Emerging Tech Conference Edge Intelligence (ETCEI 2024)

SAND5G - Security Assessments for Networks and Services in 5G Networks: From 5G to Edge

Kostas Lampropoulos[1], Kostas Pournaras[2], Christos Tranoris[2], Odysseas Koufopavlou[1], Spyros Denazis[1], Paris Kitsos[1, 3]

[1]University of Patras, [2]p-net, [3]University of the Peloponnese

Patras, Greece

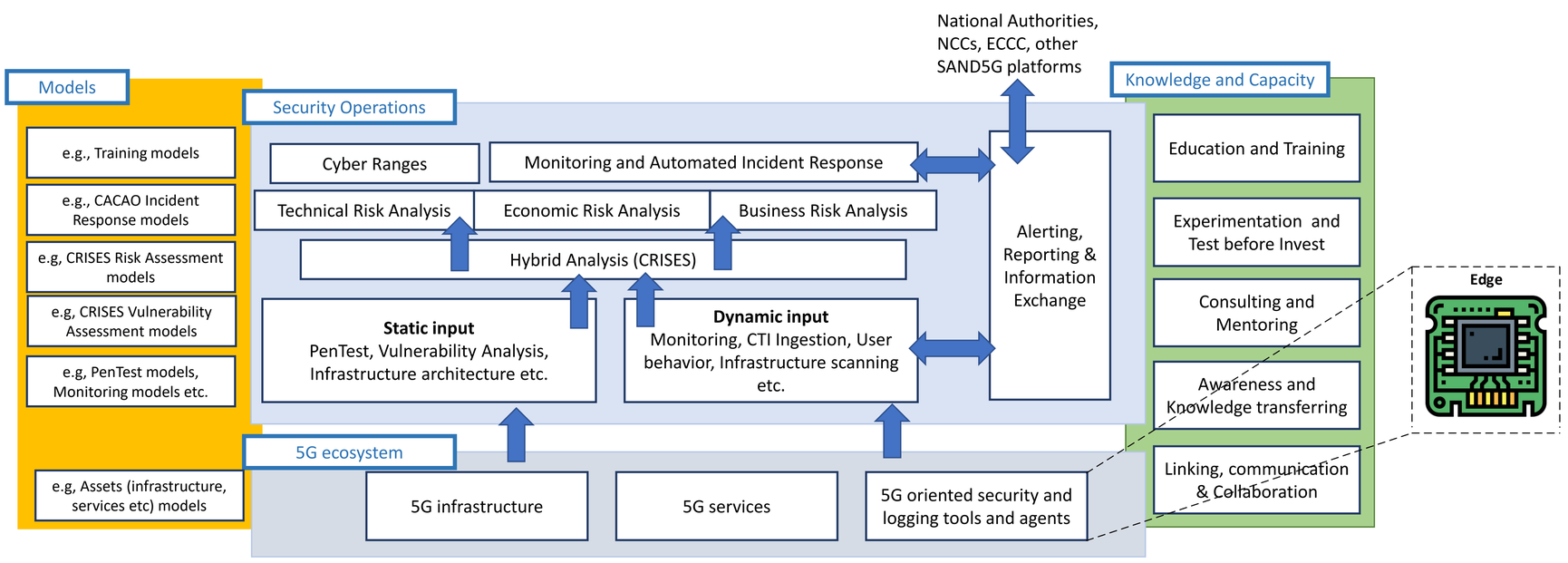
Abstract

In the framework of SAND5G, funded by Digital Europe Programme (DIGITAL) under the Cybersecurity and Trust (DIGITAL-ECCC-2022-CYBER-03) call, an efficient architecture proposed and integrated to deliver a risk assessment platform to help 5G stakeholders secure their systems, enable national authorities to oversee security measures, and align with European cybersecurity policies and proposed EU toolbox for 5G security.

Introduction

- 5G solutions necessitate a transformation of networks using open, cloud-native technologies. Both the Radio Access Networks (RANs) and the core network need to be designed with a distributed architecture, leveraging cloud-native, disaggregated, and open infrastructure to enable automated delivery of diverse services.
- Bringing computing power and network functions closer to the network edge enhances application performance, reduces bandwidth use and costs, and supports the creation of innovative, low-latency services.
- The services often require real-time data streaming for applications like virtual and augmented reality, autonomous and connected vehicles, drones, telemedicine, and Industry 4.0.
- Cybersecurity plays a crucial role in this transformation, involving the implementation of security systems, solutions, and strategies that safeguard critical business and customer data.
- Cybersecurity, includes network security, internet security, endpoint security, API security, cloud security, application security, container security, and many more.
- Edge security can take place either on devices located closer to the end-user device (such as routers or local data centers) or directly on the end-user device itself (like a sensor or other IoT device).

Extended Architecture of SAND5G



- Secure Edge Devices
  - Minimum access and permissions necessary
  - Encrypted data
  - Authentication and authorization
- Collect and analyze data
- FPGAs (e.g. a RISC-V implementation)
- Google Edge TPU
- Raspberry Pi 3
- Root-of-trust

Consortium

Acknowledgments

This article describes work undertaken in the context of the SAND5G project, “Security Assessments for Networks anD services in 5G” which has received funding from the European Union’s Digital Europe programme under grant agreement No 101127979 and is supported by European Cybersecurity Competence Center. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Contact Information

Prof. Odysseas Koufopavlou (odysseas@upatras.gr)

Dr. Konstantinos Lampropoulos (klamprop@ece.upatras.gr)

Prof. Paris Kitsos (pkitsos@upatras.gr)