Contribution ID: **53** Type: **Talk (15min + 5min)**

Collaboration without data sharing: the Federated Secure Computing architecture

Tuesday 25 February 2025 17:35 (20 minutes)

In domains with relevant security or privacy concerns, open data sharing among cooperation partners is often not an option. Here, cryptography offers alternative solutions to reconcile cooperation and data protection. Participants engage in peer-to-peer computation on encrypted data, arriving jointly at the intended result, without ever having access to each other's input data. While elegant in theory, this approach has its own challenges in terms of complexity, DevSecOps and cloud federation.

Federated Secure Computing is a free and open source initiative hosted by LMU Munich and financed by Stifterverband. The middleware between client-side business logic and server-side cryptography backend is designed to let research software engineering practitioners use secure computing with ease. It lets students write simple secure logic with as little as ten lines of Python code and can be run on IoT hardware such as Raspberry Zeros.

In this talk, we present real-world use cases and learnings in terms of state-of-the-art administrative and technical data protection measures.

I want to participate in the youngRSE prize

no

Primary authors: GOELZ, Christian Johannes; BALLHAUSEN, Hendrik

Presenter: BALLHAUSEN, Hendrik

Session Classification: Security of Research Software

Track Classification: Research Software: Cloud Technologies