

Secure Multi-Party Computing in the Cloud

Ben Getchell, Boston University

Abstract

Data is important, sharing and collaboration are important, but so is protecting the data, even from collaborators. We will present how we are combining a multi-party computation system (Conclave) and a dataset repository solution (Dataverse) on The Massachusetts Open Cloud (MOC) to enable “paranoid” parties to collaborate on joint computations over the public cloud. Using this framework some (or all) parties’ datasets will remain confidential, but the parties can run specific analytics over their collective data. This is crucial because 40 years of encryption history shows that crypto solutions only achieve widespread adoption once they are frictionless to users.

Speaker Bios



Ben Getchell is a Software engineer at SAIL, within the Hariri Institute for Computing.