Adaptive and Trusted Execution in the Cloud-Edge Continuum

The rapid growth of cloud-edge computing has driven a shift in how data processing and storage are managed. By combining cloud and edge resources, this continuum supports low-latency responses, real-time data processing, and scalable applications. However, guaranteeing adaptive and trusted execution across diverse environments, from cloud datacenters to edge devices, presents unique challenges. Technologies such as Trusted Execution Environments (TEEs) (e.g., Intel TDX, AMD SEV, ARM TrustZone, M-chip) offer hardware-level security to ensure data confidentiality and integrity. Furthermore, emerging tools like Web Assembly (Wasm) enable flexible and secure application execution across heterogeneous infrastructures. Integrating these innovations into an adaptive framework that balances performance, security, and energy efficiency remains a key research problem.

Problem Statement and Challenges

Current cloud-edge systems lack robust frameworks for adaptive, trusted execution that optimise performance without compromising security. Key challenges include:

1. **Heterogeneous Environments**: The cloud-edge continuum encompasses a mix of devices, networks, and protocols, creating a complex landscape for consistent security and adaptive performance.
2. **Real-Time Adaptability**: Dynamically varying resources and workloads require adaptive execution strategies that can respond instantly without sacrificing security.
3. **Security and Privacy**: Ensuring end-to-end security and privacy across different devices is critical, but many traditional models struggle to adaptively manage security requirements, particularly for lightweight edge nodes.
4. **Energy Efficiency**: Balancing energy efficiency with security on resource-constrained edge devices is vital to avoid excessive power consumption and maximise performance.

Objectives

This research will develop an adaptive framework leveraging TEEs, Wasm, eBPF, and other innovative tools to deliver secure, efficient, and scalable execution across the cloud-edge continuum. The primary objectives are:

1. **Design Adaptive Execution Strategies**: Develop algorithms that leverage WebAssembly (Wasm) for portable, lightweight execution, dynamically allocating tasks across cloud and edge resources with optimal performance-security trade-offs.
2. **Integrate Device-Specific TEEs**: Explore hardware TEEs (e.g., TDX for Intel, SEV for AMD, TrustZone for ARM, M-chip for Apple) to ensure confidentiality and integrity of computations across different environments.
3. **Implement Real-Time Monitoring with eBPF**: Use eBPF-based monitoring to achieve high-performance, low-overhead visibility into system behavior, enabling real-time adjustment based on security and workload demands.
4. **Develop a prototype system**: Test the framework's robustness in real-world applications e.g., smart home, validating its effectiveness under various attack models and resource constraints.

Supervisor:

Dr Devki Nandan Jha
Lecturer, School of Computing, Newcastle University
Visiting Researcher, University of Oxford
Email id: dev.jha@ncl.ac.uk