Toward Enforceable Data Usage Control in Cloud-based IoT Systems

Wenjing Lou (PI), Thomas Hou (Co-PI), Virginia Tech
Ning Zhang (PI), Washington University in St. Louis



Award #:
CNS-1916902 https://www.cnsr.ictas.vt.edu/projects_nsf_1916926.html
CNS-1916926 https://cybersecurity.seas.wustl.edu/projects/PrivacyGuard.html

Data Usage Control – An Urgent Privacy Call

- **Contextual nature of privacy:** We share personal data for intended purpose or usage scenario.
- **Encryption is not enough:** Private data needs to be used by a **data consumer (DC)**.
- **Access control is not enough:** When **data owner (DO)** shares private data to another party, they lose control on how the data will be **used**. *e.g. the Facebook-Cambridge Analytica data scandal*.
- **Data Usage Control as a Privacy Goal:** DO gets to define "*who can use my data for which purpose at what condition, price*" and has a mechanism to enforce such usage policy —enabling a secure and trustworthy data sharing economy.

Key Objectives and Challenges

- **Data Usage Policy:** Giving DO fine-grained control over the access and usage of their private data.
- **Trusted Enforcement:** Guaranteeing correctness (by DO's policy) and auditability of data usage by DCs.
- **Confidentiality:** Untrusted DCs or platforms (cloud) cannot learn DO's plaintext data.
- **Security of data sharing economy:** Fair and atomic transaction (pay for usage) between DO and DC.

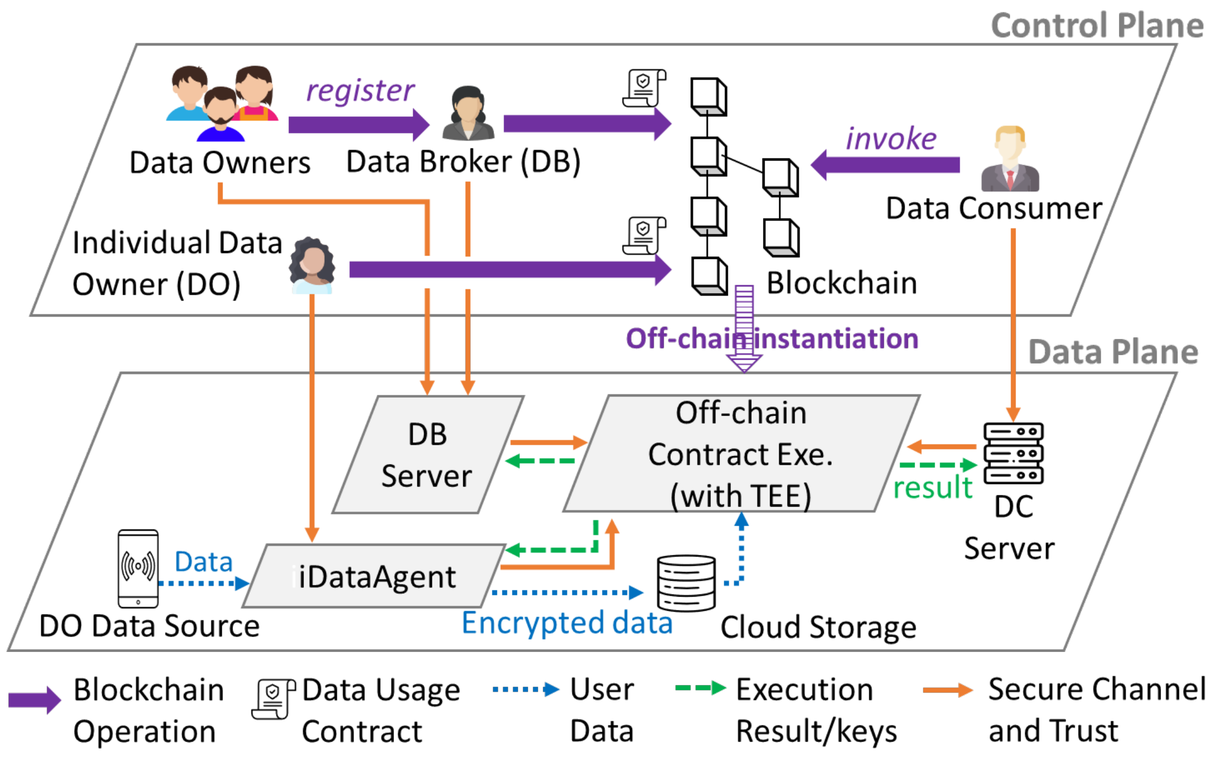
Scientific Impact

- ❖ 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.

Our Solution – PrivacyGuard

Key Methodology:

- ❑ **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.



Results: (1) DO gets paid for DC's computation on their private data; (2) DC obtains the result; (3) DO's plaintext data is never exposed; (4) Data usage is recorded and auditable by all parties.

Publication

Y. Xiao, N. Zhang, J. Li, W. Lou, Y. T. Hou, "**PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Off-chain Contract Execution**," in *European Symposium on Research in Computer Security (ESORICS)* 2020.

Source code: https://github.com/yang-sec/PrivacyGuard

Additional publications at IEEE INFOCOM 2020, IEEE Communications Surveys & Tutorials 2020, IEEE Wireless Communications 2021, and USENIX Security 2021, ACM CCS 2021, ACM WiSec 21, AAAI 2020, NDSS 2020

Broader Impact and 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.