Blockchain-based Federated Learning: privacy and incentive

ECE6903J - Distributed Machine Learning Systems (Research project)

Hugo Vanhille, Pedro Hernández Rubio

Department of Automation

2022 年 12 月

目录

1. **Background**
   - Motivation
   - Crowdsensing
2. **Research**
   - Problems
   - The privacy-preserving of crowdsensing
   - The incentive mechanism of crowdsensing
3. **System architecture**
   - Software application
4. **Security issues: privacy**
   - Single point of failure
5. **Quality management: incentive**
   - Mechanism design: multifactor
   - Mechanism design: issues
6. **Conclusions**
   - Application
   - Limitations
   - Further research

第 1 节

Background

第 1 节

Background

第 1 小节

Motivation

Motivation

Goal

Applying ML to systems (blockchain-based models)

- Research line mainly targeted to blockchain technology (its application to systems)
- Research group in Department of Automation (PhD supervisors) has been recently working in blockchain-based models applied to trust management systems
- Specifically, applied to data-aggregation systems in the Internet of Things (IoT) field crowdsensing
- Could similar approach be applied for Federated Learning?

第 1 节

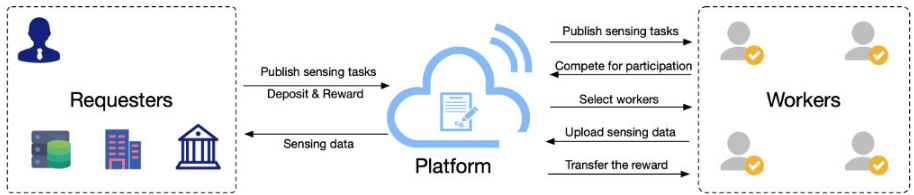
Background

第 2 小节

Crowdsensing

Crowdsensing: definition

- **Crowdsensing:** emerging paradigm of data aggregation[paper1], having a key role in data-driven applications. Specially used for getting large ammounts of IoT sensing data, by using the individual intelligent sensing devices.
- **Benefit:** improved data collection efficiency and reduced costs effectively[paper2]



Crowdsensing: issues

1. Managed and maintained centralized platforms suffer from the single point of failure

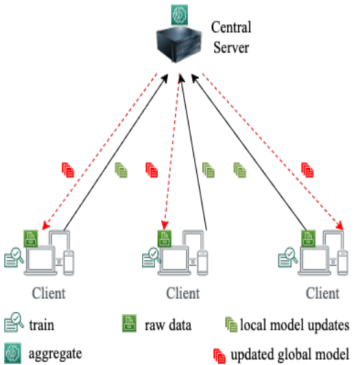


图: Topology of traditional FL

Crowdsensing: issues

1. Encouraging workers by offering appropiate incentive mechanisms (monetary usually) →auction theory guarantees benefits for both requesters and workers[paper15] but only provide short-term incentives

图: Monetary reward

图: Worker reputation

图: Data quality

第 2 节

Research

第 2 节

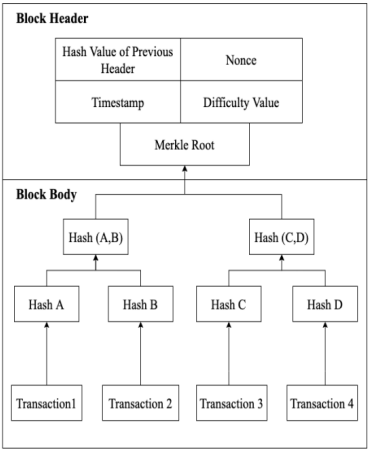
Research

第 1 小节

Problems

Blockchain background

Distributed ledger containing a time-stamped series of immutable blockchains, trustless, decentralized, proof-tampering and full traceability



第 2 节

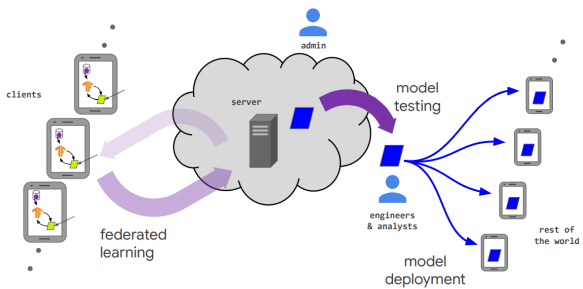
Research

第 2 小节

The privacy-preserving of crowdsensing

The privacy-preserving of crowdsensing

- FL provides an attractive structure (presented in (Kairouz et al.)) for decomposing the overall machine learning workflow into the approachable modular units we desire.
- FL provides a level of privacy to participating users through data minimization.



第 2 节

Research

第 3 小节

The incentive mechanism of crowdsensing

The incentive mechanism of crowdsensing

- Main types of incentive mechanisms:
  1. Monetary-based: distributing rewards.
  2. Reputation-based: reputation framework for worker selection (algorithms)
- **Limitations**
  1. Relies on a central platform, vulnerable to target attacks
  2. Single-attribute incentive mechanisms (multifactor incentive needed)

第 3 节

System architecture

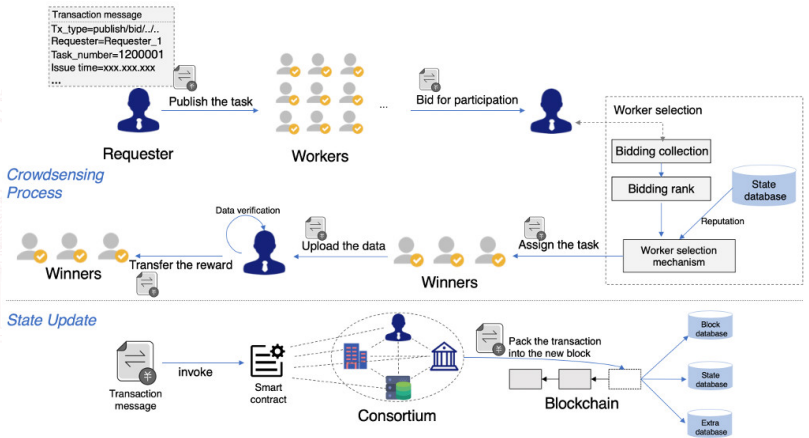
第 3 节

System architecture

第 1 小节

Software application

System architecture



第 4 节

Security issues: privacy

第 4 节

Security issues: privacy

第 1 小节

Single point of failure

第 5 节

Quality management: incentive

第 5 节

Quality management: incentive

第 1 小节

Mechanism design: multifactor

Mechanism design: multifactor

- Based on three parameters:
  1. Workers' bidding
  2. Reputation
  3. Recent data quality estimation
- Analytic Hierarchy Process (AHP) framework →(top-down)
  1. Objective level: winning workers
  2. Criteria level: parameters criteria
  3. Alternative level: workers available

Multifactor worker evaluation approach

$$\theta_i = \omega_1 B_i + \omega_2 R_i + \omega_3 Q_i \qquad \text{where } \omega_i \geq 0 \text{ and } \sum_{\omega_i=1}^{3} \omega_i = 1$$

第 5 节

Quality management: incentive

第 2 小节

Mechanism design: issues

Mechanism design: issues

1. **How to select appropriate workers?**
   - **Proposal:** decentralized architecture (blockchain technology) that lacks a single point of failure, and enhances privacy with asymmetric encryption and digital signature technology
2. **How to distribute the rewards to the workers?**

With the help of mechanism design theory[article56] two important properties for the incentive mechanism are guaranteed:

- **Incentive quality (IC):** the truthful submission of sensing cost is the worker's optimal bidding strategy
- **Individual rationality (IR):** the reward must compensate for the worker's cost (non-negative)

第 6 节

Conclusions

第 6 节

Conclusions

第 1 小节

Application

Results

A consortium blockchain-based incentive model for crowdsensing system is proposed

- **Benefits of consortium blockchain technology:**
  - resistant to the single point of failure (system security)
  - cooperative management (by requesters) reduces cost and enhances the flexibility of the system (selection criteria)
- **Benefits of hybrid incentive mechanism:**
  - encourages workers to contribute valuable data (and penalizes malicious ones)
  - ensures favorables short-term and long-term incentives for workers

第 6 节

Conclusions

第 2 小节

Limitations

Limitations

Further research:

1. Dynamic situation where evaluations attributes are changing
2. Optimization of consensus protocol (better performance)
3. Further protection of worker privacy

Possible solutions

Application of ML techniques to blockchain-based system

第 6 节

Conclusions

第 3 小节

Further research

第 I 部分

附录

参考文献

参考文献 I

[1] JIANG X, WANG H, CHEN Y, et al. MNN: A Universal and Efficient Inference Engine[EB/OL]. arXiv. 2020. https://arxiv.org/abs/2002.12418.

谢谢