Droplet: Decentralized Authorization and Access Control for Encrypted Data Streams

Hossein Shafagh, Lukas Burkhalter, Sylvia Ratnasamy, Anwar Hithnawi
Rise of Real-Time Data

Autonomous Driving

Health Care

Internet of Things

Telemetry/DevOps
Monolithic Applications

Data Sources: Fitbit Sensor, Medical Sensor, Telemetry

Storage/Servers

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

End-to-End Encryption
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

User

Fitbit Sensor

Medical Sensor

Telemetry
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

Diagram:
- User
- E.g. OAuth
- Fitbit Sensor
- Medical Sensor
- Telemetry
Access Authorization

- Authorization tokens are issued by trusted intermediary (invoked per request)
- No cryptographic guarantees / decoupled from data protection
- **Challenge 2**: Decentralized 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

Data Producer (writer)

write data

Encrypted Data

Trusted

Storage

Untrusted

Data Owner

ACL DB

Bootstrapped Access Control State Machine (Authorization Agent)

data access request

grant/deny access

transactions to log

Access Control State Machine (Decentralized Authorization Log)

Encrypted Data

Data Producer (writer)

Principal (reader)

Trusted

Semi-Trusted (restricted access)

Authorization Layer (e.g., PBFT, Nakamoto consensus)

write data

read data

manage access

read access
Overview and Threat Model

- **Data Producer (writer)**
  - Trusted

- **Principal (reader)**
  - Semi-Trusted (restricted access)

- **Storage**
  - Encrypted Data
  - Untrusted

- **Actions**
  - **write data**: Trusted → Untrusted
  - **read data**: Untrusted → Semi-Trusted

- **Authorization Layer**
  - (e.g., PBFT, Nakamoto consensus)

- **Access Control Module**
  - ACL DB
  - Bootstrapped Access Control
  - State Machine (Authorization Agent)
  - Grant/deny access
  - Transactions to log
  - Access control updates
Overview and Threat Model

- Trusted
- Semi-Trusted (restricted access)
- Trusted

Data Producer (writer)
Principal (reader)
Data Owner

write data
read data

Encrypted Data

Access Control State Machine (Decentralized Authorization Log)

Authorization Layer (e.g., PBFT, Nakamoto consensus)

Trusted
Semi-Trusted (restricted access)
Untrusted
Overview and Threat Model

1. **Data Producer (writer)**: Trusted
2. **Principal (reader)**: Semi-Trusted (restricted access)
3. **Data Owner**: Trusted
4. **Authorization Layer (e.g., PBFT)**
5. **Encrypted Data**: Untrusted
Droplet: Encryption-based Access Control

- **Data Producer (writer)**
- **Principal (reader)**
- **Data Owner**

Write data stream

Storage

- Encrypted Data

Access Control State Machine

ACL DB

Bootstrapped Access Control

Decentralized Authorization Log

Data access request

Grant/deny access

Transactions to log

Access control updates
Droplet: Encryption-based Access Control
Droplet: Encryption-based Access Control

- Data Producer (writer)
- Principal (reader)
- Data Owner

- Write data stream
- Encrypted Data
- Key Stream: $k_0, k_1, k_2, k_3, k_4, \ldots$
- Time-encoded key-streams

- Access Control State Machine (Authorization Agent)
- Data access request
- Grant/deny access
- Transactions to log
- Access control updates

Key Stream: $k_0, k_1, k_2, k_3, k_4, \ldots$ and
Time-encoded key-streams
Droplet: Encryption-based Access Control

- Data Producer (writer)
- Principal (reader)
- Data Owner

- Write data stream
- Encrypted Data
- Data Producer (writer)
- Principal (reader)
- Data Owner

- Key Stream: $k_0, k_1, k_2, k_3, k_4, \ldots$
- Time-encoded key-streams

- Access Control State Machine (Decentralized Authorization Log)
- ACL DB
- Bootstrapped Access Control State Machine (Authorization Agent)
- Data access request
- Grant/deny access
- Transactions to log
- Access control updates

- Binary Hash Tree
- Shared nodes/branches
- Derived DEK
- DEK (Data Enc Key)
- Dual key encryption
- SEK (Subscriber Enc Key)
- Enc_{DEK}(time)
Droplet Authorization

Data Producer (writer)

Principal (reader)

Data Owner

Access Control State Machine (Decentralized Authorization Log)

write data stream

access control updates

Storage

Encrypted Data

27
Droplet Authorization

Data Producer (writer)

write data stream

Principal (reader)

Data Owner

access control updates

Access Control State Machine (Decentralized Authorization Log)

Encrypted Data

ACL DB

Bootstrapped Access Control State Machine

Decentralized Authorization Log

grant/deny access

transactions to log

Storage
Droplet Authorization

- **Data Producer (writer)**
- **Principal (reader)**
- **Data Owner**

**Access Control Updates**

**Access Control State Machine** (Decentralized Authorization Log)

- $tx_a$: register device
- $tx_g$: add principal
- $tx_r$: add/revoke

**Decentralized Authorization Log (blockchain)**

**Entry**
- Owner
- Stream ID
- Private Access Policy
- Encrypted Keys

**State Updates**

**Authorization Agent**
Droplet Authorization

- **Data Producer (writer)**
- **Principal (reader)**
- **Data Owner**
- **Data Access Request**
- **Grant/Deny Access**
- **Transactions to Log**
- **Access Control Updates**
- **Bootstrapped Access Control State Machine (Authorization Agent)**
- **Access Control Module**
- **AC DB**
- **Encrypted Data**

**Diagram Description:**
- Data Producer (writer) writes data stream.
- Principal (reader) accesses data.
- Data Owner manages access control updates.
- Access Control State Machine (Decentralized Authorization Log) monitors access requests.
- Bootstrapped Access Control State Machine updates AC DB.
- Access Control Module accesses Encrypted Data.

**Key Terms:**
- **Droplet Authorization**
- **Encrypted Data**
- **Access Control Module**
- **ACL DB**
- **Bootstrapped Access Control State Machine**
- **Access Control State Machine** (Decentralized Authorization Log)
- **AC DB**
- **Encrypted Data**
Droplet Authorization

Data Producer (writer)

Data Producer (writer)

write data stream

Principal (reader)

data access request

transactions to log
access control updates

Data Owner

Access Control State Machine (Decentralized Authorization Log)

Access Control Module

grant/deny access

transactions to log
access control updates

Encrypted Data

Bootstrapped Access Control State Machine (Authorization Agent)

AC DB

Encrypted Data
Implementation

- **Droplet Reference Implantation** ([https://dropletchain.github.io/](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 Chart](chart.png)

Throughput [get/s] vs DHT Number of nodes and Amazon S3.
Read Throughput

![Bar chart showing read throughput for different DHT numbers of nodes and two options: Vanilla and Secure. The x-axis represents the number of nodes (16, 32, 64, 128, 256, 512, 1024), and the y-axis represents throughput [get/s]. The Secure option consistently shows higher throughput compared to Vanilla.]
Read Throughput

Throughput [get/s]

<table>
<thead>
<tr>
<th>DHT Number of nodes</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
<th>256</th>
<th>512</th>
<th>1024</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vanilla Secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Read/Write Latency

![Graph showing Read/Write Latency](image)

- **Store**
- **Get**
- **Routing Store**
- **Routing Get**

- **DHT Number of nodes**: 16, 32, 64, 128, 256, 512, 1024
- **Time [ms]**: 0 to 180
- **Amazon S3**

---

37
Read/Write Latency

![Graph showing read/write latency for different DHT numbers of nodes and Amazon S3. The graph compares Store, Get, Routing Store, and Routing Get operations.](image_url)
Read/Write Latency

![Graph showing Read/Write Latency with different DHT Number of nodes and Time [ms] for Store, Get, Routing Store, and Routing Get.]
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