Overview

Internet has tremendous untapped potential for cooperation.

Now: limited, ad hoc sharing, with uncertain security.

Goal: secure, reliable computation and storage on a highly available decentralized infrastructure.

Example Applications

Unified Medical Database: Hospitals share a single, consistently updated medical record for each patient.

Wikipedia++: A universal knowledge repository. Each user has a distinct view according to security privileges.

Decentralized Social Networking: Data can be used by any application while enforcing user privacy.

Language Features

Information-flow annotations provide explicit per-object confidentiality and integrity policies.

Confidentiality policy: 
{Patient -> Doctor, Insurance}

Integrity policy: 
{Patient <- Doctor}

Transactions provide a simple conceptual framework for managing concurrency.

Persistence annotations prevent unexpected dangling references while avoiding the “persist-the-world” phenomenon.

Challenges

Automatic partitioning of data and code based on security policy.

Dissemination of popular objects while enforcing consistency and security.

Transactions spanning multiple clients and trust domains.

Function-shipping moves computation closer to data.