Droplet: Decentralized Authorization and Access Control for Encrypted Data Streams

Hossein Shafagh, Lukas Burkhalter, Sylvia Ratnasamy, Anwar Hithnawi

ETH zürich

Berkeley
UNIVERSITY OF CALIFORNIA

Rise of Real-Time Data

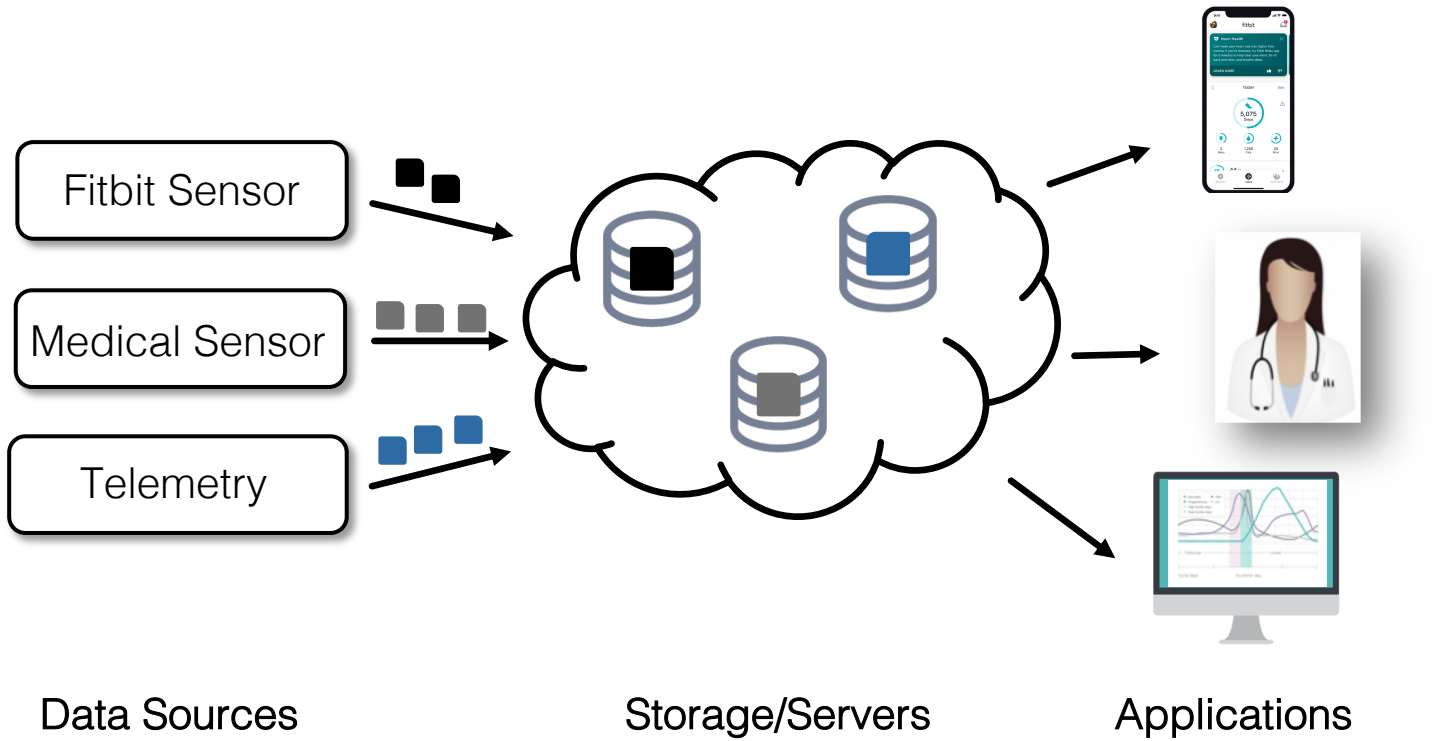
Autonomous Driving

Internet of Things

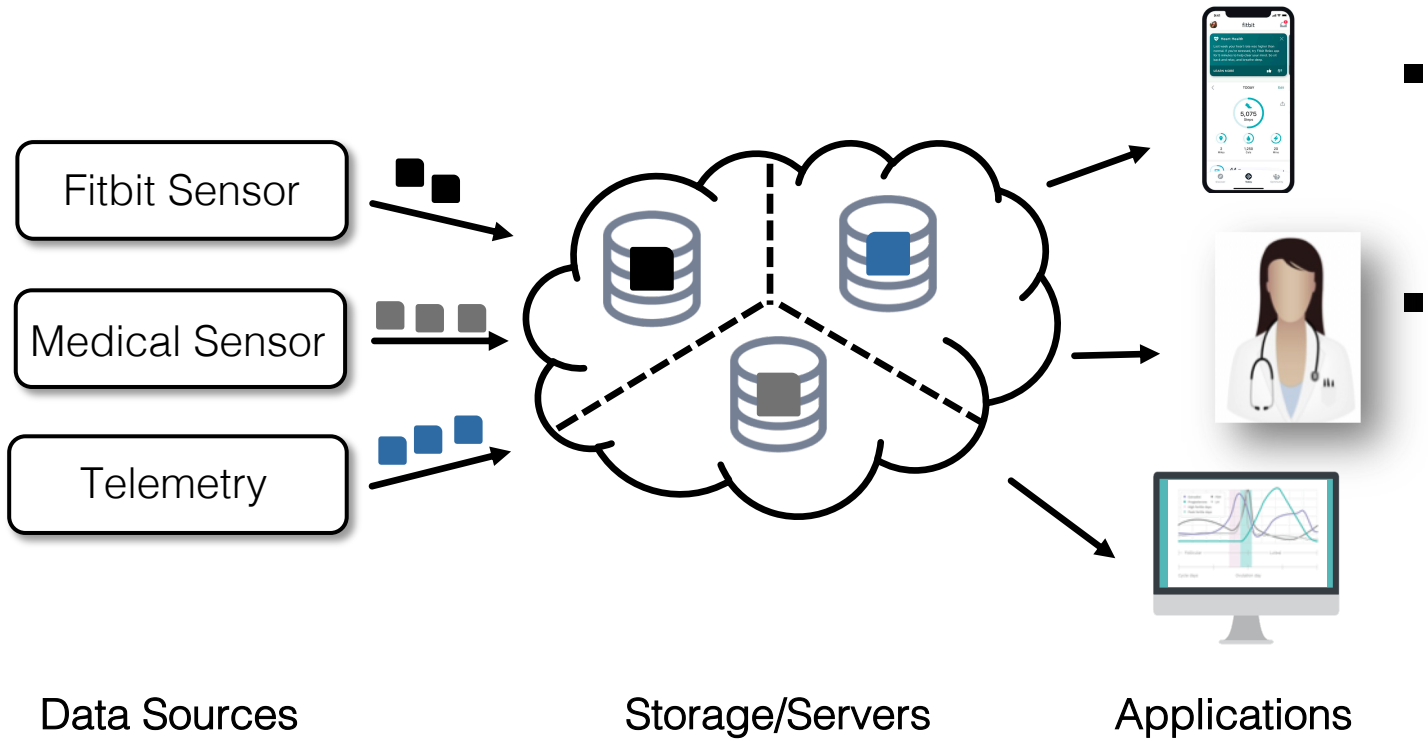
Health Care

Telemetry/DevOps

Monolithic Applications

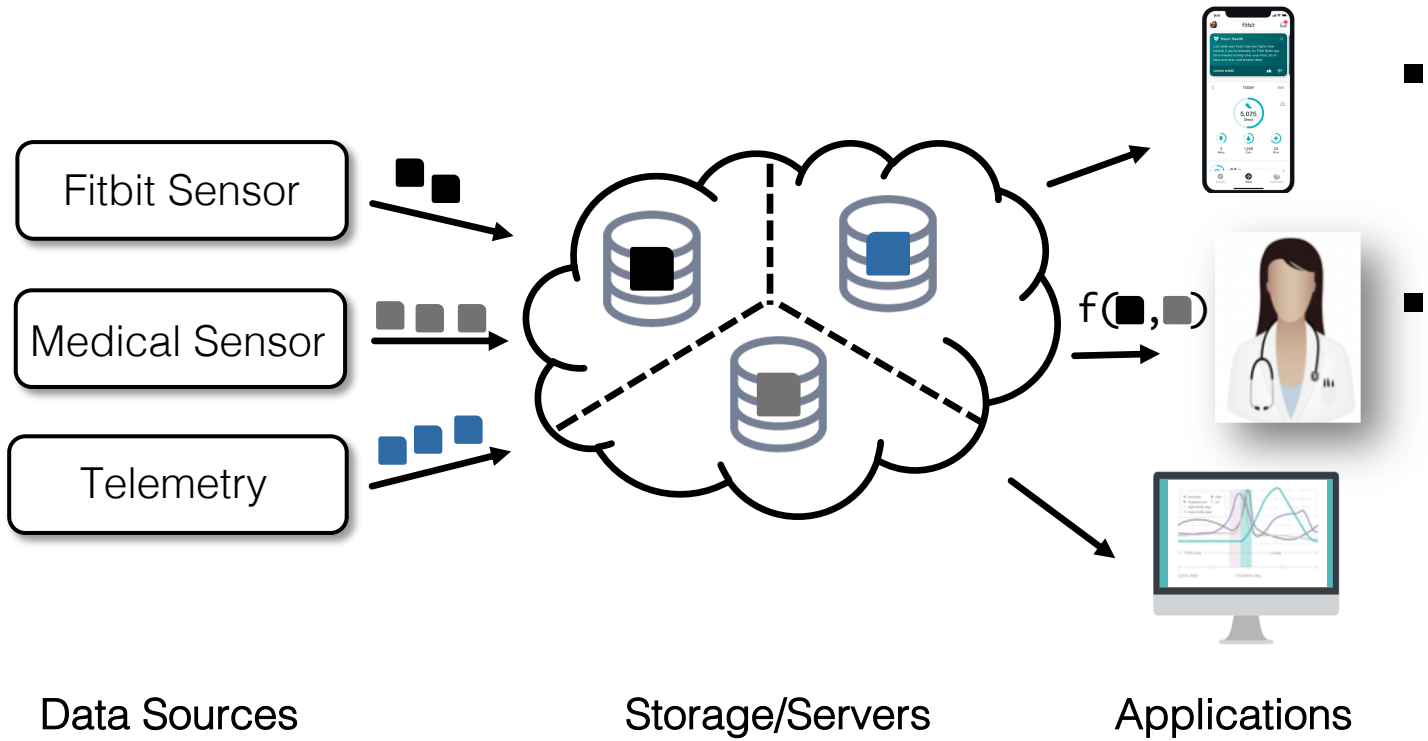


Monolithic Applications



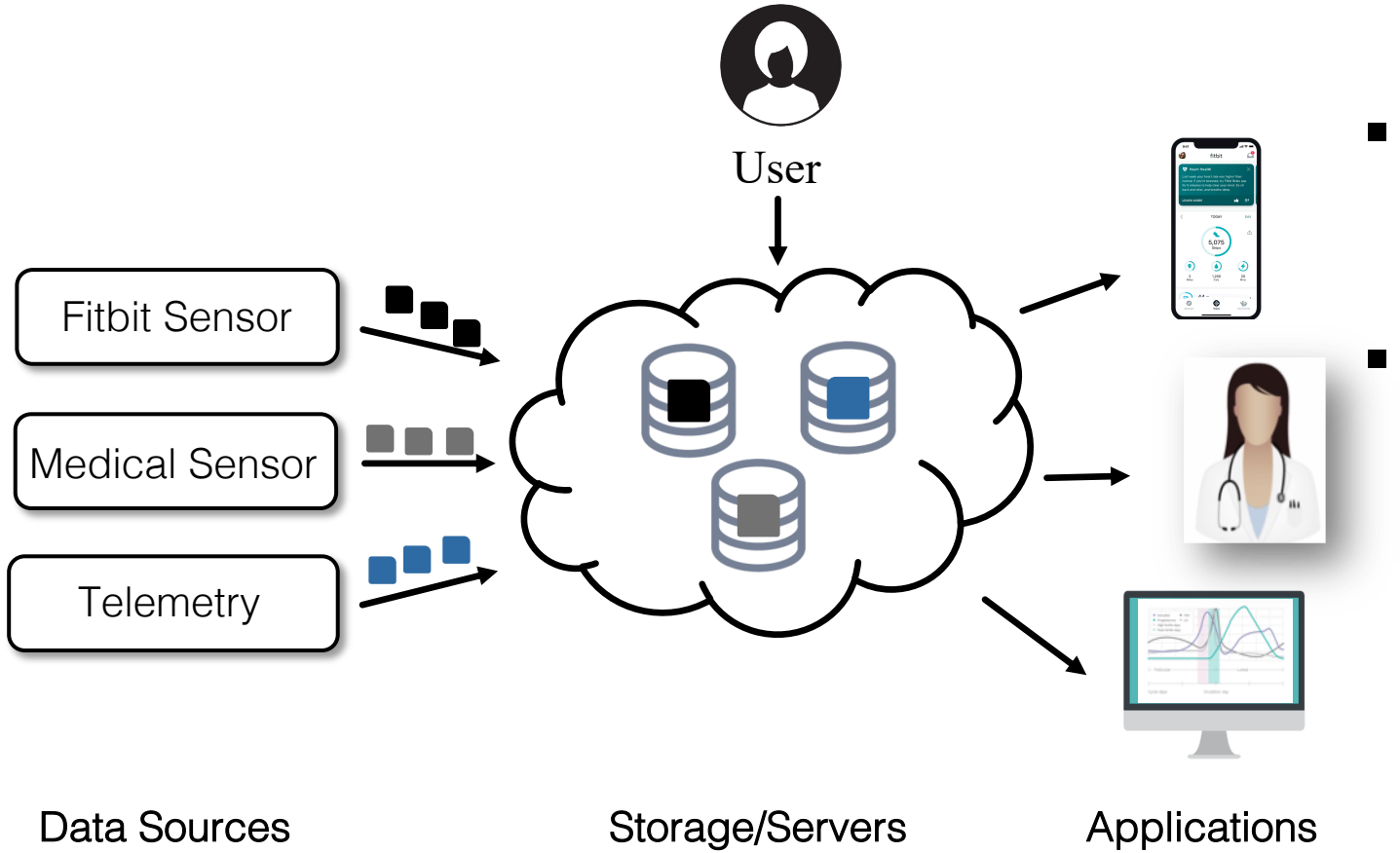
- data is governed and controlled by application providers
- data lives in narrow and disjoint silos → hindering fusing data from multiple sources

Monolithic Applications



- data is governed and controlled by application providers
- data lives in narrow and disjoint silos → hindering fusing data from multiple sources

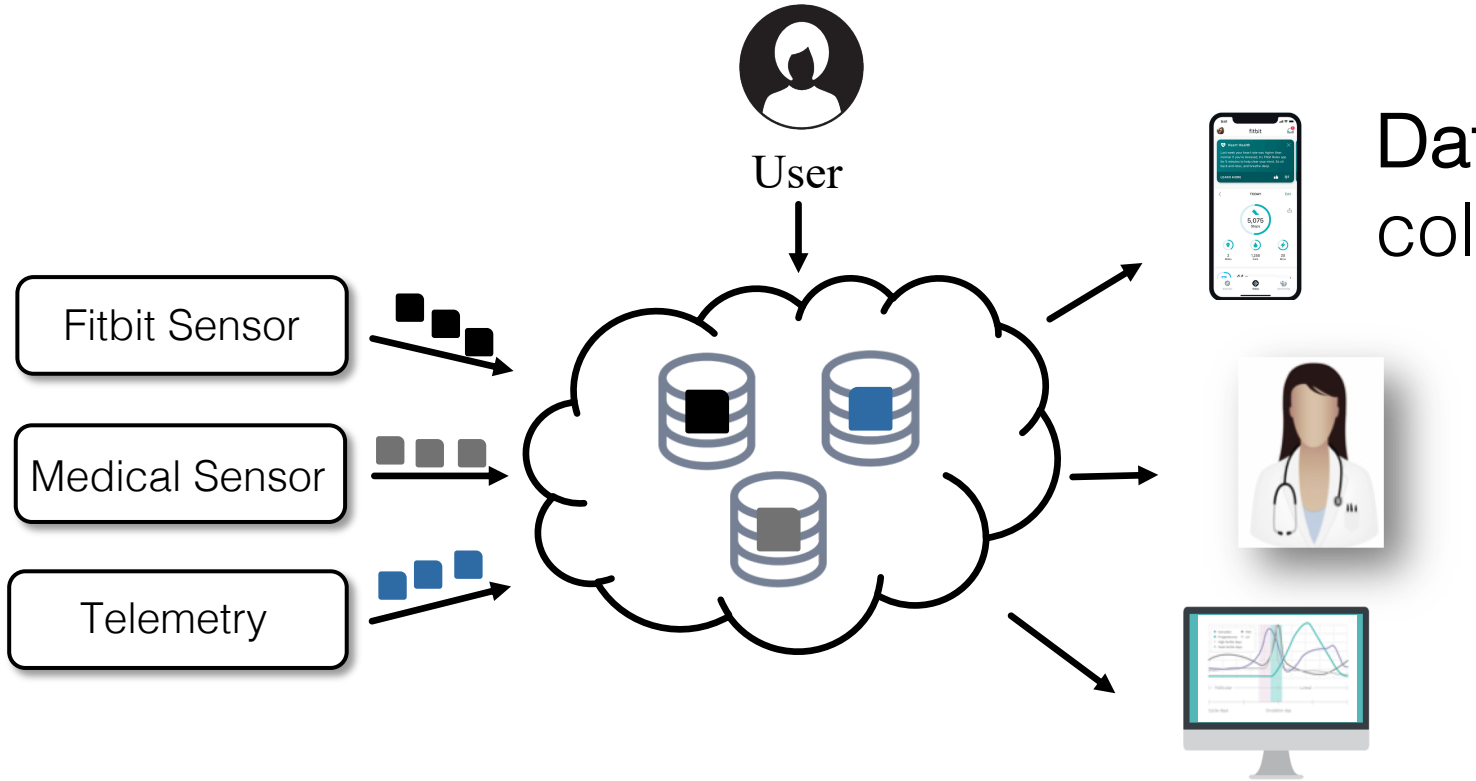
User-centric Model



- decouple user-data from application's logic
- users in full control of their data

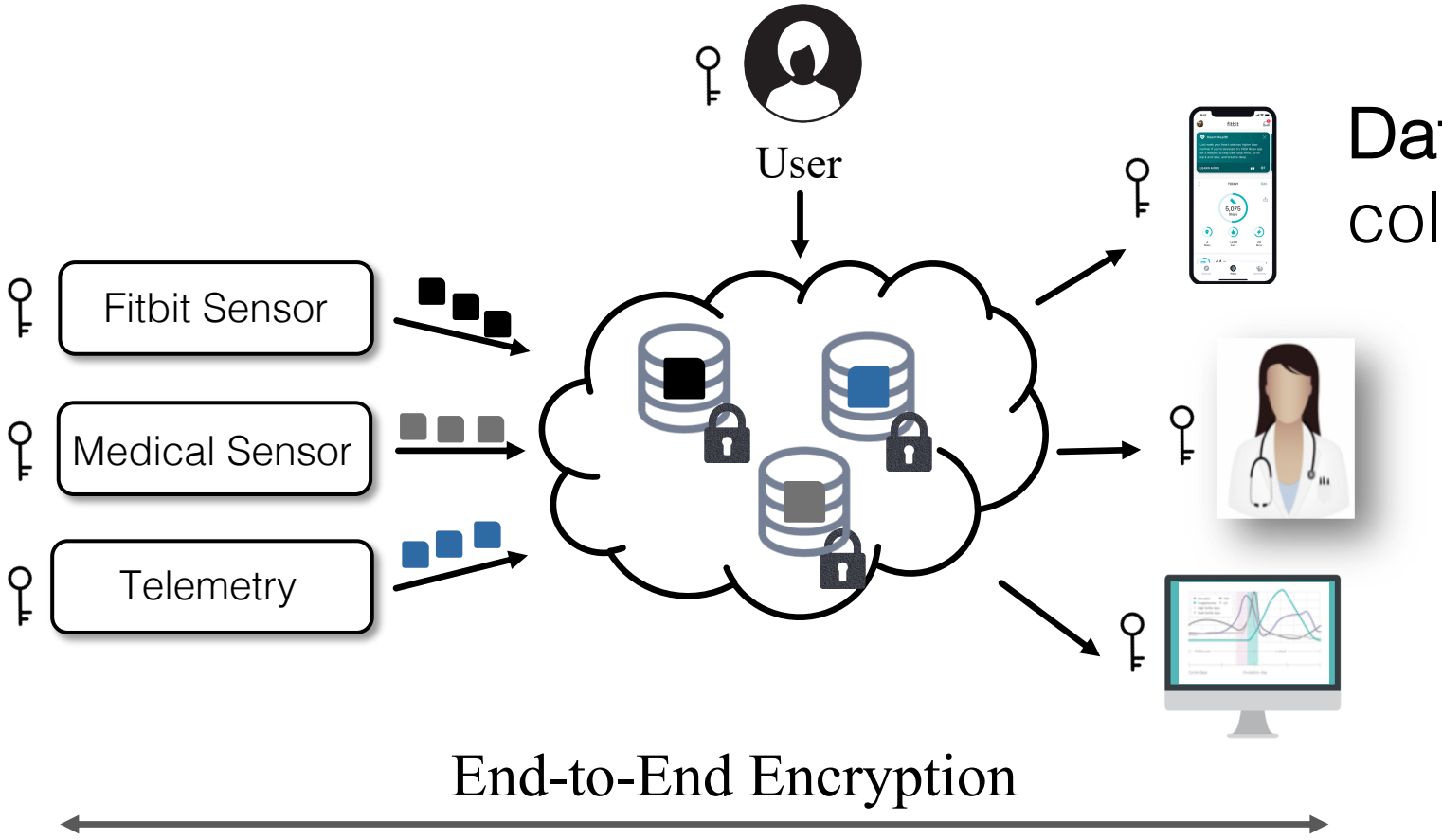
How to realize **secure** and **decentralized** access control in a user-centric architecture?

Privacy-sensitive Data



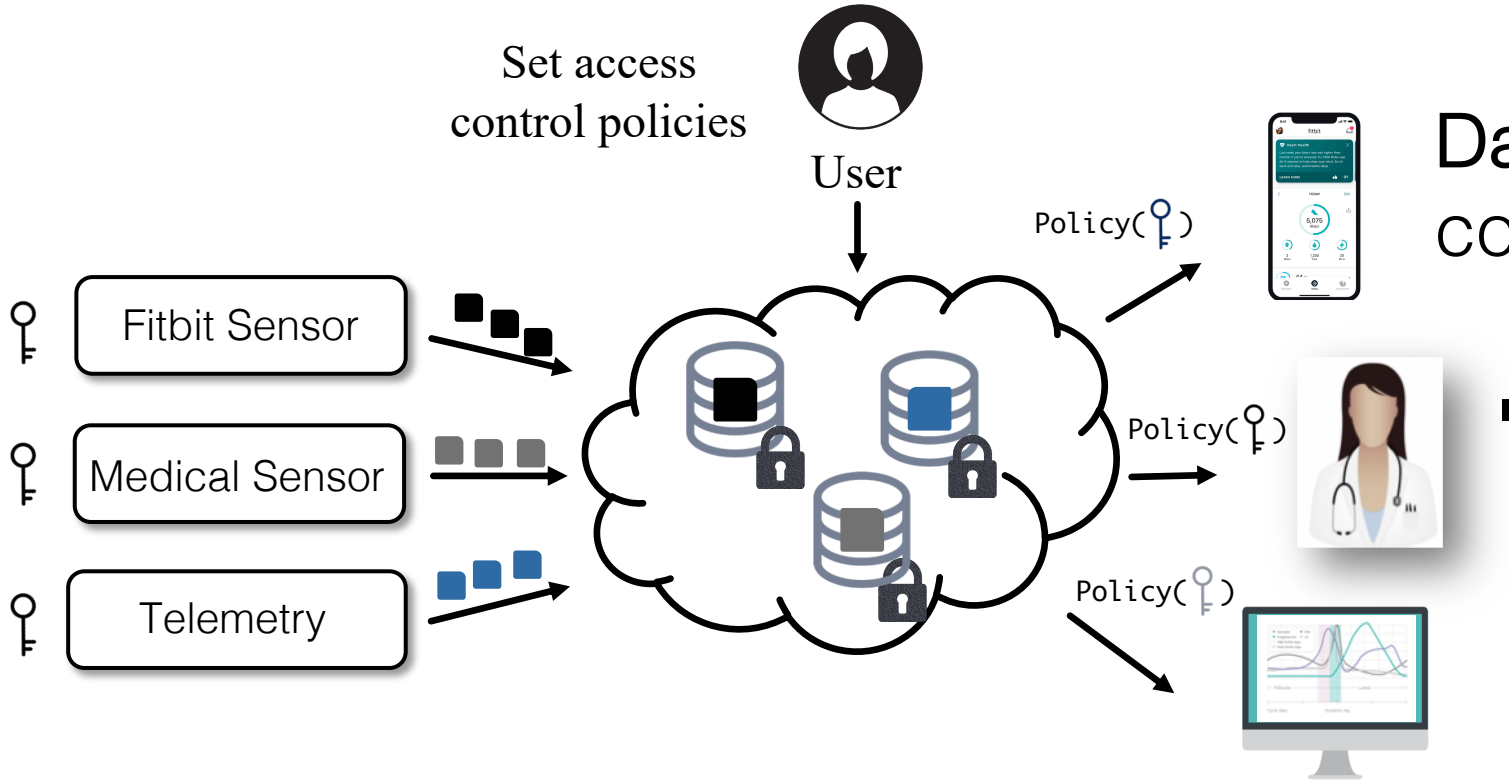
Data protection: IoT devices collect privacy-sensitive data

Privacy-sensitive Data: End-to-End Encryption



Data protection: IoT devices collect privacy-sensitive data

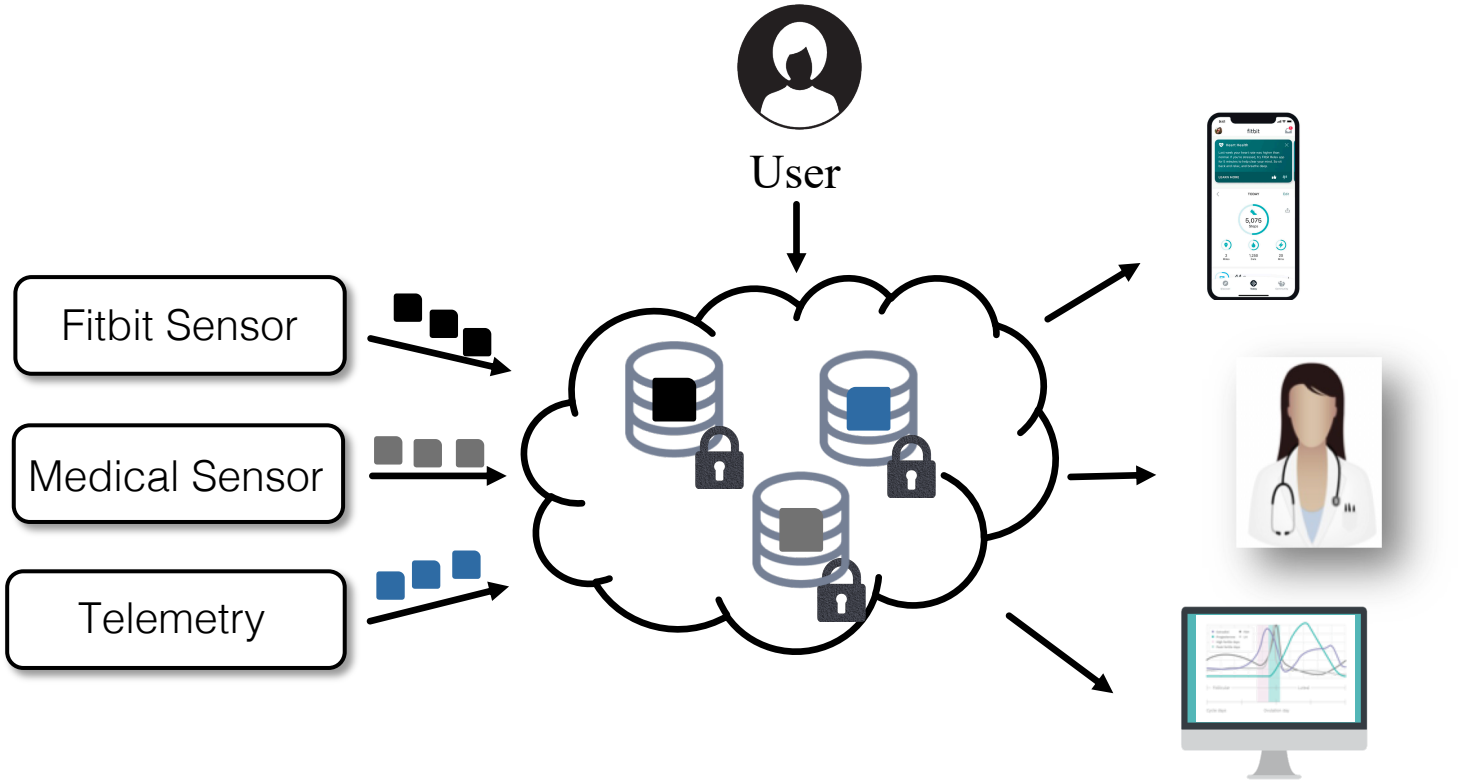
Privacy-sensitive Data: End-to-End Encryption



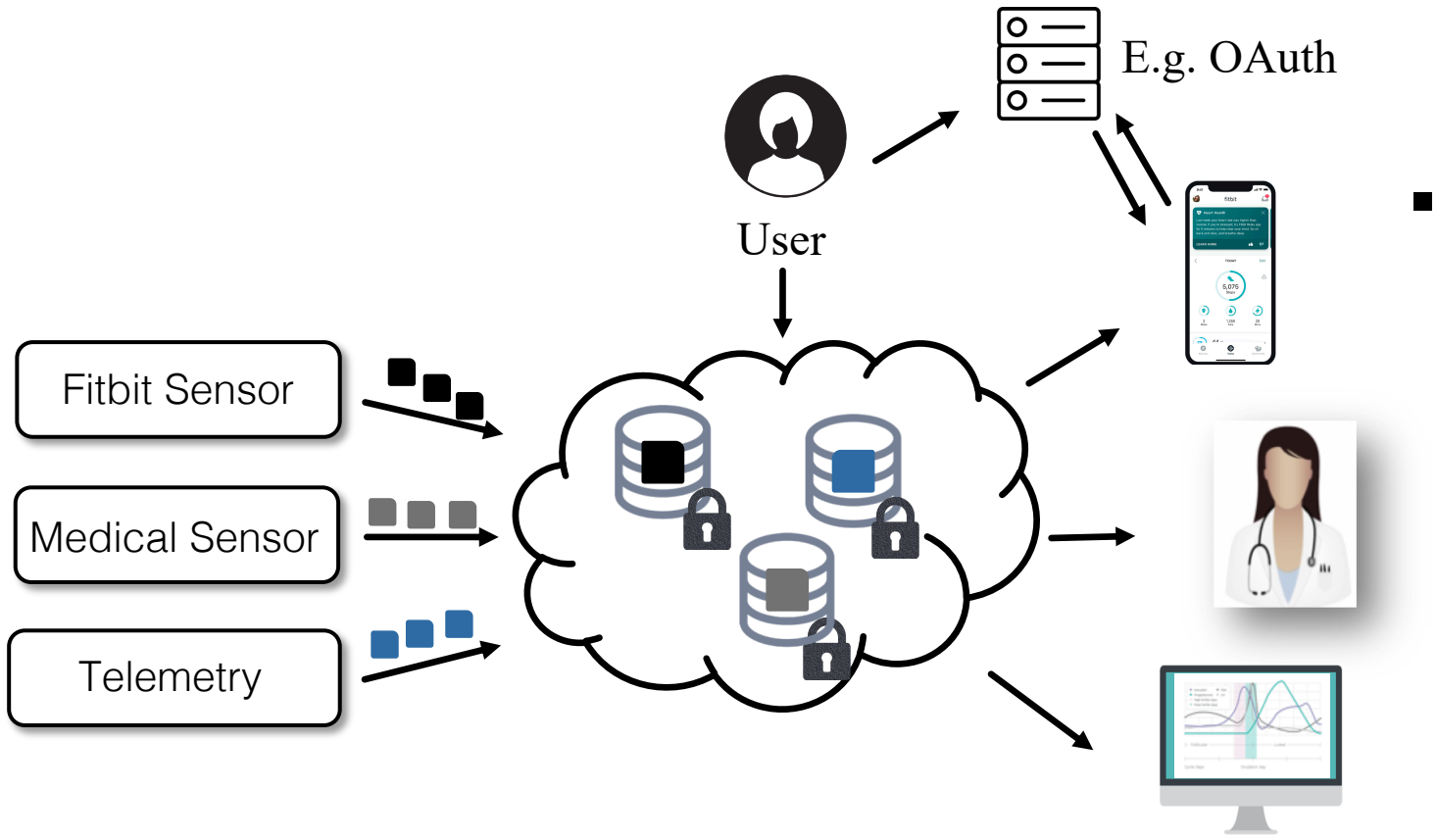
Data protection: IoT devices collect privacy-sensitive data

- **Challenge 1 :** fine grained data protection that is consistent with stream sharing semantics

Access Authorization

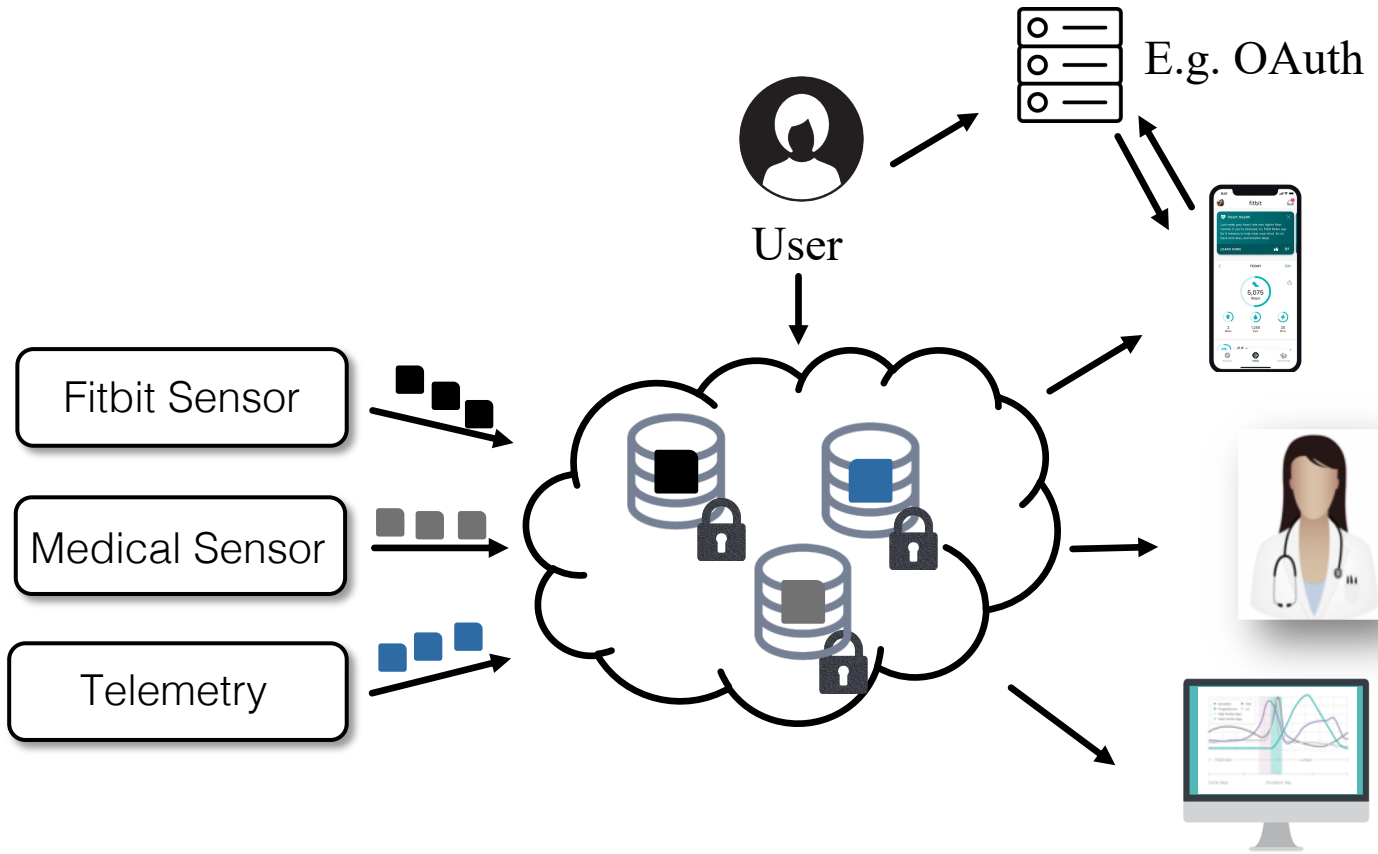


Access Authorization



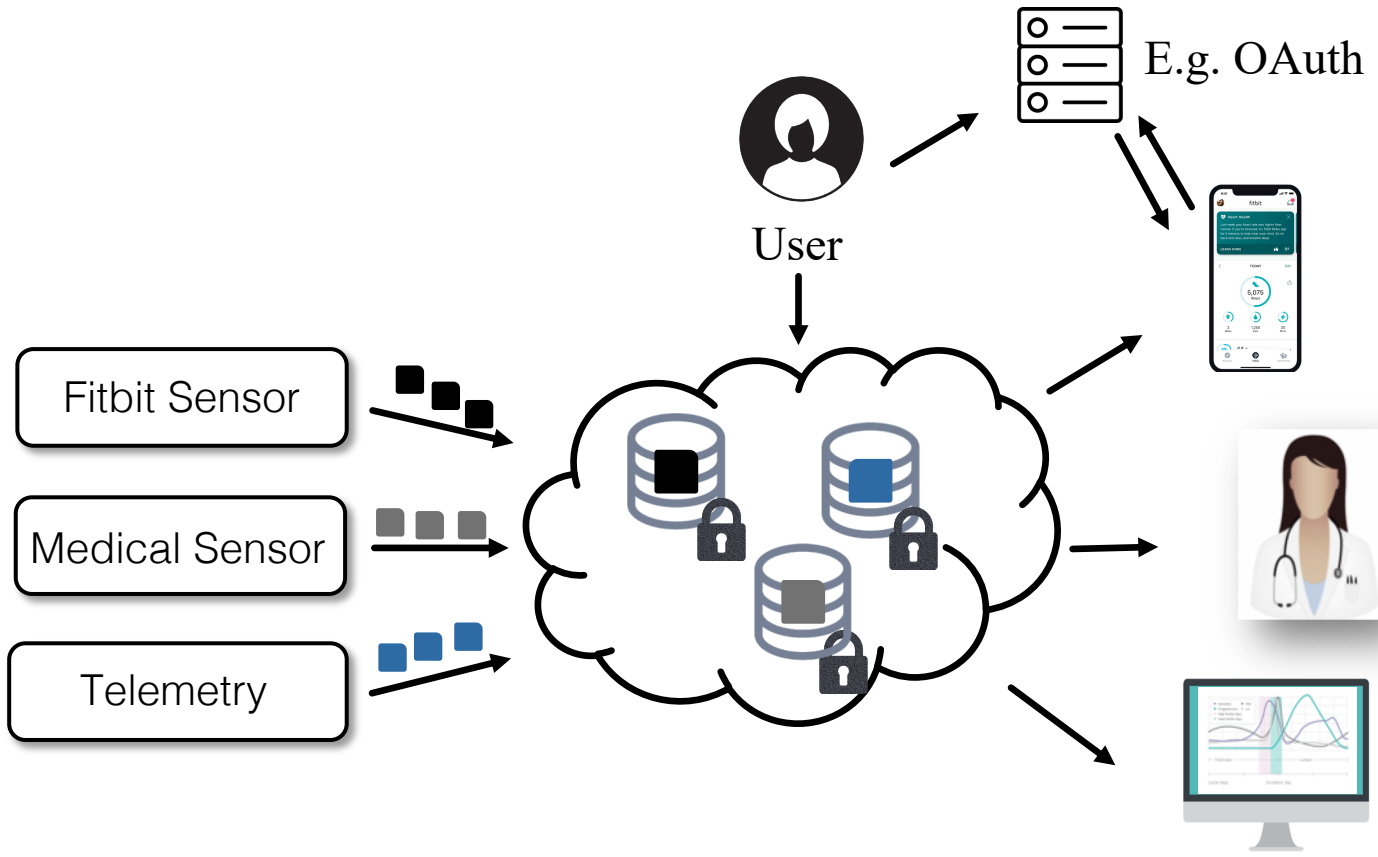
- authorization tokens are issued by trusted intermediary (invoked per request)

Access Authorization



- authorization tokens are issued by trusted intermediary (invoked per request)
- no cryptographic guarantees / decoupled from data protection

Access Authorization



- authorization tokens are issued by trusted intermediary (invoked per request)
- no cryptographic guarantees / decoupled from data protection
- **Challenge ❷: d**ecentralized authorization that adheres to end-to-end encryption

Droplet in a Nutshell

a new decentralized data access control service

Droplet in a Nutshell

a new decentralized data access control service

- co-design: access control & authorization for end-to-end encryption

Droplet in a Nutshell

a new decentralized data access control service

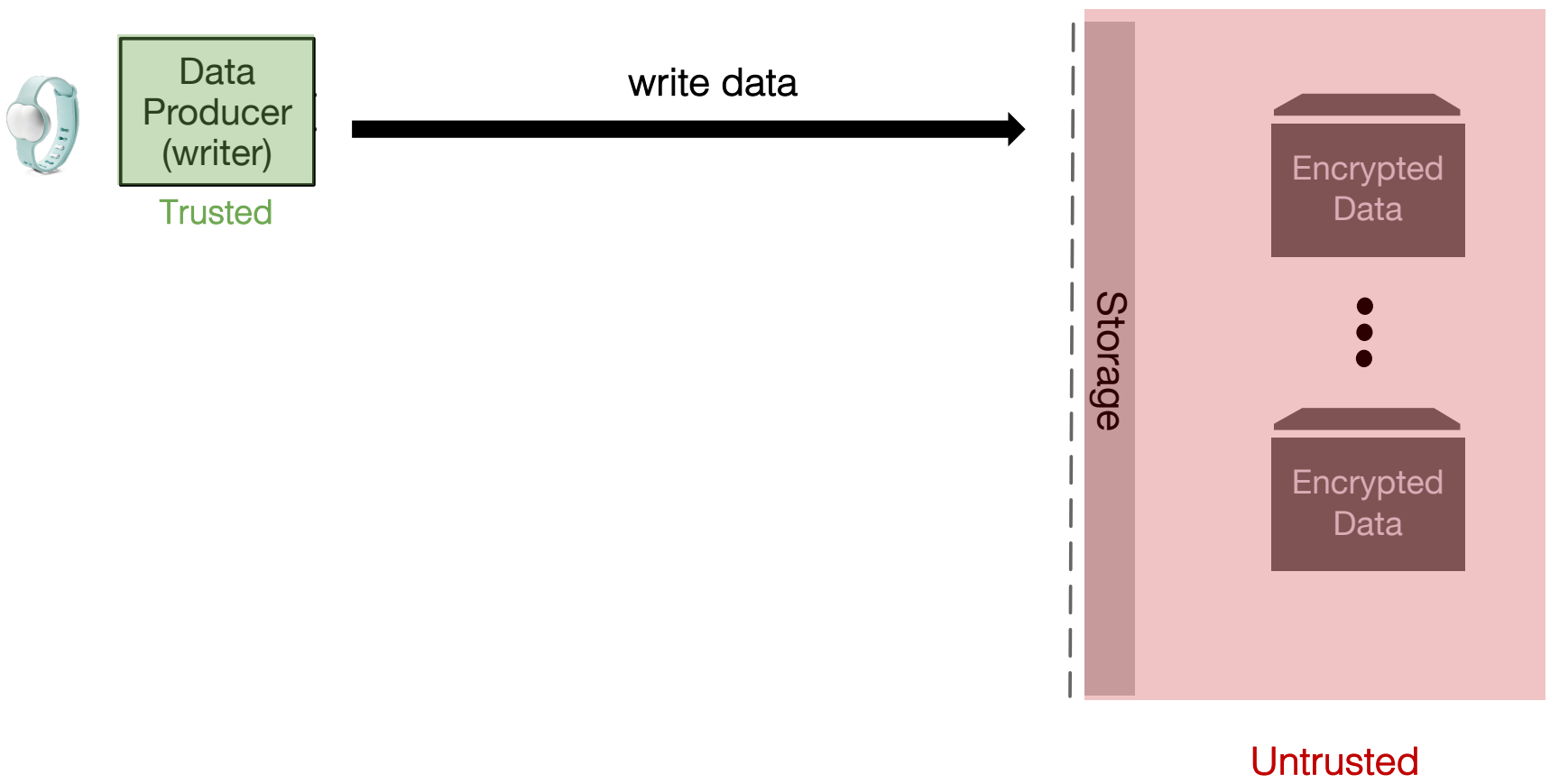
- co-design: access control & authorization for end-to-end encryption
- a new cryptographic access control construction tailored for stream data

Droplet in a Nutshell

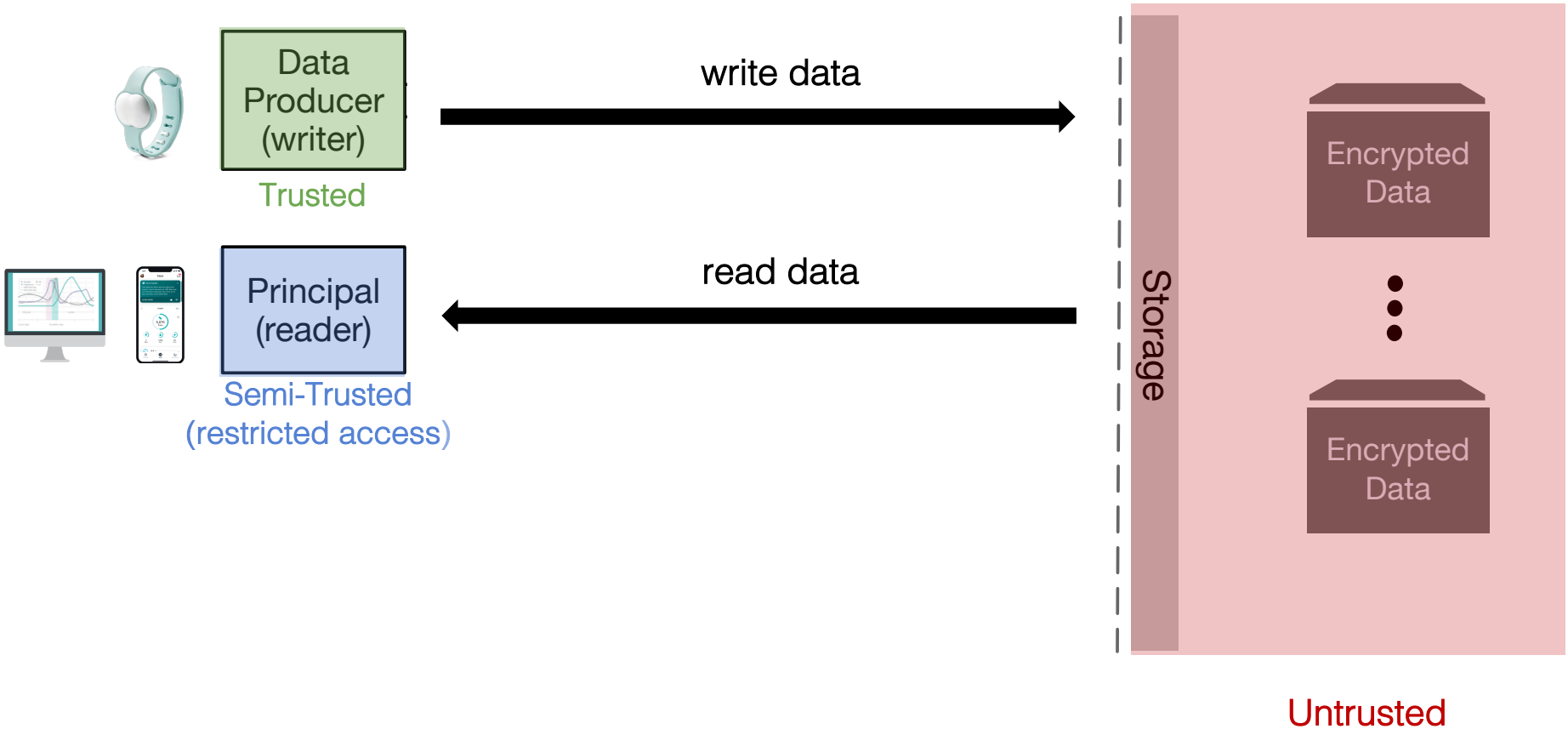
a new decentralized data access control service

- co-design: access control & authorization for end-to-end encryption
- a new cryptographic access control construction tailored for stream data
- a new decentralization authorization service
  - operates without central authority
  - protects the privacy/integrity of access permissions
  - permission discovery

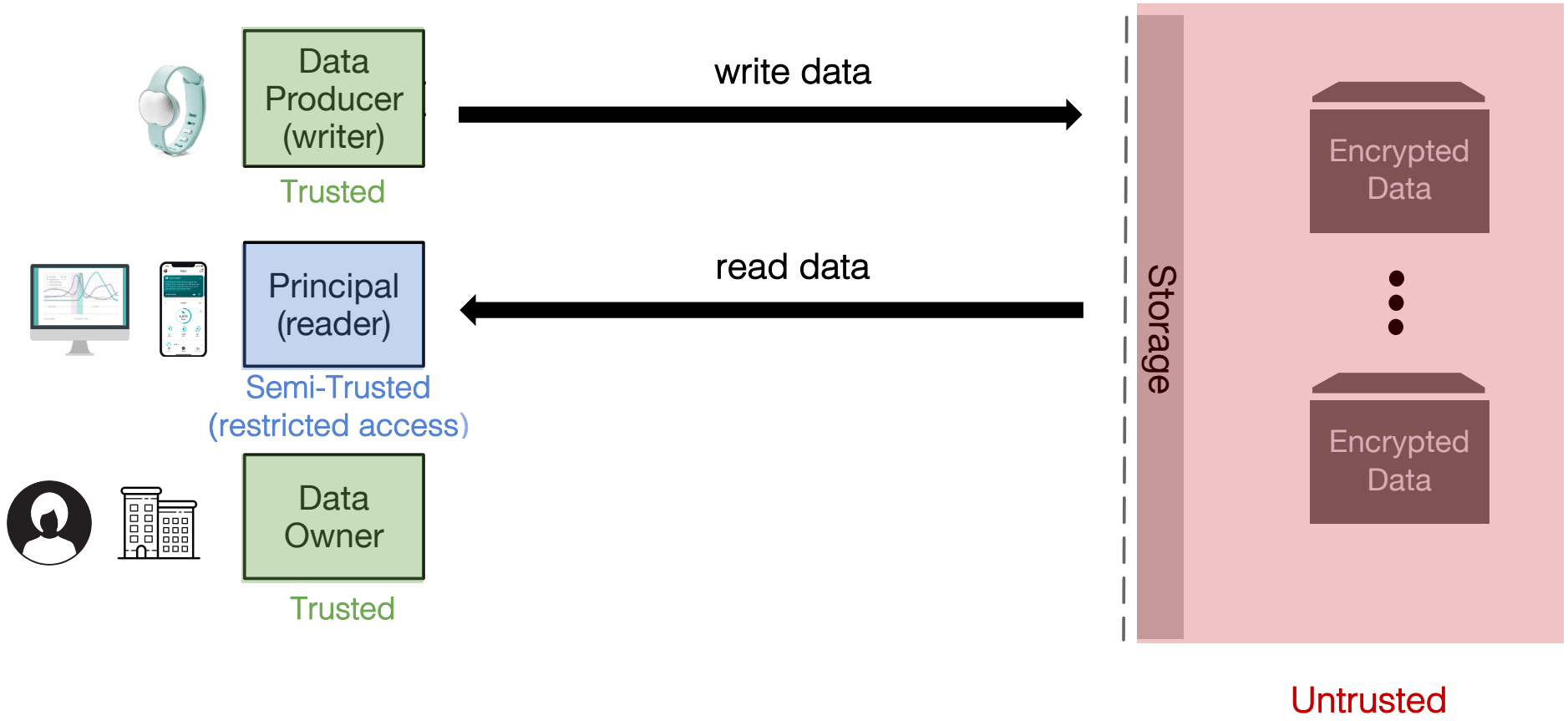
Overview and Threat Model



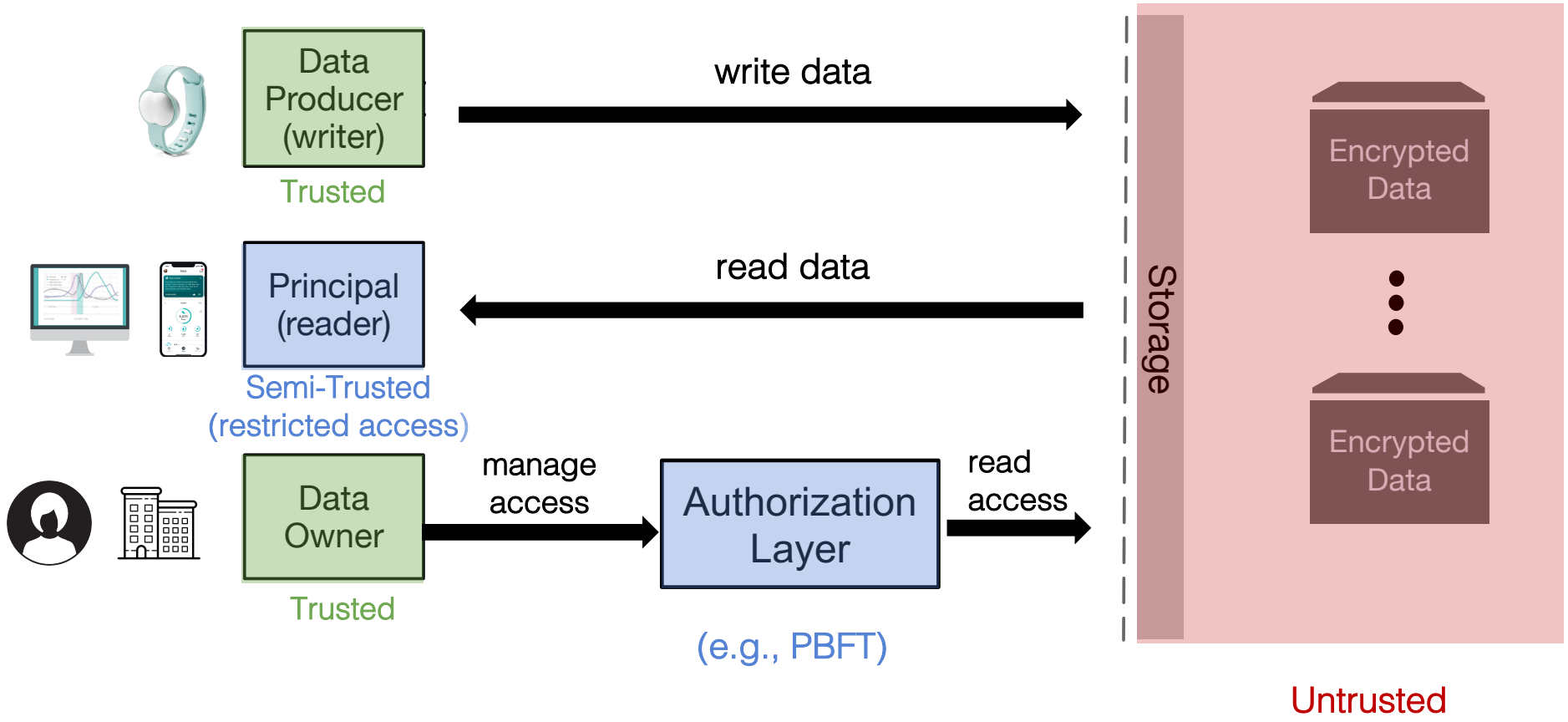
Overview and Threat Model



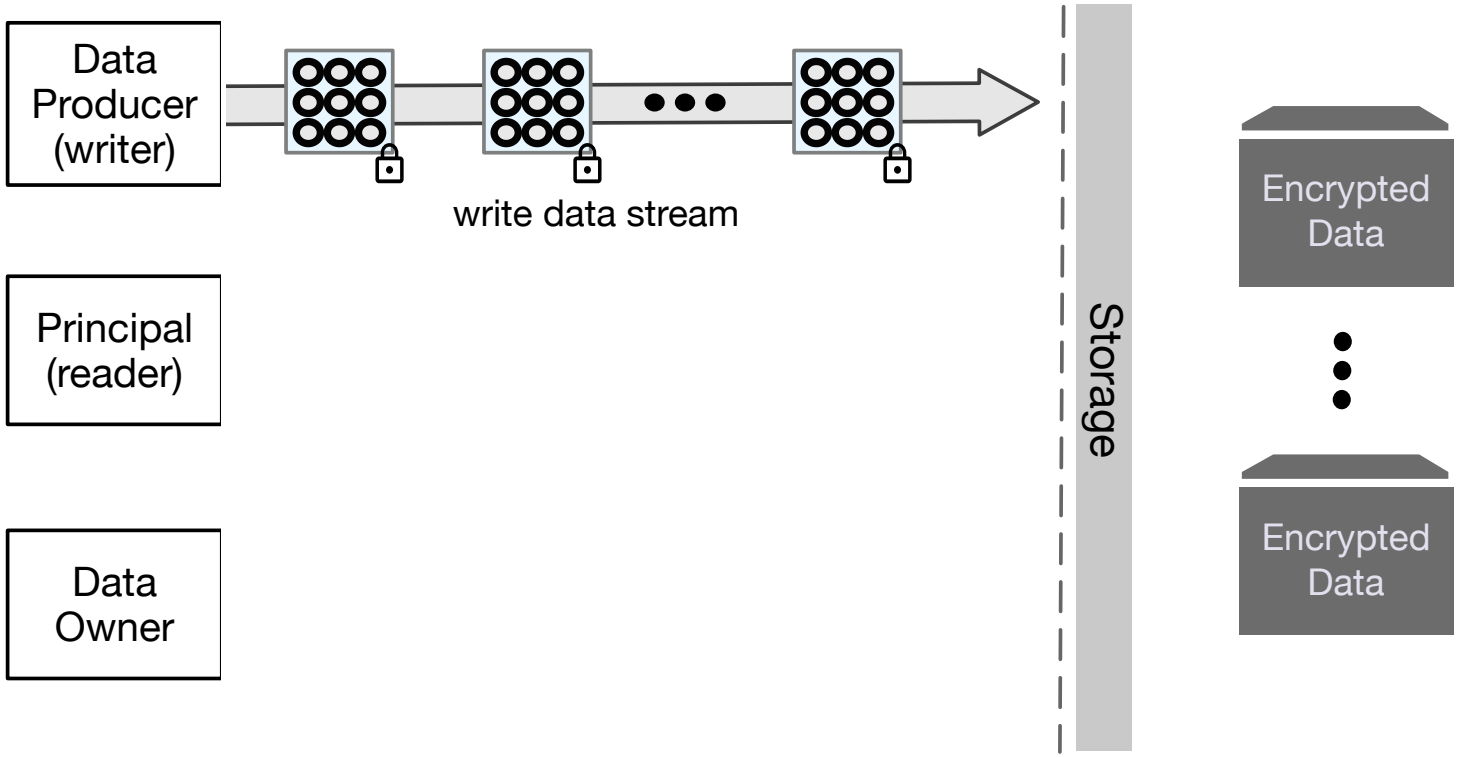
Overview and Threat Model



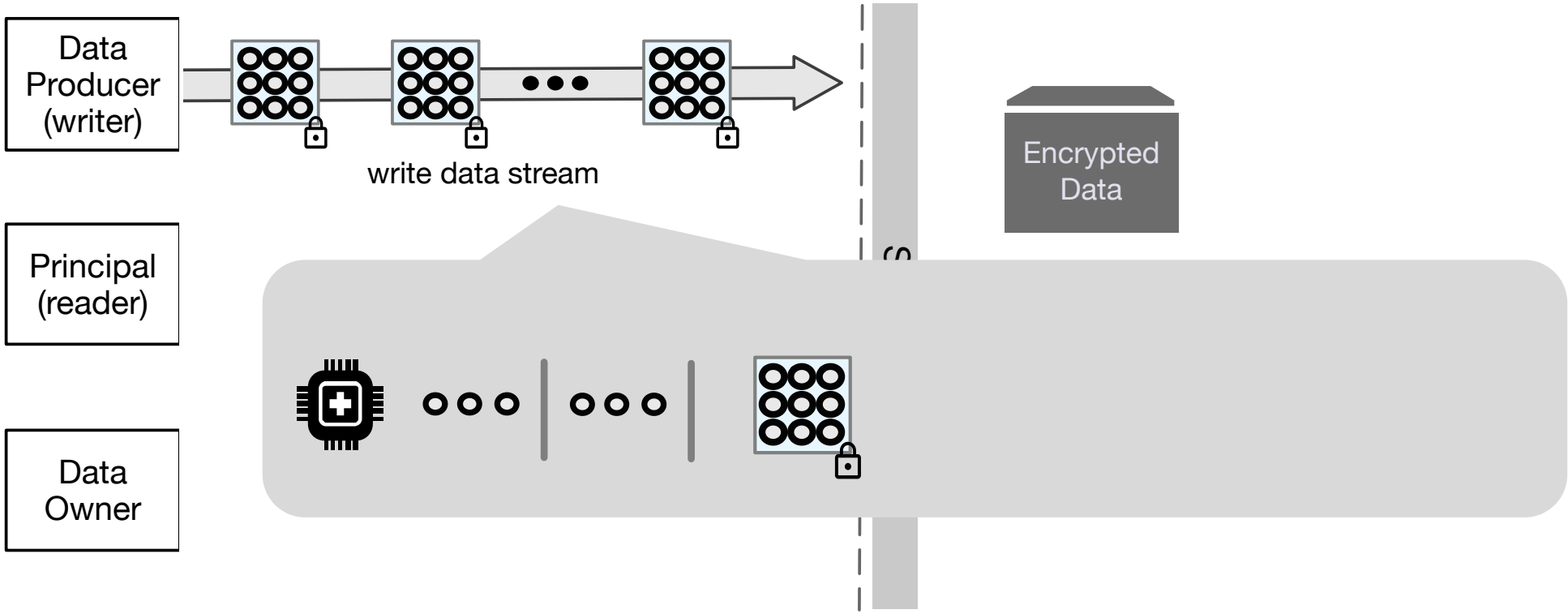
Overview and Threat Model



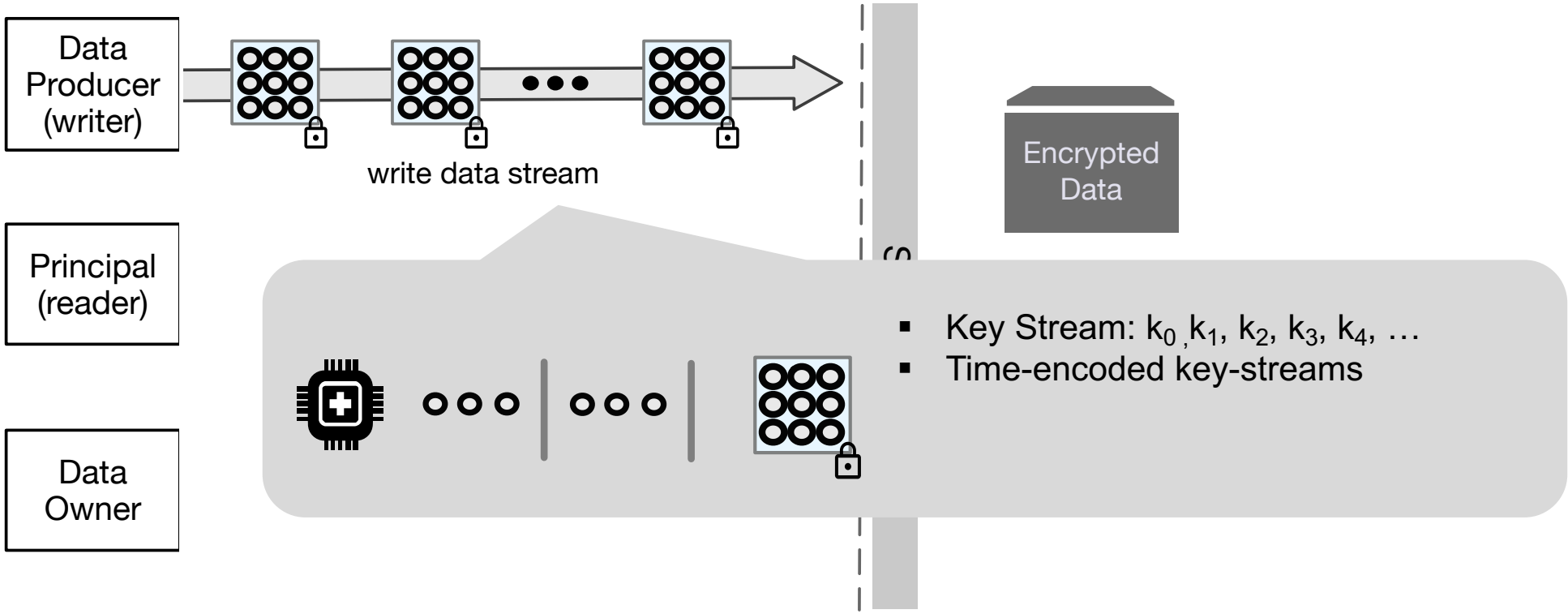
Droplet: Encryption-based Access Control



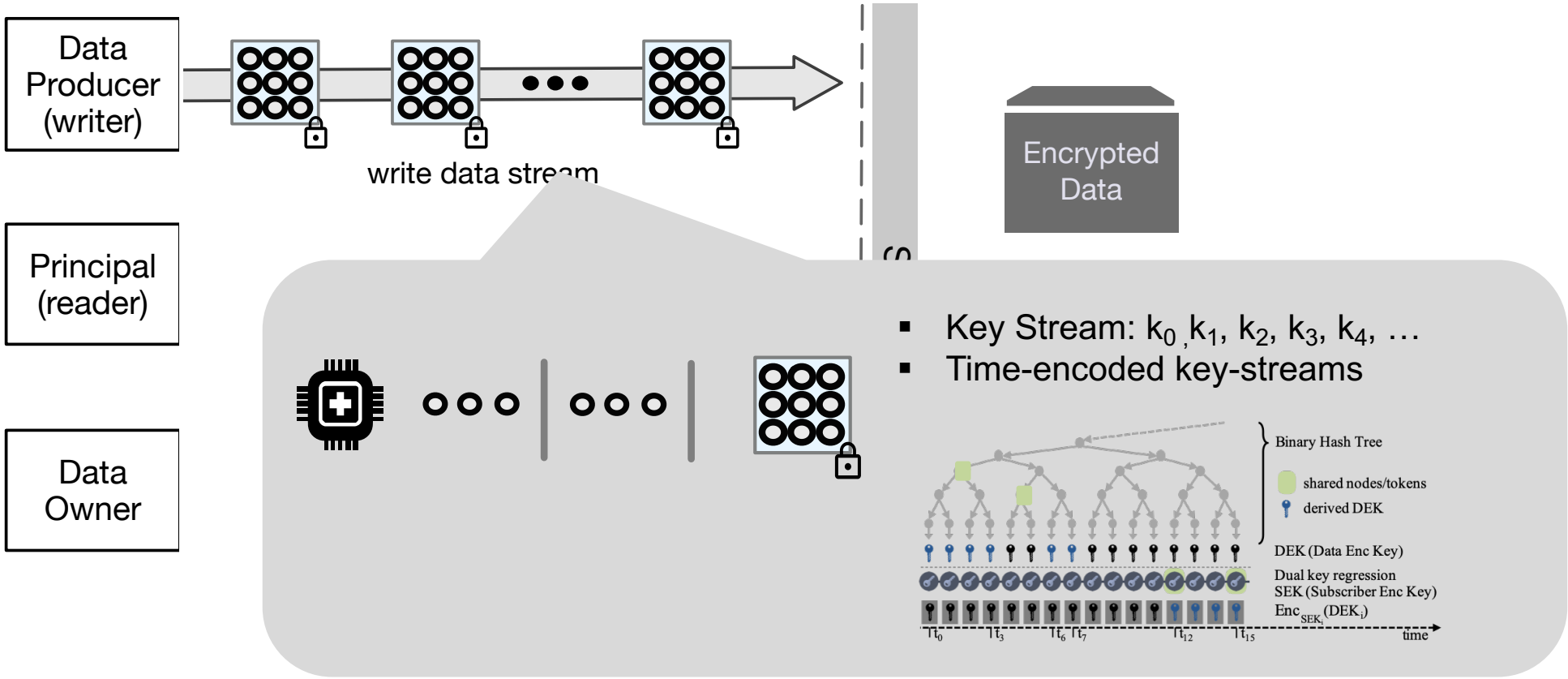
Droplet: Encryption-based Access Control



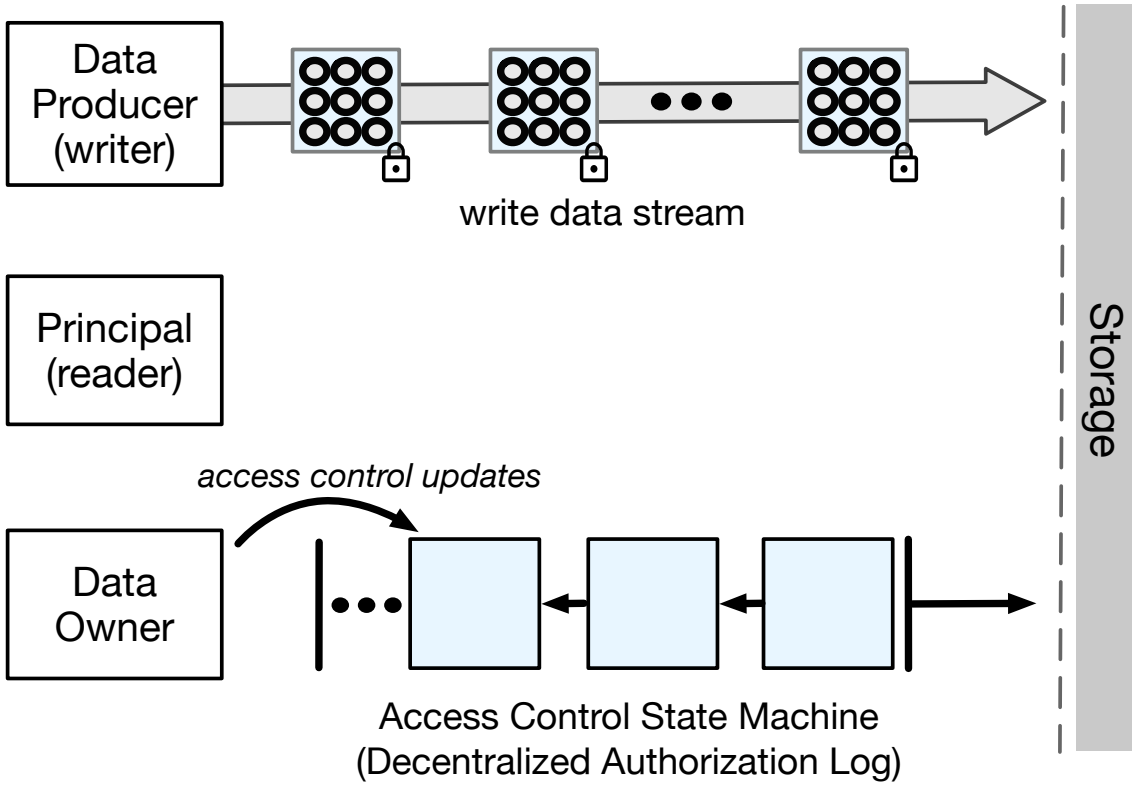
Droplet: Encryption-based Access Control

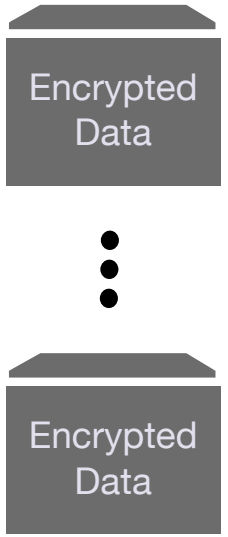


Droplet: Encryption-based Access Control

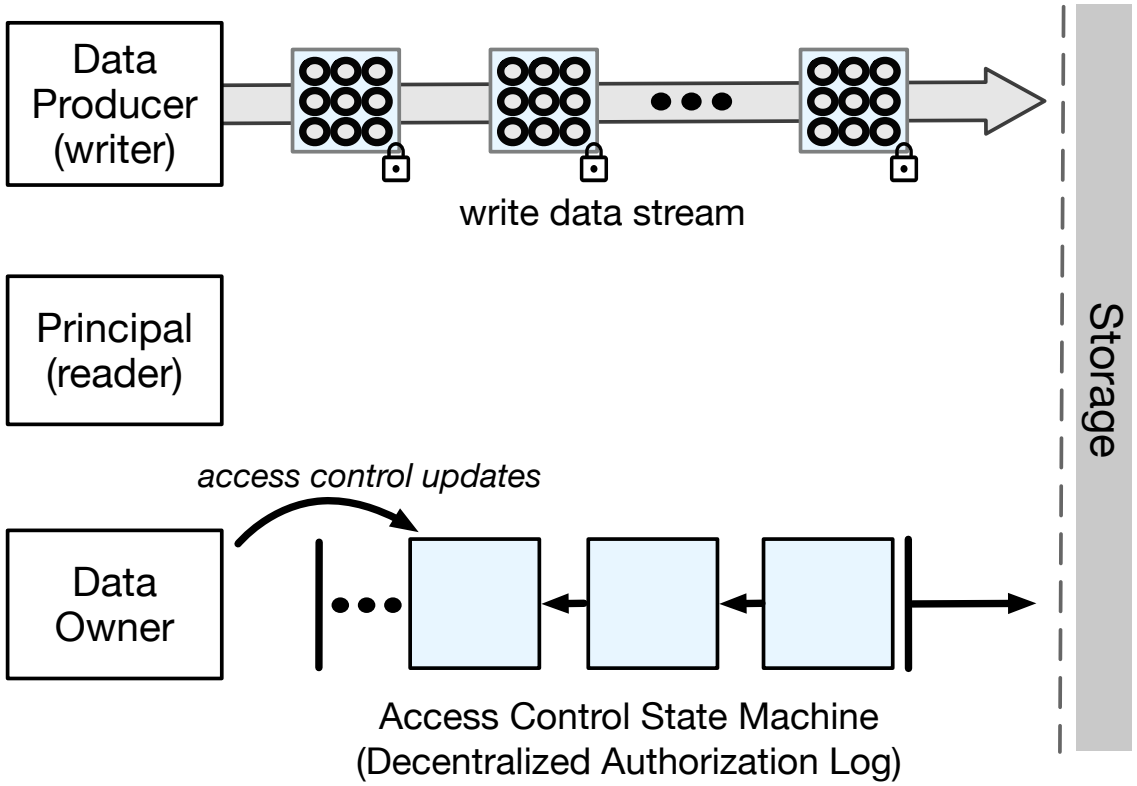


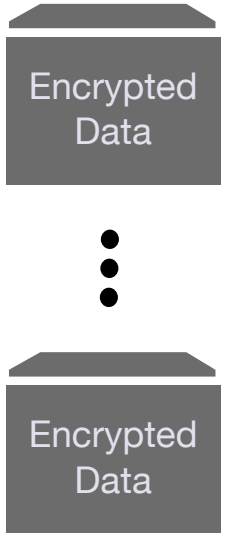
Droplet Authorization



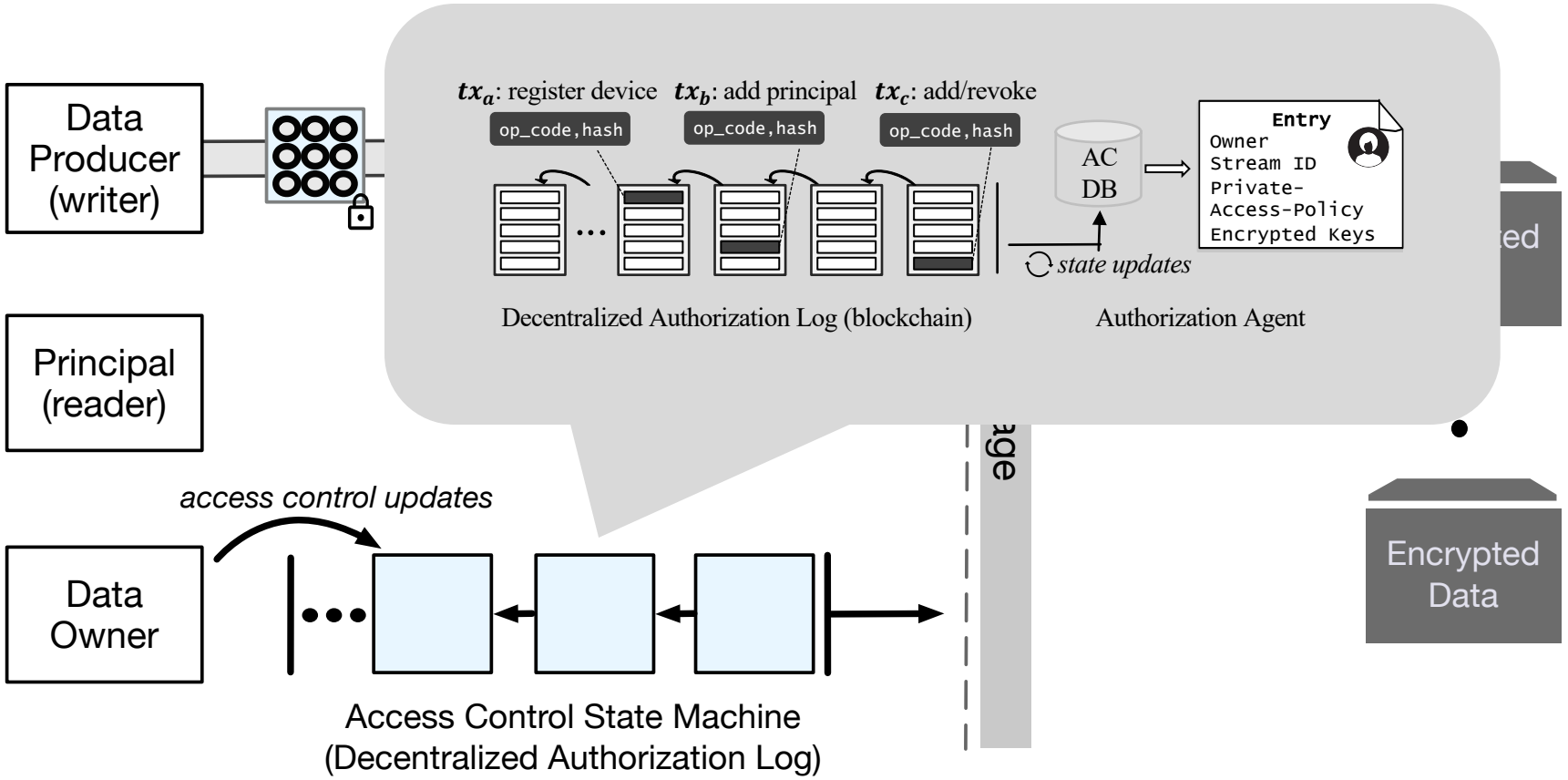


Droplet Authorization

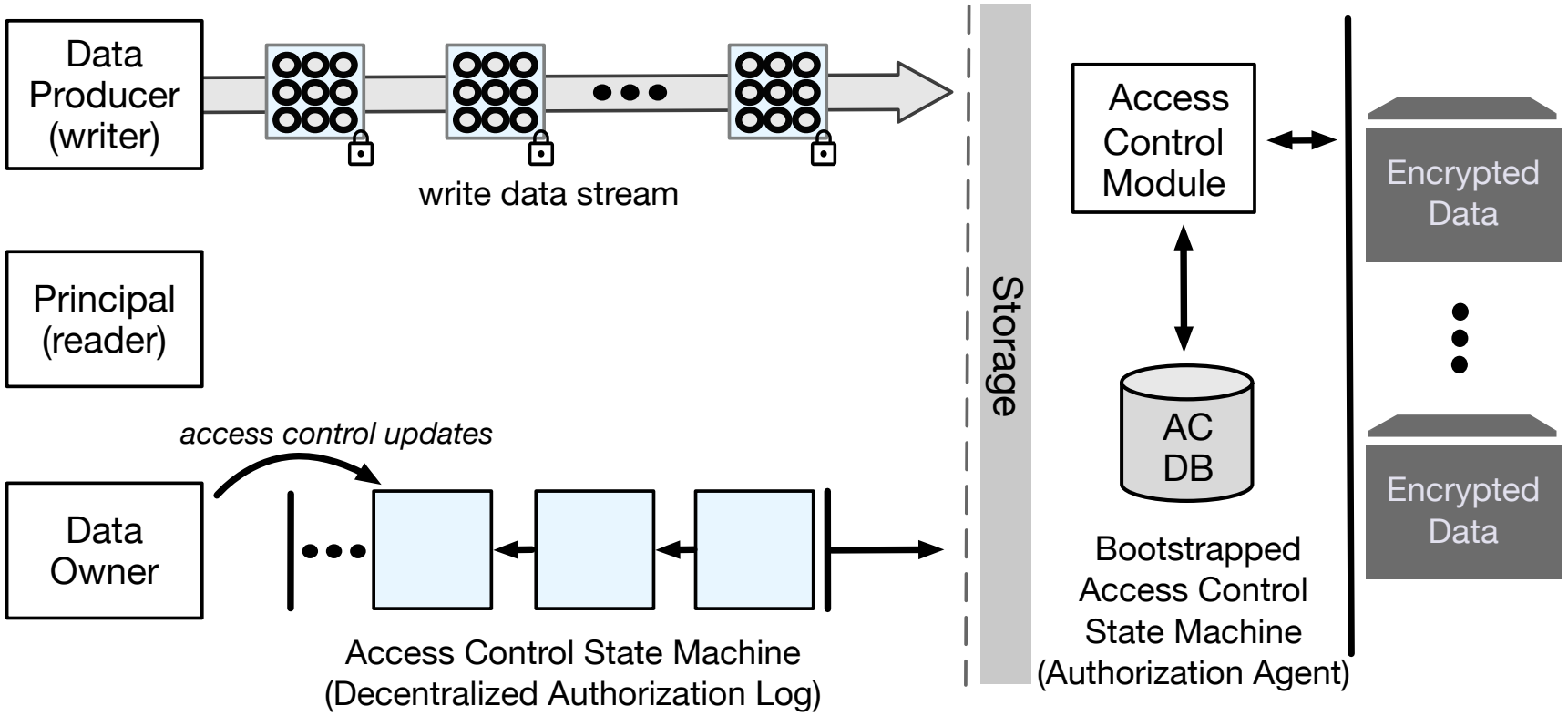




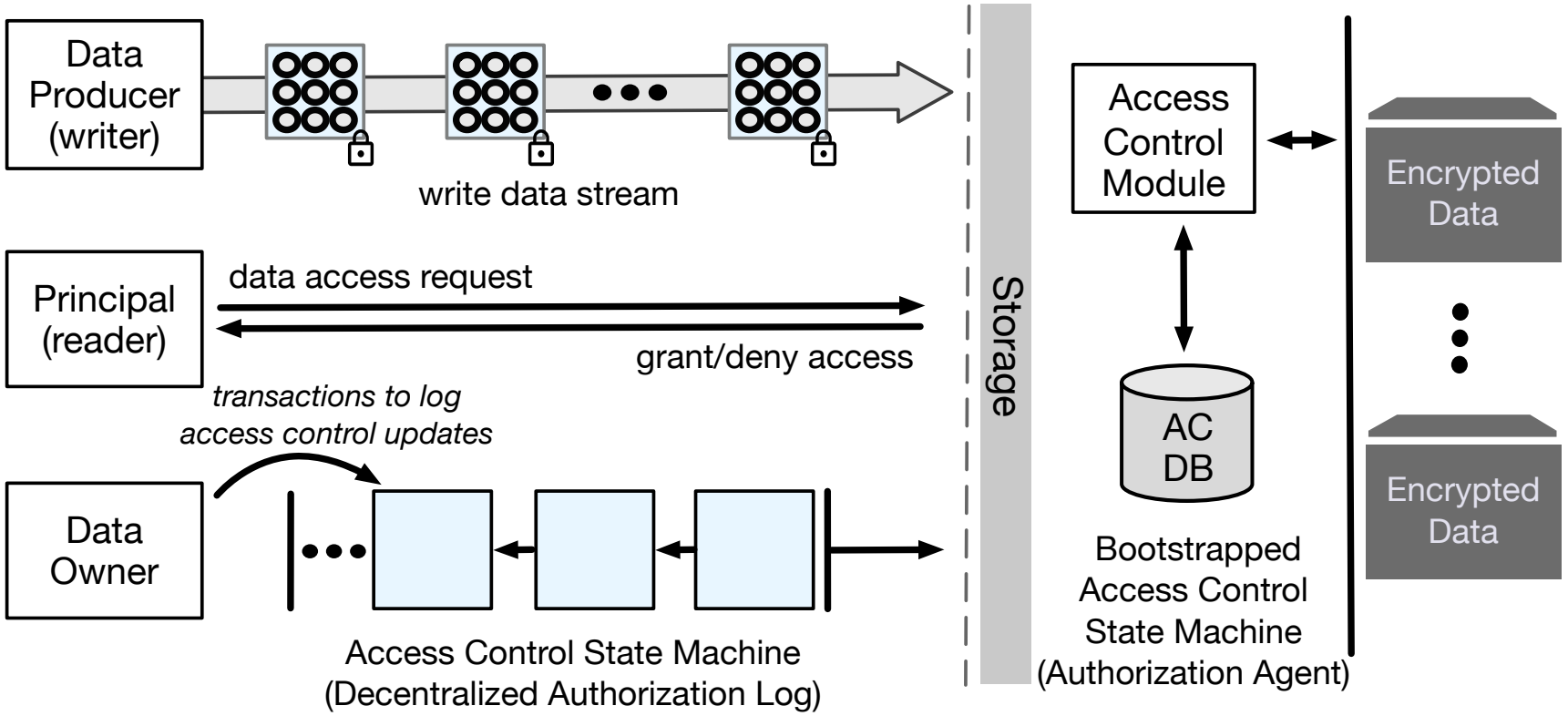
Droplet Authorization



Droplet Authorization



Droplet Authorization

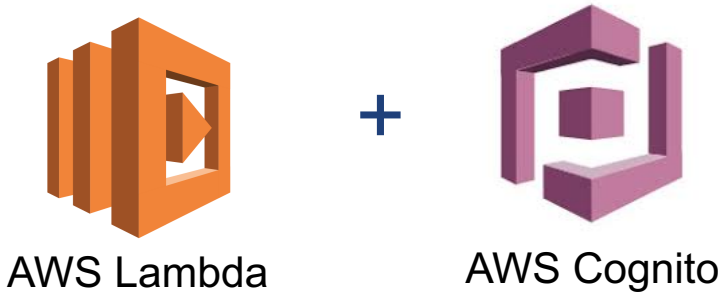


Implementation

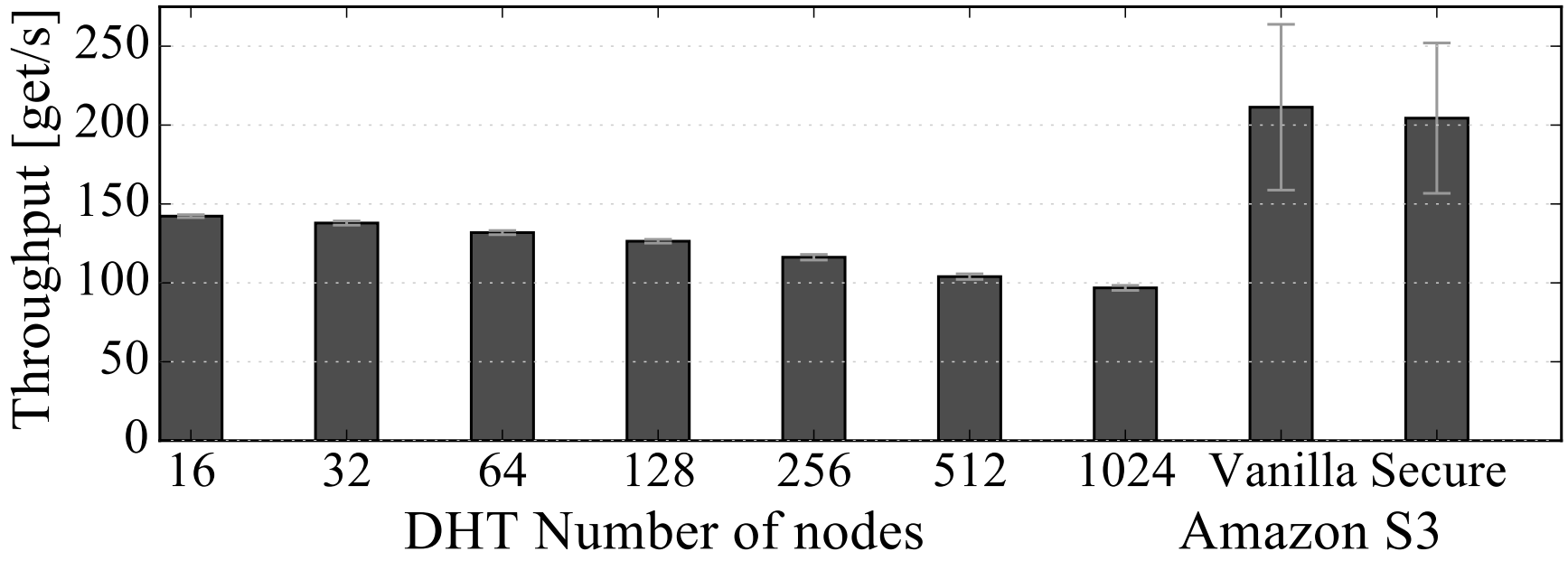
- Droplet Reference Implantation (https://dropletchain.github.io/)
  - Actors: client engine, storage-node engine, authorization agent (virtualchain)
  - Storage: Cloud (AWS S3), p2p storage (S/Kademlia)
  - Platforms: IoT (ARM Cortex), smartphone (Nexus 5), cloud (Amazon t2.micro)

Case Study: Serverless Computing

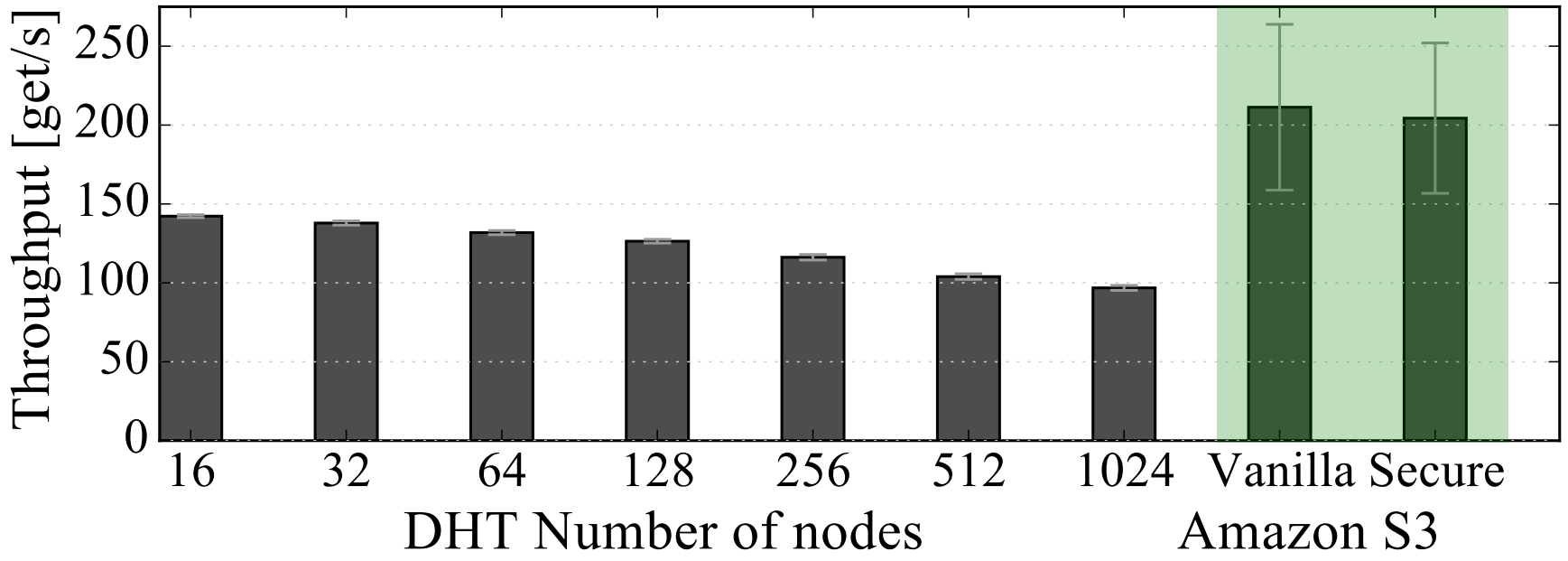
- Long-lived and more broadly-scoped access tokens for OAuth2
- Lookup latency 0.4% longer with Droplet



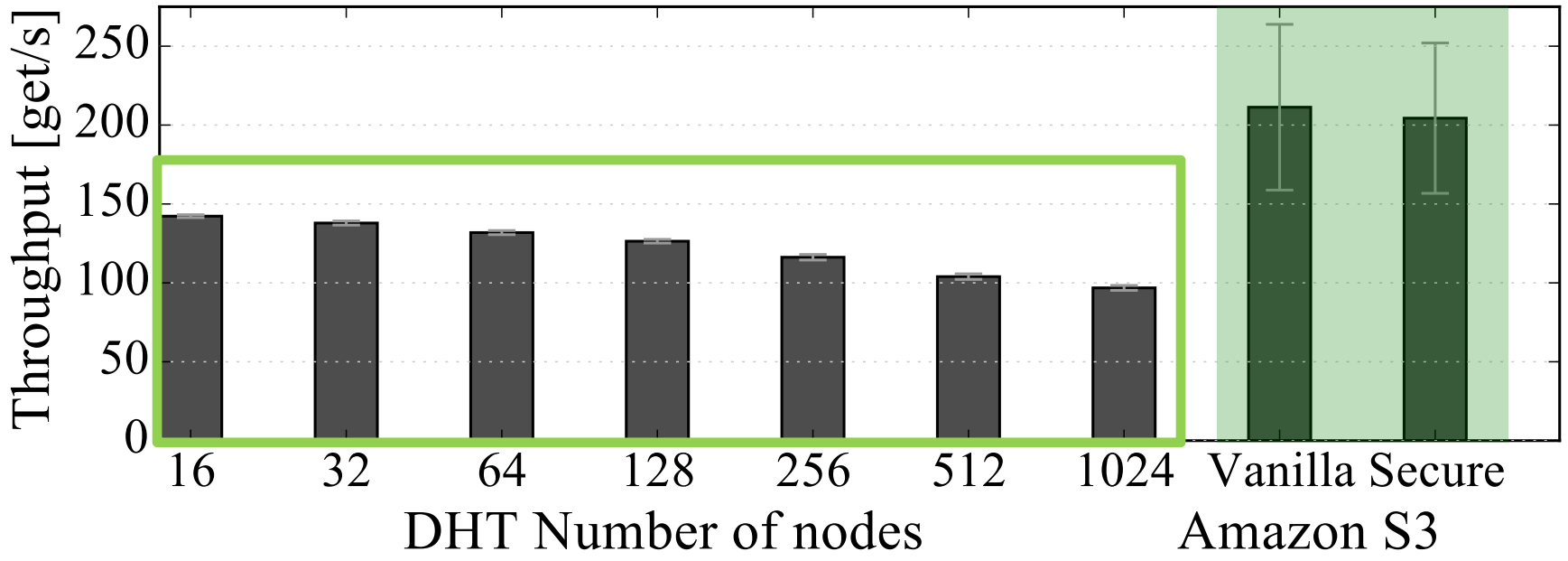
Read Throughput



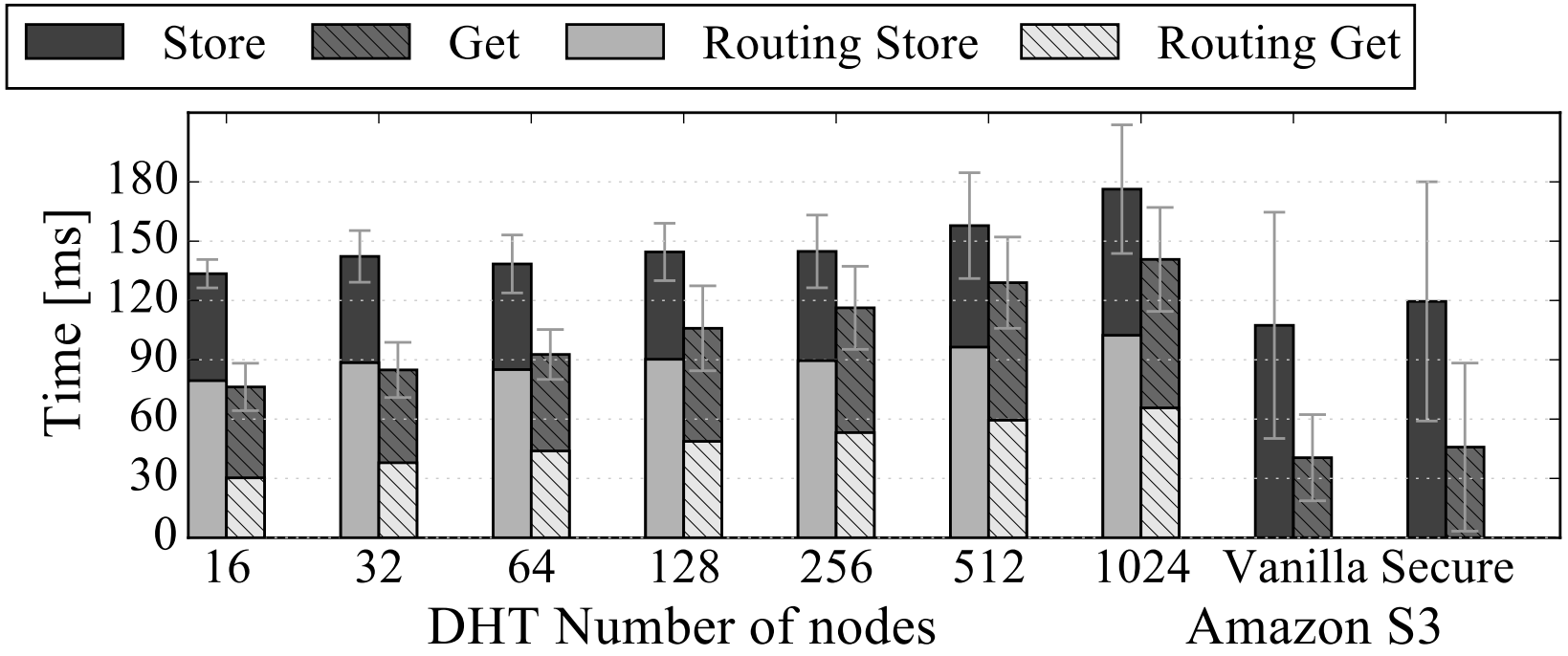
Read Throughput



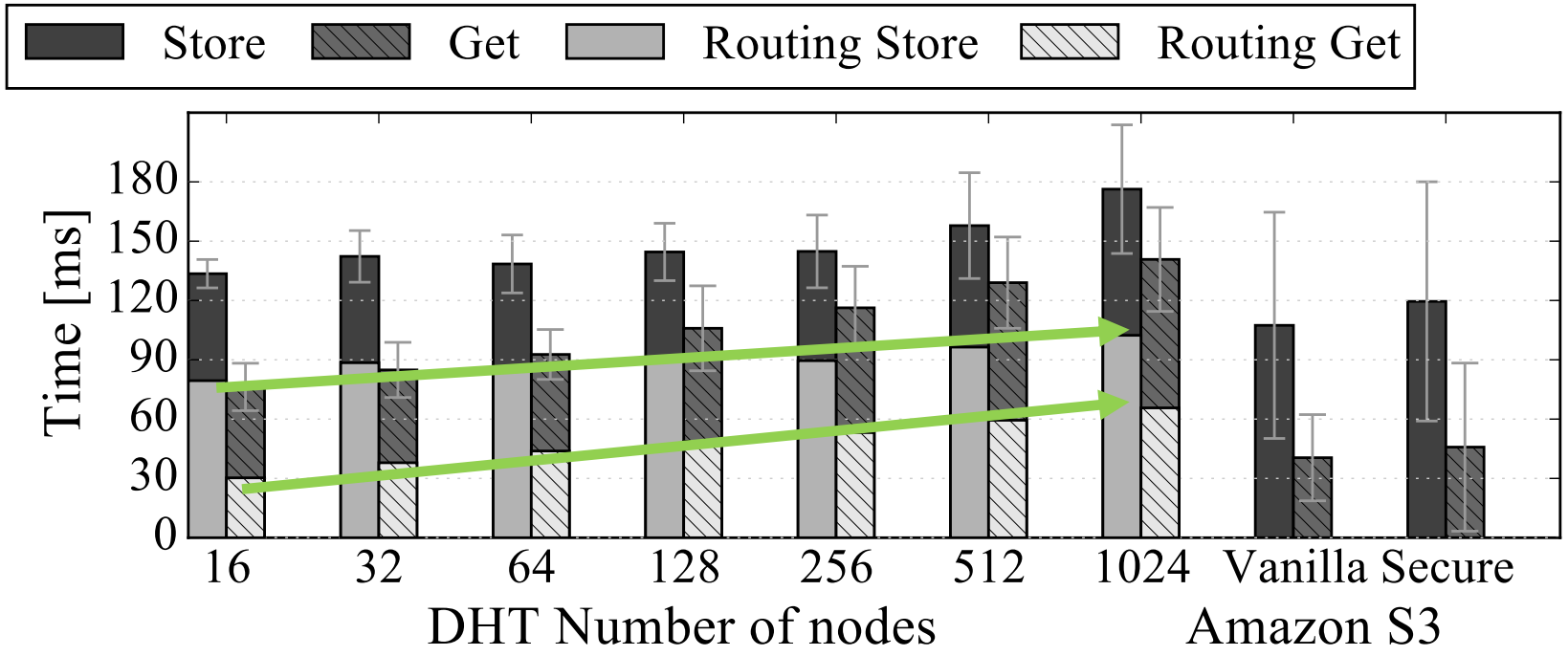
Read Throughput



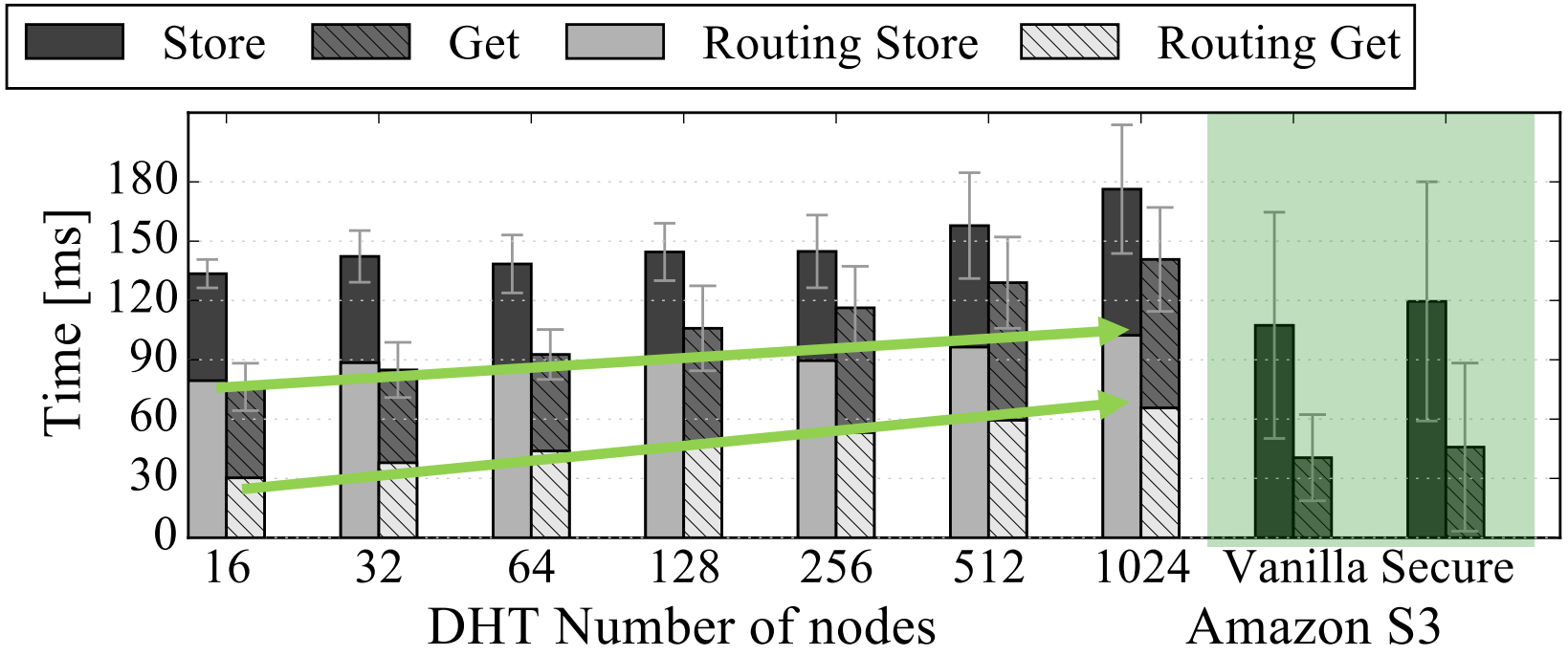
Read/Write Latency



Read/Write Latency



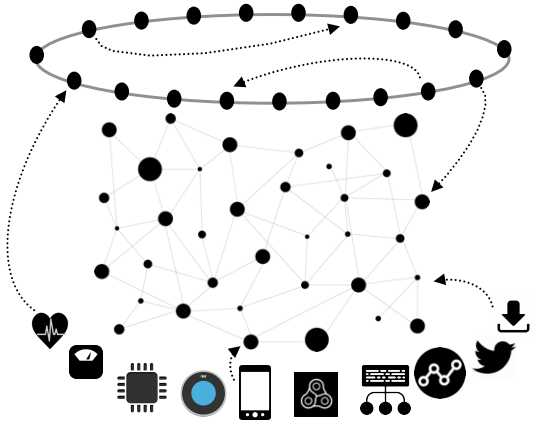
Read/Write Latency



Conclusion

Droplet is a new decentralized authorization and data access control service:

- a new cryptographic access control construction tailored for stream data
- a new decentralization authorization service
- ensures data owner's sovereignty and ownership over their data



dropletchain.github.io