Go0: Reimagining Data, Privacy, and the Internet with Zero-Knowledge Computing and Distributed Systems

Chinya Salimpasha, Mohammed Suhail (School: The Learning Centre)

Data security and privacy stand critical in today’s internet infrastructure, yet 2018 - witnessed disastrous data breaches affecting 2B people across the globe. Background audit reveals existing authentication systems (login, payments) post sensitive data from the client device to the server and save the credentials in a database during the registration phase and repeat the process to authenticate against the database. These storage points (databases) are hotspots for a bad guy; from where all the data disaster begins. To address this, I built a new system that leverages zero knowledge computing and private distributed systems - Go0. Zero knowledge computing enables authentication(registration/authentication) without exchanging user data between client and server. Hence a database isn’t required for ZKP based systems. With an Iterative design approach, I designed a protocol with the outline of mathematical proofs introduced in Fiat-Shamir's Zero Knowledge Heuristics. I started engineering a powerful set of web services; Go0 Login, Go0 Pay and Go0 KYC. That demonstrates the capabilities of zero knowledge computing for specific use cases without sending user data on submit or storing it in the server side during registration and authentication. I harnessed the unique characteristics of distributed ledgers with my Go0 web services for user recovery operation and KYC. The protocol and web services were tested successfully against 30+ cryptographic attack environments and with an authentication latency. The Highlight of the research is able to do authentication in diverse use cases with zero knowledge computing and validating its practical implementation, feasibility and impact at large. Zero data shared = Zero Worries of Data Breaches|go0 apps - https://go0.io/try