

Toward Secure & Reliable HPC Workloads: Leveraging eBPF for Syscall Filtering

Anila Ghazanfar, Julian Kunkel

Motivation

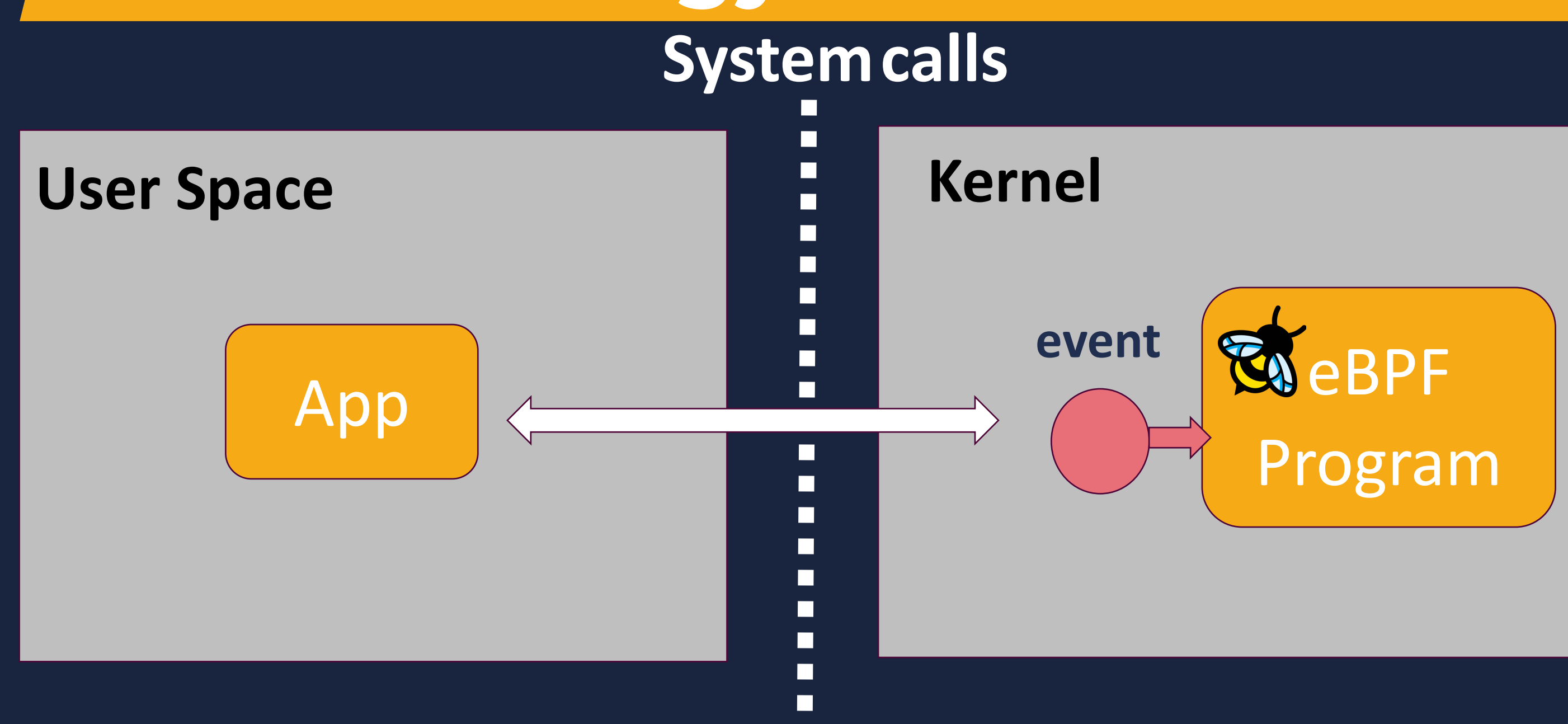
- HPC workloads in shared data centers require **reliable and isolated execution**.
- Conventional fault tolerance** adds overhead and lacks security integration.
- Similarly, **traditional security mechanisms** add performance overheads and lack fine-grained control.
- Healthcare systems** require compliance with privacy regulations, as failures or breaches can disrupt critical tasks.
- Need for **adaptive fault tolerance** and **lightweight security mechanisms**.

 eBPF Syscall filtering brings security at the kernel level for HPC Workloads.

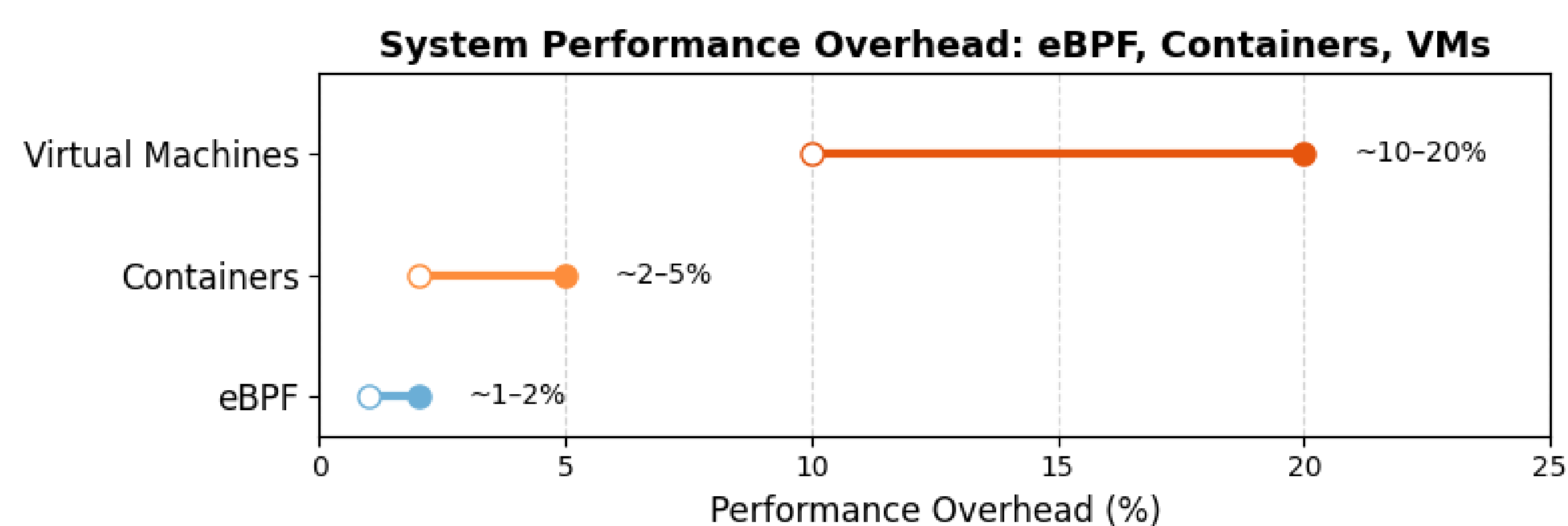
Research Objectives

- Design a unified framework that integrates **fault tolerance and security** in heterogeneous HPC systems.
- Design and implement **eBPF-based system call filters** to enhance security by restricting unauthorized file I/O access.
- Ensure **minimal performance overhead** compared to existing solutions (e.g., SELinux, seccomp).

Methodology



Comparison



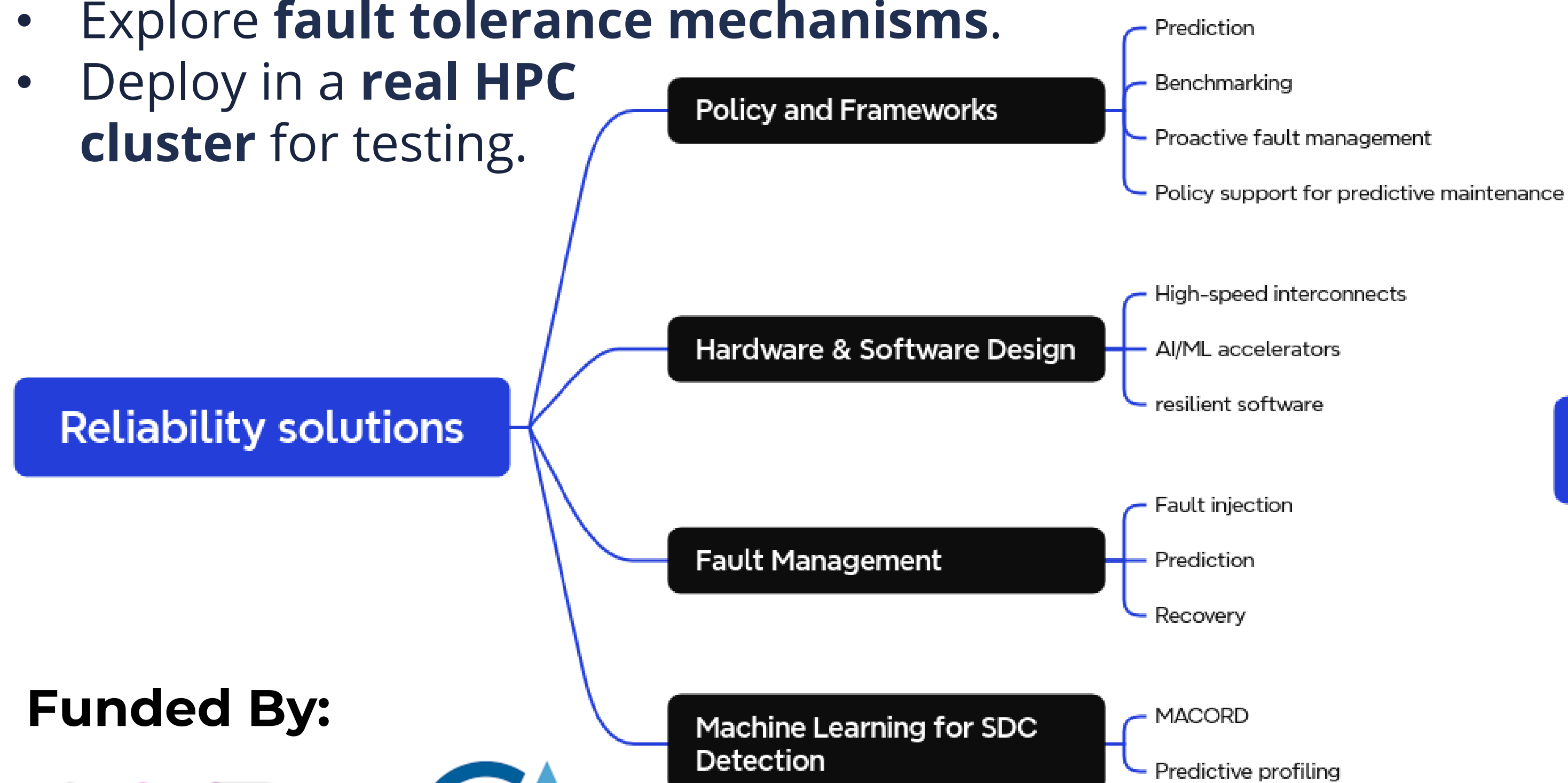
Note: Values are approximate; ranges are based on findings from multiple sources (see references).

Expected Contributions

- Unified lightweight framework** for enhancing both reliability and security in HPC.
- Performance evaluation and Trade-off analysis** between security overhead and fault-tolerance mechanisms in HPC.
- Open-source toolkit** for security and failure event detection.

Future Work

- Expand filtering to **network and GPU syscalls**.
- Explore **fault tolerance mechanisms**.
- Deploy in a **real HPC cluster** for testing.



Funded By:



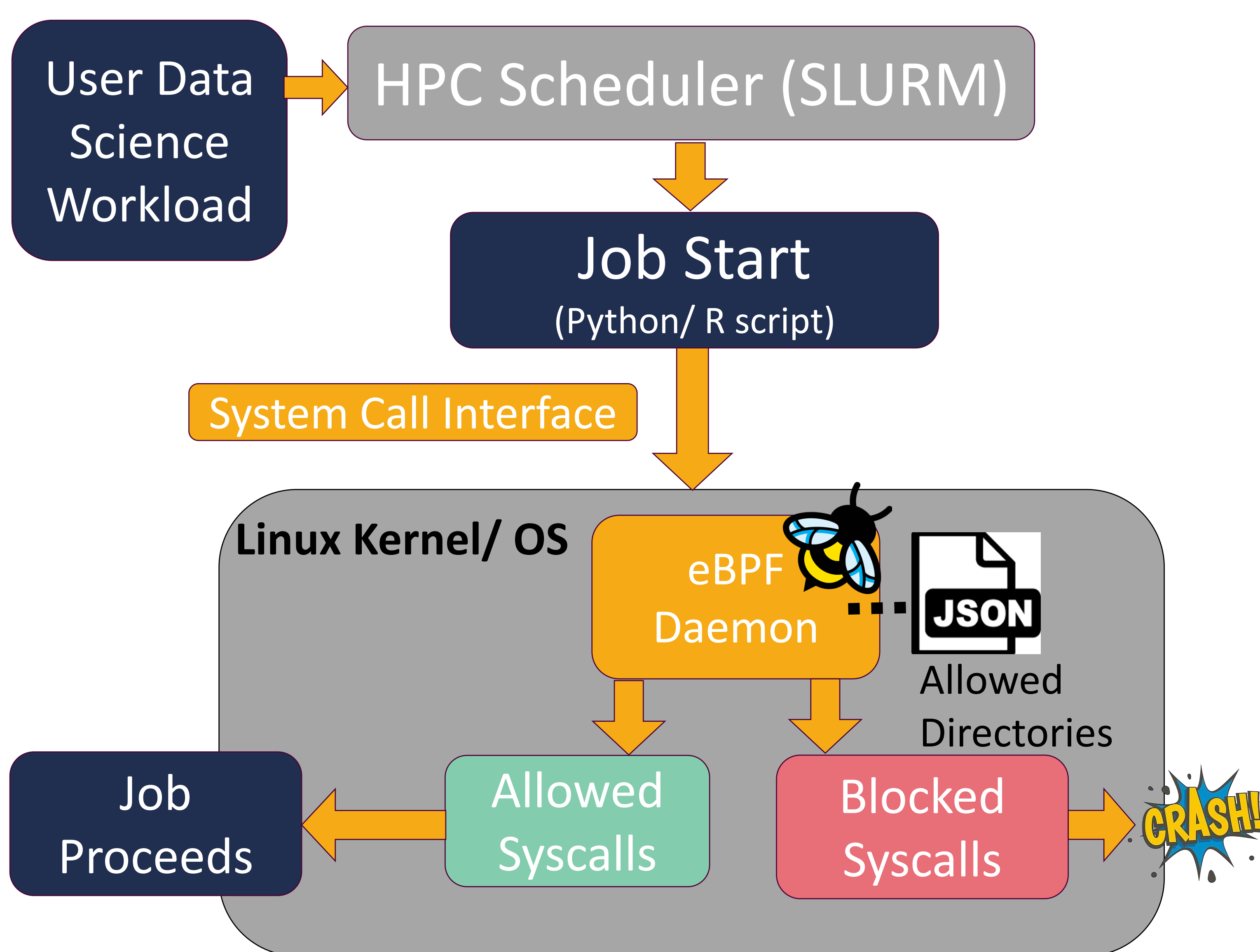
Anila Ghazanfar

[✉ anila.ghazanfar@stud.uni-goettingen.de](mailto:anila.ghazanfar@stud.uni-goettingen.de)

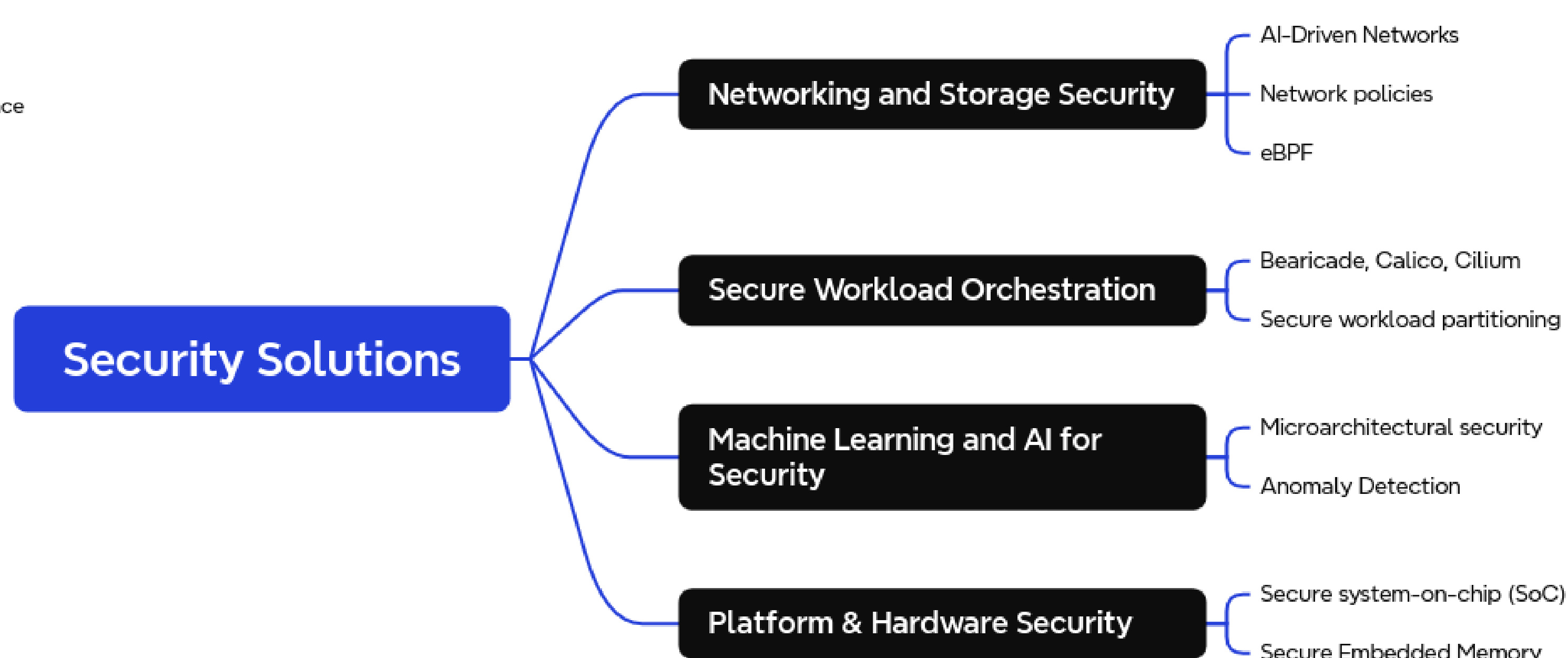
Prof. Dr. Julian Kunkel

[✉ julian.kunkel@gwdg.de](mailto:julian.kunkel@gwdg.de)

Planned HPC Workflow



Analysis



References

- Jia, J. et al. (2023). Programmable System Call Security with eBPF. arXiv:2302.10366.
- Li, Z. et al. (2017). Performance Overhead Comparison between Hypervisor and Container based Virtualization. arXiv:1708.01388.
- van Rijn, V., & Rellermeier, J. S. (2021). A Fresh Look at the Architecture and Performance of Contemporary Isolation Platforms. Middleware 2021.