Trellis++ a Practical Privacy-Preserving Food Safety Framework
Servio Palacios, Aaron Ault, James Krogmeier, Bharat Bhargava

Motivation
As IoT data volumes increase in a privacy-conscious world, an alternative model where provable computation happens closer to the data is needed. Unfortunately, including the edge in the computational resources can lead to a higher risk of data leakage or theft of confidential data.

Goals
• Move parts of the computational kernels to the edge of the network to take advantage of the computational capabilities of the edge nodes [1].
• Address a critical issue on edge computing: producing auditable computations that also prevent theft of confidential data.

Use case
• This project aims to prove the safety of food through its lifecycle computing on encrypted data to obtain proof of safety while keeping all these data private to the requirements of the data owners.

Trellis++ Architecture

Contributions
• Oblivious smart contracts
• A privacy preserving computation framework
• An opensource implementation [2]

References