BEAF: A Blockchain and Edge Assistant Framework with Data Sharing for IoT Networks

Report: Yingxun Hu
Email: hyx@njust.edu.cn
Nanjing university of science and technology
01 / Introduction
02 / System Model
03 / The Framework BEAF
04 / Security Analysis
05 / Performance Discussion
06 / Conclusions
Introduction
Background

An Information Carrier

the fifth generation (5G)

artificial intelligence technology

IoT market has fully exploded
Introduction

decentralized authentication

privacy threats and data sharing

malicious tracking
Introduction

- resource allocation
- social cost saving
- information resource utilization rate reasonably
- user privacy disclosure
- data integrity problem
- unauthorized data access
Introduction

Blockchain + Edge Computing

data security privacy protection
Introduction

Consortium blockchains
Introduction

- Edge computing
- Data generating
- Data processing
- Data analysis
Literature review

1. A medical data sharing model via blockchain
2. A secured proxy-based data sharing module in IoT environments using blockchain
3. A secure solution for intelligent vehicle data sharing
4. A new mechanism SeShare for data storing based on blockchain
5. The user-controlled privacy-preserving user profile data sharing based on blockchain

- The use of traditional public key infrastructure (PKI)
- A new class of privacy indicators -- Data Controller Indicators (DCIs)
- A public key re-encryption scheme

Scheme

- A cross-domain based data sharing scheme in cooperative edge computing
- A distributed algorithm developed for VNET
System Model
System model

- traditional centralized cloud architectures
  - security
  - scalability

- Edge computing
  - computing resources
  - data processing

- Blockchain
  - the resource allocation of edge networks

BEAF

users
System model

Figure 1
System model

User
- upload data
- query & download data

Edge Node
- distribution computation
  → data upload, data encryption and data downloaded

Background Server
- Syst. Management
- Trace malicious user

Blockchain
- Data storage
- Tracing
Requirements

- Confidentiality
- Data integrity
- Availability
- System reliability
- System scalability
- System efficiency
- Stability and ease of use
The Proposed Framework BEAF
Framework

Figure 2
Register:

- $U \rightarrow BS : Id_U, \text{reg}, U_{\text{Info}}$
- $BS \rightarrow BC : Id_U, \text{reg}, U_{\text{Info}}$
- $BC \rightarrow BS : \text{secret}$
- $BS \rightarrow U : \text{secret, indel.html}$
Framework

Login:

- $U \rightarrow BS : Id_U, \text{secret}, \log_U$
- $BS \rightarrow BC : Id_U, \text{secret}, \log_U$
- $BC \rightarrow BS : true$
- $BS \rightarrow U : \text{indel.html}$
Framework

Upload:

1. $U \rightarrow BS : Id_U, file_U, U_{\text{per}}, \text{perOrg and req\_up}$
2. $U \rightarrow EN : file_U$
3. $EN \rightarrow BC : file_U$
4. $BS \rightarrow BC : Id_U, U_{\text{per}}, \text{perOrg}$
5. $BC \rightarrow BS : suc$
6. $BS \rightarrow U : suc$
## Framework

### Query:

1. **ONE**
   - \( U \rightarrow EN : Id_U, req\_Info \)

2. **TWO**
   - \( EN \rightarrow BC : Id_U, req\_Info \)

3. **THREE**
   - \( BC \rightarrow EN : Info \)

4. **FOUR**
   - \( EN \rightarrow U : Info \)

### Download:

5. **FIVE**
   - \( U \rightarrow EN : file_N \)

6. **SIX**
   - \( EN \rightarrow BC : file_N \)

7. **SEVEN**
   - \( BC \rightarrow EN : file_U \)

8. **EIGHT**
   - \( EN \rightarrow U : file_U \)
Security Analysis
Security analysis

**Confidentiality**
- Registered users
- Encryption

**Availability**
- Monitor
- Consensus mechanism

**Reliability, stability, and scalability**
- Illegal / incomplete
- Single point of failure

**Data integrity**
- Authentication
- Encryption
- Immutability

**Traceability**
- Source & ownership
- Other disputes
- Liability determinations
Performance Discussion
Performance discussion

Environment

1. Webstorm2020.1.1.x64
2. express-session:1.17.1
3. docker 21.03
4. Fabric-node-sdk1.4
5. Nodejs v8.17.0
6. Golang 1.10.3
7. Npm 6.13.4
8. Ubuntu 18.04
## Performance discussion

<table>
<thead>
<tr>
<th>Performance</th>
<th>Specific Indicators</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average Response Time</strong></td>
<td>Query (Single file)</td>
<td>372ms</td>
</tr>
<tr>
<td></td>
<td>Query (All file)</td>
<td>362ms</td>
</tr>
<tr>
<td></td>
<td>Upload</td>
<td>572ms</td>
</tr>
<tr>
<td></td>
<td>Download</td>
<td>291ms</td>
</tr>
<tr>
<td><strong>Reliability</strong></td>
<td>System stable</td>
<td>7*24h</td>
</tr>
<tr>
<td></td>
<td>(operation duration)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System failure rate</td>
<td>5 times/week</td>
</tr>
</tbody>
</table>

TABLE II. The performance of the proposed BEAF
Conclusions
Conclusions

- **Objectives**: secure data sharing and privacy preservation
- **Security**: data security, data authenticity, privacy protection, data tamper resistance, and traceability
- **Performance**: data query efficiency and system reliability.
- **BEAF**: employ blockchain and edge computing paradigms
THANKS!