# From Confidential Cloud Computing to Next-Generation Edge Computing

Patrick Jauernig

Sanctuary

System Security Lab, TU Darmstadt

sanctuary

System Security Lab

TECHNISCHE UNIVERSITÄT DARMSTADT

# Sanctuary @ TU Darmstadt

**Emmanuel Stapf**

M.Sc. IT Security,
Computer Science &
IT Management

**Patrick Jauernig**

M.Sc. IT Security,
Computer Science &
IT Management

**Ferdinand Brasser**

Dr.-Ing.
M.Sc. IT Security

**Ahmad-Reza Sadeghi**

Prof. Dr.-Ing.
Co-Founder Sirrix AG

## Security Expertise

Deep knowledge in
security solutions

## Research Excellence

Publications on top-tier
IT security conferences

## Real-World Impact

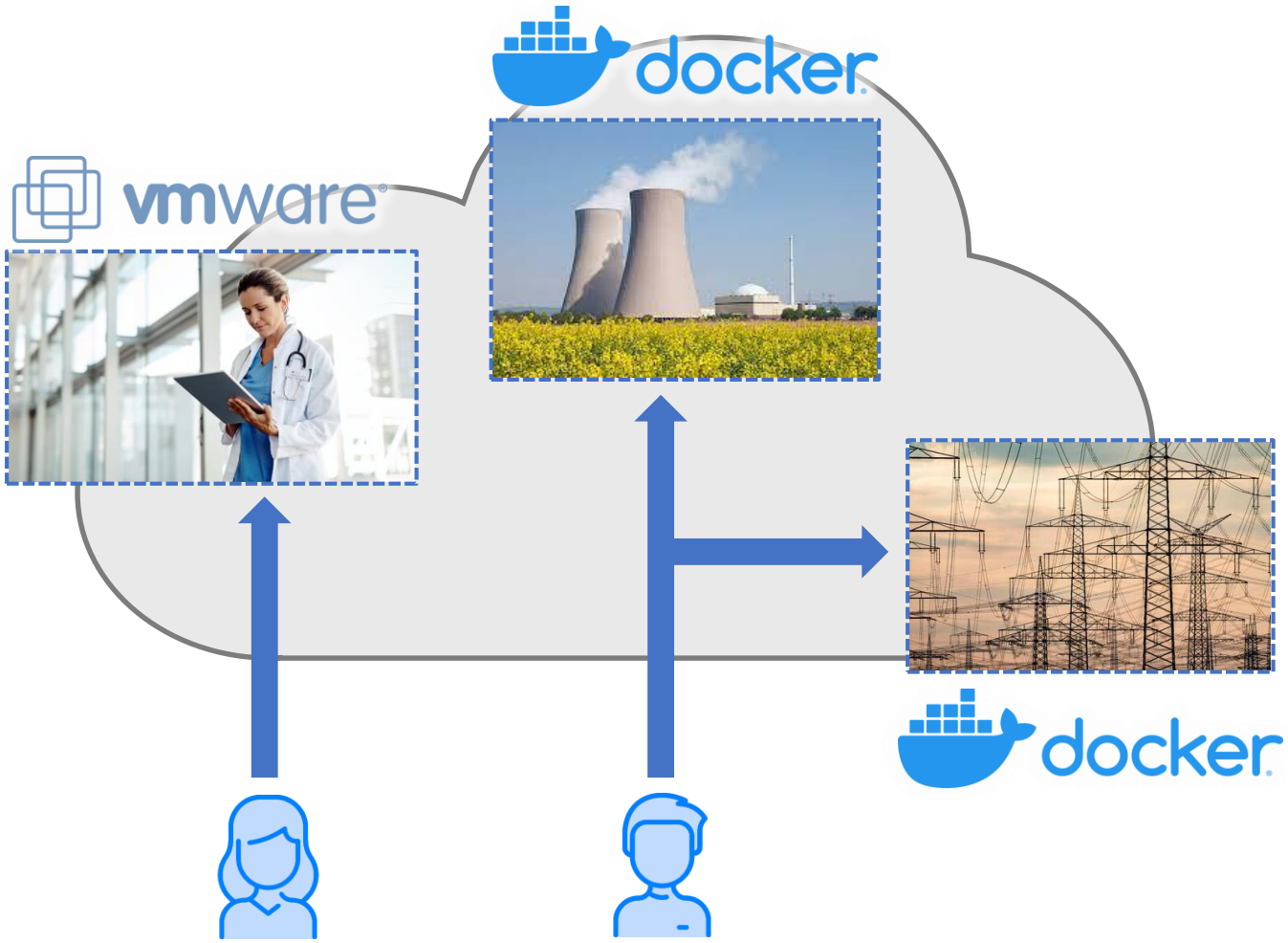
Successful collaboration within
high-profile industry projects

sanctuary

startup secure ATHENE

Bundesministerium für Bildung und Forschung

# The Confidential Computing Dilemma




- Diverse cloud-native workloads
  - IaaS, CaaS, PaaS
- Inflexible security solutions
  - Inefficient workarounds to support different workloads
- Complex deployment & mgmt.
  - Requires expert knowledge

sanctuary

# Research Directions

- Adapt TEEs to support cloud workloads
  - Combine TEEs & containers: Google (AMD SEV), MS Azure (Intel SGX)

- We are not there yet!
  - Secure orchestration of containers is an open research challenge
  - TEEs need to get more flexible

**Trusted Container Extensions: A Security Architecture for Container-based Confidential Computing**

**Abstract:** Cloud computing has emerged as a corner stone of today's computing landscape. More and more

**1 Introduction**

sanctuary

# Edge Computing Gains Traction

- Connection to embedded edge devices gets more important

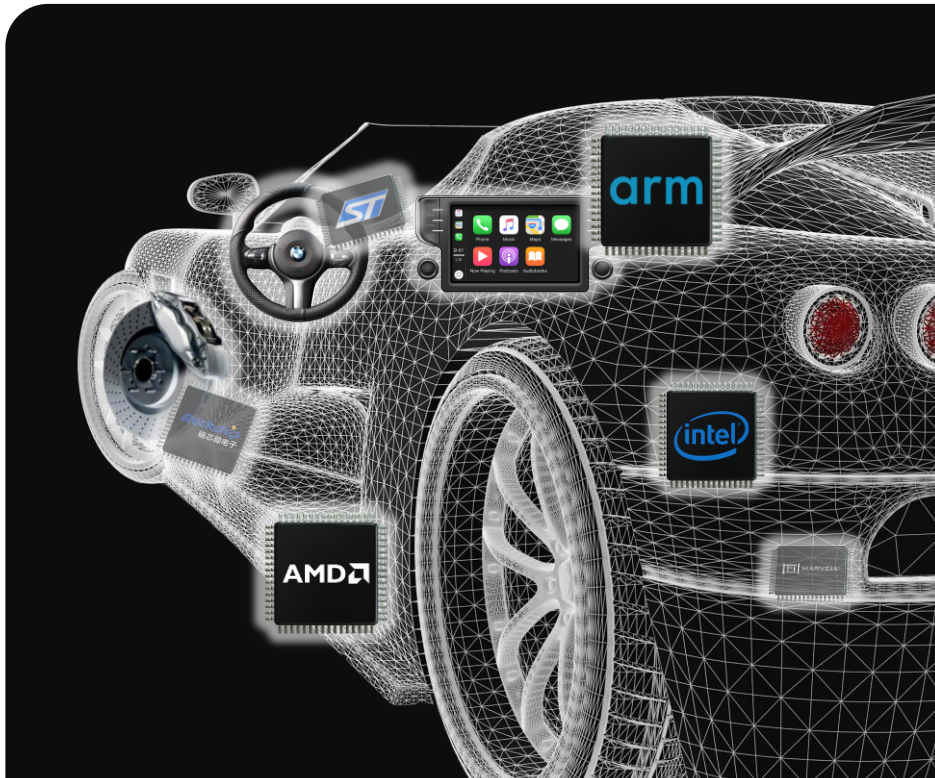
- Major driver for
  - autonomous cars & v2x
  - compute-heavy spacecraft
  - critical infrastructure

sanctuary

# Confidential Edge Computing

- Challenges
  - Highly individual, highly distributed systems
  - Tedious deployment/communication

- Our approach:
  - Service consolidation
    - E.g., using virtualization
  - TEEs for confidential edge computing
    - Security Services
  - Cloud-native deployment & management




sanctuary

# Takeaways

- Confidential Cloud Computing is possible today

- Next step: bridging the gap to Confidential Edge Computing
  - Leverage TEEs, also for measuring integrity
  - Bring Cloud workflows to the Edge



Contact us at info@sanctuary.dev