Hybrid Approaches for Secure Cloud Computing

**Topic**

Computing in third-party datacenters – so-called “clouds” – has many benefits. Due to multi-tenancy and other intrinsic characteristics, public clouds are however considered to be insecure. Several techniques have been employed to overcome the security limitations of such clouds in practice, including most notably garbled circuits and partially homomorphic encryption. Intel has also recently released the SGX CPU security enhancements. Each of these techniques has its benefits and limitations.

### Tasks

The goal of this thesis is to investigate the combination of different techniques such as garbled circuits and partially homomorphic encryption for efficient secure cloud-based big data analysis. Tasks include:

- The analysis and comparison of different techniques.
- The implementation and evaluation of program analysis and compile-time support for the application of combined techniques.

### References


### Contact

**Prof. Dr. Stefan Katzenbeisser**
katzenbeisser@seceng.informatik.tu-darmstadt.de

**Prof. Dr. Patrick Eugster**
peugster@dsp.tu-darmstadt.de