers in journals and conferences:

- ***"Secure and Efficient Transciphering for FHE-based MPC."* – Diego F. Aranha, Antonio Guimarães, Clément Hoffmann, Pierrick Méaux:** A new method to convert encrypted data for efficient use in multi-party computation with fully homomorphic encryption.
- ***"Verifiable Computation for Approximate Homomorphic Encryption Schemes."* – Ignacio Cascudo, Anamaria Costache, Daniele Cozzo, Dario Fiore, Antonio Guimarães, Eduardo Soria-Vazquez:** Introduces techniques for verifiable computing on data encrypted with approximate (non-exact) homomorphic schemes.
- ***"Aloha-HE: A Low-Area Hardware Accelerator for Client-Side Operations in Homomorphic Encryption."* – Florian Krieger, Florian Hirner, Ahmet C. Mert, Sujoy Sinha Roy:** This work presents a lightweight hardware engine to speed up homomorphic encryption tasks on devices.
- ***"Minimize the Randomness in Rasta-Like Designs: How Far Can We Go?"* – Lorenzo Grassi, Fukang Liu, Christian Rechberger, Roman Walch, Fabian Schmid**: Analyzes cipher designs to reduce randomness requirements, improving efficiency of cryptographic primitives.
- ***"Practical Two-Party Computational Differential Privacy with Active Security."* – Fredrik Meisingseth, Christian Rechberger, Fabian Schmid:** Proposes a two-party protocol that achieves differential privacy with provable security against active adversaries.
- ***"Accelerating Multiparty Noise Generation Using Lookups."* – Fredrik Meisingseth, Christian Rechberger, Fabian Schmid:** Describes a technique to speed up the generation of noise terms in MPC protocols via lookup tables.
- ***"Skyscraper: Fast Hashing on Big Primes."* – Clémence Bouvier, Lorenzo Grassi, Dmitry Khovratovich, Katharina Koschatko, Christian Rechberger, Fabian Schmid, Markus Schofnegger:** Introduces a new high-speed hash function design optimized for large prime fields, with applications in zero-knowledge and blockchain.
- ***"Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi."* – Katharina Koschatko, Reinhard Lüftenegger, Christian Rechberger:** Explores advanced algebraic cryptanalysis techniques on the Anemoi cipher using Gröbner bases.
- ***"Opening the Blackbox: Collision Attacks on Round-Reduced Tip5, Tip4, Tip4′ and Monolith."* – Fukang Liu, Katharina Koschatko, Lorenzo Grassi, Hailun Yan, Shiyao Chen, Subhadeep Banik, Willi Meier:** Details new cryptanalysis results, finding collision vulnerabilities in reduced-round versions of several symmetric primitives (Tip5, Tip4, Monolith), contributing to the cryptographic analysis efforts in CONFIDENTIAL6G.

CONFIDENTIAL6G Consortium

CONFIDENTIAL6G

Keep in touch with us!
Stay updated on CONFIDENTIAL6G news, results and upcomming events.