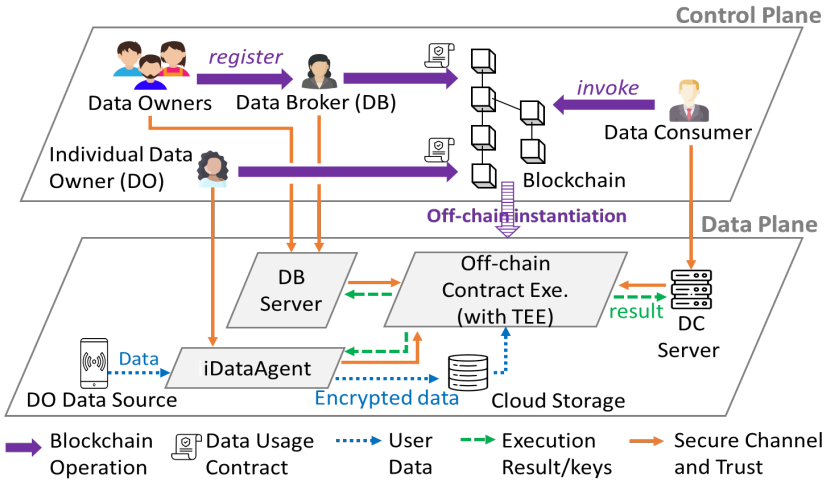
Toward Enforceable Data Usage Control in Cloud-based IoT Systems

VIRGINIA TECH

Washington University in St. Louis

Challenge:

- **Data Usage Control** as a Privacy Goal: Data owner defines "who can use my data for which purpose at what condition, price, etc."
- A technical mechanism to enforce such usage policy —enabling a secure and trustworthy data sharing economy.



Scientific Impact:

- New data usage control framework and enforcement mechanism to enable new privacy goal---preventing second-hand unauthorize data uses
- The new data usage control framework is applicable to wider domains, e.g., user-controlled data sharing in medical research.

Solution:

- Blockchain smart contract for enforcing the data usage policy, usage record keeping (for auditability), and DO compensation.
- Trusted execution environment (TEE) for executing the DC applications off-chain without exposing plaintext data into untrusted cloud.
- Secure result commitment protocol for a fair and atomic DO-DC transaction.

Broader Impact and Broader Participation:

- Open-sourced software implementation at: https://github.com/yang-sec/PrivacyGuard
- Developed 4 new courses in the cyber security master program.
- Developed multiple privacy modules in the undergraduate computer science curriculum.
- Supported participation of 3 female students in REU.
- Supported outreach in a local elementary school.

CNS-1916902: Wenjing Lou and Tom Hou (Virginia Tech), https://www.cnsr.ictas.vt.edu/projects_nsf_1916926.html

CNS-1916926: Ning Zhang (Washington University in St Louis), https://cybersecurity.seas.wustl.edu/projects/PrivacyGuard.html