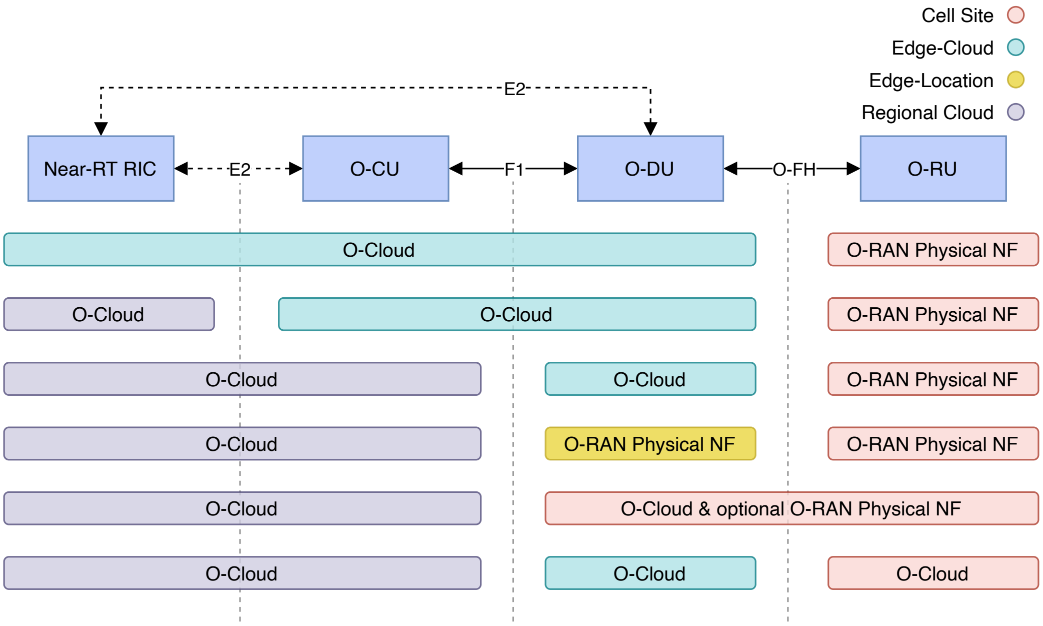
6G-RIC
Research and Innovation Cluster

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Open RAN for Next-G Secure Telecommunication Platforms

FELIX KLEMENT, ALESSANDRO BRIGHENTE, MICHELE POLESE, WUHAO LIU, MAURO CONTI AND STEFAN KATZENBEISSER

How can we analyze the new threat environment in a programmatic way? How can the expanding virtualization surface be secured?



In Next-Gen RANs, there are many possible combinations of the different deployment variants. The figure shows how the individual network functions (in the upper part of the figure) can be used and combined either as PNF or as Cloudified NF. This results in a total of six different scenarios, which differ in terms of the use of the respective O-RAN key technology and the deployment location used. O-RAN PNF means that it is a fully-fledged physical O-RAN network function. There may also be mixed forms between the two.

KEY FINDINGS

The Radio Access Network (RAN) paradigm is moving towards the next generation of wireless networks. As part of this transition and the concurrent development of Open RAN methodologies, it is critical to address the emergence of several new threats that significantly impact network security.
In response to this imperative, we have introduced a novel methodology that integrates the MITRE ATT&CK framework with empirical evidence to evaluate specific threats arising during the migration to open 6G networks.
Moreover, in a separate study, we explored the security implications of virtualizing RAN network deployments through O-RAN using Kubernetes. We identified essential best practices essential for ensuring a secure deployment and presented them for consideration.

Securing the Open RAN Infrastructure: Exploring Vulnerabilities in Kubernetes Deployments / Felix Klement, Alessandro Brighente, Michele Polese, Mauro Conti, Stefan Katzenbeisser

Towards Securing the 6G Transition: A Comprehensive Empirical Method to Analyze Threats in O-RAN Environments / Felix Klement, Wuhao Liu, Stefan Katzenbeisser
IEEE Journal on Selected Areas in Communications, 2023