Peer-to-Peer Networking and Applications (2024) 17:2595–2607
https://doi.org/10.1007/s12083-024-01728-5

Invisible man: blockchain-enabled peer-to-peer collaborative privacy games in LBSs

Beining Zhang[1] · Hang Shen[1] · Tianjing Wang[1] · Guangwei Bai[1]

Received: 4 November 2023 / Accepted: 6 May 2024 / Published online: 24 May 2024

Abstract
Most user-collaborative location privacy protection mechanisms assume that collaborative group members are trustworthy and can strictly enforce collaboration rules. Such assumptions do not match reality and reduce the usability of the schemes. In this paper, we propose Invisible Man, a blockchain-enabled framework for peer-to-peer collaborative privacy games for location-based services. The framework enables users to protect their privacy in extreme environments and allows members of a collaborative group without trust to collaborate efficiently. To defend against inference attacks, a user-collaborative privacy game model is constructed, and a dual-verification mechanism with Chainlink and Witnet oracles is developed to provide security guarantees for model generation. Members can conduct cooperative games under the guidance of the model. To realize secure and efficient in-group collaboration, a blockchain-based reward and punishment mechanism for collaboration is designed, integrating token incentives and a blacklisting mechanism to ensure the verifiability and audibility of user behaviors. Security analysis and extensive simulation results demonstrate that the proposed scheme achieves high security and privacy with low costs.

Keywords Blockchain · Location-based service · Collaborative privacy game · Oracle · Token incentive

1 Introduction

Location-based services (LBSs) provide location-related value-added services to positioning devices through mobile internet. While bringing great convenience to our lives, their extensive use also severely threatens user privacy [1]. Privacy game mechanisms [2, 3] can tailor protection strategies according to attack means, thus effectively defending against inference attacks based on user profiles. Such methods remain effective even when the privacy protection strategies are leaked. Most existing privacy games employ a user-centric paradigm [4, 5], adjusting protection policies according to user profiles. In contrast, collaborative privacy game mechanisms (CPGMs) take a group-centric approach and interfere with the attacker's observations by hiding the behaviors of individual users within the group. However, for collaboration to be effective, team members must be honest, trustworthy, and comply with the collaboration rules. Most CPGMs make such assumptions by default, but this is inconsistent with reality with reduced applicability [6].

An effective CPGM must be able to address both external threats and internal harms to the group. External threats come from untrustworthy LBSs, which can infer secrets (e.g., destinations, hobbies, home addresses, workplaces) based on historical locations or activity trajectories [7, 8]. Internal threats arise from malicious or selfish group members. Malicious members may steal sensitive information from group interactions, while selfish members may react sluggishly or falsely claim that tasks have been completed.

Blockchain originated from Bitcoin technology and is essentially a replicated state machine protocol in a Byzantine environment [9]. Its decentralized, auditable, and tamper-proof characteristics can help build more secure distributed systems and address the applicability issues of CPGMs.

✉ Hang Shen
hshen@njtech.edu.cn

Beining Zhang
202161120012@njtech.edu.cn

Tianjing Wang
wangtianjing@njtech.edu.cn

Guangwei Bai
bai@njtech.edu.cn

[1] College of Computer and Information Engineering (College of Artificial Intelligence), Nanjing Tech University, Nanjing 211816, China

First, the blockchain ledger can permanently store users' historical behaviors, facilitating the record and traceability of critical collaboration data and illegal user behaviors. Second, incentive mechanisms can curb malicious behaviors of users in collaborations, providing an ideal platform for regulating collaborative behaviors. The above considerations have driven our development of a blockchain-based group collaboration scheme with challenges. Privacy game relies on trusted user data off the chain, and the process of data being retrieved to the chain carries an enormous security risk. Smart contracts deployed on the blockchain can collaborate with oracle contracts [10], which opens up new ideas to address this challenge.

1.1 Challenges and related works

Mobile Internet is a complex environment, which brings many challenges to collaborative privacy protection in LBSs:

1. **Collaborative privacy protection:** Collaborative privacy protection mechanisms do not need to rely on third-party anonymity servers, and hiding user identities through collaboration is the focus of researchers. In MobiCrowd [11], users search caches from neighbors before initiating a query. The query is directly published to the LBS if the required content is not found. This work provides valuable references. CTPP [12] is a virtual machine-based scheme where mobile users can communicate with multi-hop neighbors and share cache information. EPcloak [13] prevents privacy leakage when users communicate directly with the LBS. If a user cannot obtain service locally, queries are sent to virtual requesters individually. The user's identity, points of interest (POIs), and location are from the virtual requester, user, and initiator. Chow et al. [14] designed a P2P (peer-to-peer) spatial anonymity strategy where users randomly select k-1 neighbors to form an anonymous set, then send the formed hidden area or any non-query user's location to the LBS. Niu et al. [15] improved [14] to defend against variance-based attacks. Unlike the above works assuming mutual trust among group members, P^4QS [16] focuses on collaboration between strangers. By using symmetric and asymmetric encryption, each user only obtains the required information, but at the cost of additional system overhead. For insecure decentralized systems, Jin et al. [17] proposed a security enhancement scheme for data sharing that maintains accountability through pseudonymous identity verification while protecting user privacy. How to effectively carry out cooperation and behavior supervision in a group under the premise of incomplete trust needs further research.
2. **Privacy games by collaboration:** The game mechanism can find the optimal solution to balance the privacy level and service quality loss while considering the demands of both parties. However, most existing privacy game models focus on two-party game scenarios. In the zero-sum Bayesian game models proposed by Shokri et al. [5, 18], the attacker establishes a one-on-one game with the user utilizing prior knowledge, where the user aims to maximize privacy level while ensuring service-quality loss is above a given threshold. Shen et al. [19] analyzed trajectory privacy protection under quality loss and energy constraints by constructing a one-on-one privacy game centered on the user. The optimal data obfuscation problem is transformed into a user-attacker privacy game [20], where the joint differential-distortion privacy metric ensures privacy level and utility cost remain optimal when using a single metric. Few studies focused on multi-party privacy games in LBSs. Considering multi-party privacy conflicts in online social networks, Ding et al. [21] modeled the interaction behaviors among co-owners as a multi-participant non-cooperative game, where the network structure characterized social relationships among co-owners. Hong et al. [4] analyzed strategy interactions between users and adversaries in dynamic Bayesian games, proving the user's equilibrium strategy depends on the adversary's capability of accessing geographic data. In [22], they further studied how multiple users collaboratively query with obfuscation to defend against inference attacks. The above works focus on strategy selection and privacy protection under one-to-one and multi-party non-cooperative games. Modeling a multi-player cooperative game and finding the optimal combination of strategies need further investigation.
3. **Trust in collaboration:** The collaborative privacy protection mechanism can avoid the shortcomings of centralized management, relying on a trusted third party. However, most existing protection mechanisms assume that members trust each other. Fewer studies have addressed trust and security issues in collaborative LBS queries. Li et al. [23] used anonymous digital certificates and anonymous stealth zones to protect the privacy and security of vehicles in LBSs, and records and maintain the trust values through blockchain to defend against various attacks. Feng et al. [24] used consortium blockchain to manage trust data and identify misbehaving vehicles. Their scheme adopted edge computing and cross-region anonymizer cooperation to construct trusted cloaking areas for efficient location privacy preservation. In [25], the authors maintained two blockchains simultaneously to store all vehicles' query records and digital certificate information, allowing the authority to track and investigate malicious users.

Chaudhary et al. [26] used consortium blockchain to realize the decentralized registration and authentication of vehicles, and the system's transparency was achieved by storing vehicles' identities through blockchain. They also designed an anonymous communication mechanism based on blockchain to hide user identities. In [27], the authors realized decentralized vehicular network architecture and adopted *k*-anonymous unified technology to prevent vehicle location disclosure. The scheme in [28] implemented decentralized insurance contract execution and claim processing and realized personalized and dynamic adjustment of auto insurance pricing through secure data collection. A blockchain-based data transaction scheme was proposed in [29], which supports fine-grained data transactions and realizes privacy protection through cryptography. These studies show blockchain can provide an excellent solution to user collaboration security and trust issues.

1.2 Main contributions

This paper proposes a blockchain-based peer-to-peer collaborative privacy game framework for LBSs, which includes secure CPGM generation and a reward and punishment mechanism for collaboration, enabling originally distrustful in-group members to collaborate efficiently and jointly defend against external and internal attacks.

- A multi-user collaborative privacy game model is constructed, which imposes mobility privacy to reduce the probability of actual data being inferred in successive queries, and combines distortion privacy to measure anti-attack effectiveness. The on-chain and off-chain data interactions are achieved through the Oracle mechanism, aiming to provide a security guarantee for model generation. Group members disguise query messages and select collaborators under the guidance of the game model;
- A reward and punishment mechanism is designed to achieve secure and efficient privacy gaming. Token-based incentives motivate users to actively participate in collaboration by giving them positive rewards, while a blacklisting mechanism ensures that user behavior is regulated and the gaming process is auditable;
- Security analysis and simulation results demonstrate the effectiveness of CPGM in urban areas and suburbs. In particular, CPGM can significantly improve the overall privacy level over that provided by traditional one-on-one privacy game mechanisms. Our findings also indicate that simply expanding group size fails to raise user privacy levels continuously and can lead to increased collaborative costs; fortunately, an optimal group size provides a high privacy level at the lowest cost.

The remainder of this paper is organized as follows. Section 2 describes the system model, consisting of threat models and design goals. In Section 3, we construct the secure generation framework for CPGM and detail its generation. Section 4 designs a secure and verifiable in-group collaboration scheme. We conduct security analysis in Section 5 and validate the performance through simulations in Section 6. Section 7 concludes this paper and discusses future work.

2 System model

Consider a blockchain-based collaborative LBS scenario, shown in Fig. 1, in which two types of malicious participants exist:

- **Suspicious LBS** may infer the real identity of queries based on the background knowledge and associate the query information with their real identities for malicious behavior.
- **Untrusted collaborators** refer to the group member participating in query forwarding and result returning.

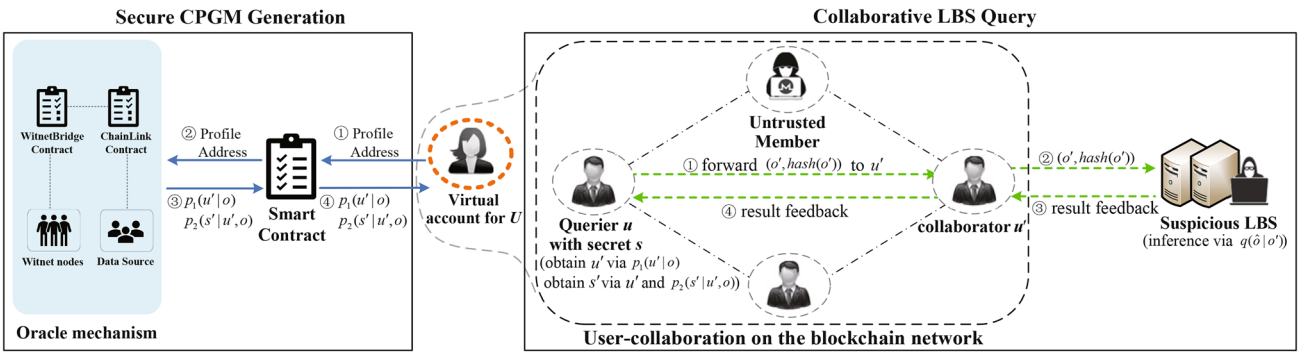


Fig. 1 Collaborative privacy game framework

They may refrain from responding to collaboration requests, forward query results, and even tamper or forge query requests and results. Some members may cheat smart contracts to obtain repeated rewards for legitimate cooperation behavior.

Users on the blockchain network can spontaneously form collaborative groups, leverage oracles to retrieve off-chain data, and generate customized CPGMs. Members in each group perform combined queries under the guidance of the CPGM to defend inference attacks based on prior knowledge. Meanwhile, an in-group scheme integrating token incentives and a blacklisting mechanism is designed to ensure the security and verifiability of in-group collaboration.

2.1 Scheme overview

As shown in Fig. 1, the proposed framework consists of secure CPGM generation and collaborative LBS query, where the defined notations and operations are as follows.

- U represents the set of collaborative group members;
- $o = \{u, s\}$ is the original query information, which consists of the identity of querier u, and s is the secret of the querier (e.g., u's location or preference);
- $p_1(u'|o)$ is a forwarding function for the querier u. When o is given, the collaborator u' for u is determined by sampling from the probability distribution;
- $p_2(s'|u', o)$ is a fuzzy function for the querier. Given u' and o, it can output a fuzzified secret s' based on the probability distribution. u forwards the generated s' to the collaborator u';
- $o' = \{u', s'\}$ is an LBS query submitted by the collaborator u'. It is observable by users across the network;
- $q(\hat{o}|o')$ is the inference function held by the listener, where $\hat{o} = \{\hat{u}, \hat{s}\}$, and $\hat{u}$ and $\hat{s}$ represent estimates of the querier's identity and secret, respectively. After observing o', the listener infers the original querier and secret encapsulated in $\hat{o}$ by running $q(\hat{o}|o')$.

As shown in the left box of Fig.1, the steps of secure CPGM generation are as follows.

① The virtual account of each collaboration group sends the address of the profile off-chain storage of the collaboration group to the smart contract;
② Smart contracts input the profile address to oracles;
③ The oracle nodes obtain credible user profile data from off-chain through the profile address, generate a verifiable CPGM (containing forwarding function $p_1(u'|o)$ and fuzzy function $p_2(s'|u', o)$) based on the profile, and sends it to smart contracts (see Section 3 for details);
④ Smart contracts upload a digest of the function and send the function to the virtual account.

As shown in the right-hand box of Fig.1, the steps of collaborative LBS query on the blockchain network include.

① When an LBS query is required, u identifies a collaborator u' based on $p_1(u'|o)$, generates a disguised secret s' based on $p_2(s'|u', o)$, and then sends the obfuscated query $o' = \{u', s'\}$ along with $hash(o')$ to u';
② The collaborator u' sends to the LBS in his identity to shield u;
③ The LBS processes the query o' and provides the query result to u'. A suspicious LBS administrator can use $q(\hat{o}|o')$ to infer u's identity and secret;
④ u' sends the results of the LBS feedback back to u.

2.2 Threat models

Consider an extreme environment where the threats are described as follows.

- **Selfishness:** Collaborators do not forward queries to the LBS or do not return query results to save their resources;
- **Data Tampering:** Collaborators may publish tampered or forged queries that tamper with the returned results, resulting in a querier being unable to get correct query services;
- **Distributed Denial of Service (DDoS) Attack:** Malicious nodes send duplicate queries to the LBS to disrupt its service functionality;
- **Reward Repeat Claim Attack:** After completing a task, a malicious collaborator attempts to repeatedly claim the token rewards of the task by continuously creating new identities and accounts;
- **Inference Attack:** An attacker uses statistical or machine learning methods to infer the user identity and secret, $\hat{u}$ and $\hat{s}$, of a querier based on a prior disclosure.

2.3 Design goals

Our scheme should achieve the following design goals:

- **Privacy Protection:** 1) Group members do not need to worry about privacy leakage caused by the protection functions, $p_1(u'|o)$ and $p_2(s'|u', o)$, falling into the hands of third parties. Even if the protection is stolen or the algorithmic logic is in the hands of an attacker, the scheme can still guide the collaborative group to defend itself against external attacks effectively; 2) It is difficult for an attacker to associate the identity of a querier with an LBS request; 3) The real identities of the members of the collaborative group are not visible to the public.

- **Security:** 1) The source and integrity of the off-chain user profile data should be able to be verified; 2) The generation process of CPGMs should be auditable and verifiable; 3) The protection function should be black-boxed, making the outputs difficult to be falsified.
- **Trustworthiness:** 1) On-chain and off-chain data interactions should be trustworthy so that the final generated CPGMs can be trusted and used by users; 2) Abnormalities or irregularities in intra-group collaboration should be traced and punished to build trust.

3 Secure CPGM generation

In this section, we explained CPGM construction and explored how to secure model generation with the assistance of two types of oracles.

3.1 Modeling of collaborative privacy games

Fig. 2 illustrates the collaborative privacy game framework in this work, described in detail below.

3.1.1 Defense and attack mechanisms

The Euclidean space scenario in which users can move to any location was taken into consideration in this study. Users want to protect their secrets through crowd collaboration when communicating with untrusted LBS. As shown in the game framework in Fig. 2, we assume that a collaborative group member $u \in U$ wants to protect his privacy for $s \in S$.To do this, querier u needs to choose a collaborator within the group to help him release the obfuscated query, $o' = \{u', s'\}$, which consists of the following steps.

The choice of the collaborator is affected by the information o of the original enquirer, which is determined by the following probability distribution.

$$p_1(u'|s,u) = p_1(u'|o) = \Pr\{U = u'|O = o\} \tag{1}$$

After identifying a suitable u' by p_1, u transforms his secret s into an observable fuzzified message s' to prevent s from being directly exposed during subsequent transmissions. The output of s' is affected by o and u', which is determined by the following probability distribution.

$$\begin{aligned} p_2(s'|u',s,u) &= p_2(s'|u',o) \\ &= \Pr\{S = s'|U = u', O = o\} \end{aligned} \tag{2}$$

p_1 and p_2 are the pure strategies of exclusively and deterministically outputting observable u' and s' for secrets u and s.

Given the prior data $\pi(o)$, and combining (1) and (2), we have

$$p(o', o) = p(\{u', s'\}, o) = \pi(o)p_1(u'|o)p_2(s'|u', o). \tag{3}$$

Based on (3), the probability of o' under condition o is written as

$$p(o'|o) = \frac{p(o', o)}{\pi(o)} = p_1(u'|o)p_2(s'|u', o). \tag{4}$$

The adversary can be seen as an entity aiming to find the user's secret to minimize the user's privacy by observing the output of the protection mechanism. An attacker can infer the possible privacy set $\hat{o} = \{\hat{u}, \hat{s}\}$ from the observable privacy set $o' = \{u', s'\}$. We define the probability distribution of $\hat{o} = \{\hat{u}, \hat{s}\}$ being the real privacy set $o = \{u, s\}$ as follows.

$$q(\hat{o}|o') = \frac{\pi(\hat{o})p(o'|\hat{o})}{\sum_{\hat{o} \in O} \pi(\hat{o})p(o'|\hat{o})} \tag{5}$$

The goal of $q(\hat{o}|o')$ is to invert obfuscation mechanisms $p_1(u'|o)$ and $p_2(s'|u', o)$ to estimate $\hat{o}$. The inference error determines the effectiveness of the inference algorithm, which is measured by the distortion privacy metric. Note

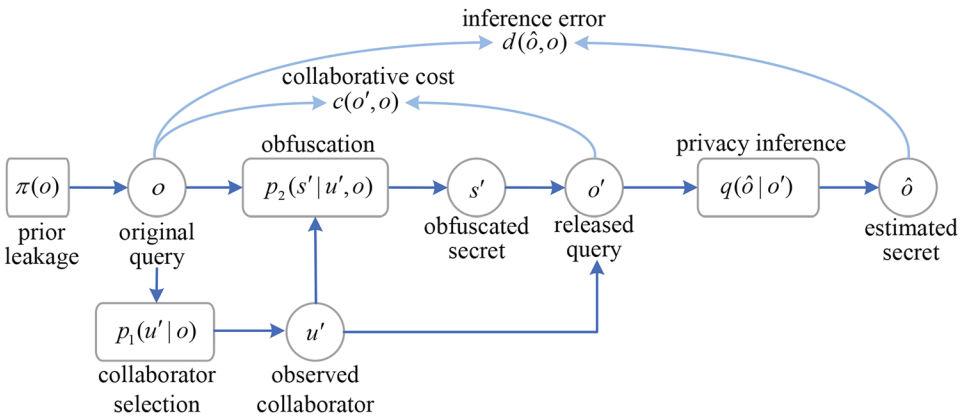


Fig. 2 Collaborative privacy game workflow

that q is not simply an inference of Bayesian probability but a mobile pattern attack against continuous query scenarios, i.e., the attacker can exploit more mobile information with the spatiotemporal correlation of consecutive queries.

For any observation o', we express the actual querier's o as the probability distribution over the possible locations $\hat{o}$.

$$\Pr(\hat{o}|o) = \sum_{o' \in O} p(o'|o) q(\hat{o}|o') \tag{6}$$

3.1.2 Privacy metrics

Given that users may publish queries continuously, there is often a correlation between temporally adjacent queries. The attacker can use this correlation [30, 31] to infer the user's private information from multiple consecutive locations. Privacy inferred from continuous queries is defined as mobility privacy [32]. Suppose that the protection functions releases data ${o_t}'$ at time t and publishes data ${o_{t-n}}'$ at previous n moments, mobility privacy can be calculated as

$$\frac{q(\hat{o}|{o'}_t, {o'}_{t-1}, {o'}_{t-2}, ..., {o'}_{t-n})}{q(\hat{o}|{o'}_t)}. \tag{7}$$

where subscript n represents the number of historical observation locations considered when measuring the risk of privacy leakage. Specifically, the "contextual information" the attacker can refer to is positively related to n.

After the observable o' is released, the attacker gets the estimated value $\hat{o}$ by inference on the original query. The weighted distance is used to quantify the distortion, which reflects the difference between o and $\hat{o}$. Users do not have to worry about their information becoming exposed if a sizeable weighted distance between o and $\hat{o}$ exists.

The privacy gain of the user with secret o is defined as a distance between the two data points: $d(\hat{o}, o)$, where $\hat{o}$ is the a posteriori estimation of the secret. Based on (4), (5) and (6), the expected distortion privacy of the group is calculated as (8) at the top of the next page.

$$\begin{aligned}\sum_{o \in O} \pi(o) \sum_{\hat{o} \in O} \Pr(\hat{o}|o) d(\hat{o}, o) &= \sum_{o \in O} \pi(o) \sum_{o' \in O} p(o'|o) \\ &\quad \sum_{\hat{o} \in O} q(\hat{o}|o') d(\hat{o}, o) \\ &= \sum_{o \in O} \pi(o) \sum_{u' \in U} p_1(u'|o) \\ &\quad \sum_{s' \in S'} p_2(s'|u', o) \\ &\quad \sum_{\hat{o} \in O} q(\hat{o}|o') d(\hat{o}, o)\end{aligned} \tag{8}$$

$$\begin{aligned}\sum_{o \in O} \pi(o) \sum_{\hat{o} \in O} p(o'|o) c(o', o) &= \sum_{o \in O} \pi(o) \\ &\quad \sum_{u' \in U} p_1(u'|o) \sum_{s' \in S'} p_2(s'|u', o) c(o', o)\end{aligned} \tag{9}$$

$$q^* = \arg\min_q \sum_{o \in O} \pi(o) \sum_{u' \in U} p_1(u'|o) \sum_{s' \in S'} p_2(s'|u', o) \sum_{\hat{o} \in O} q(\hat{o}|o') d(\hat{o}, o) \tag{10}$$

It is impossible for the attacker to have all the information about a user. Thus, there is a discrepancy between the inferred user location distribution and that inferred under ideal conditions (with all the information known). The more minor the discrepancy of $d(\hat{o}, o)$, the greater the accuracy.

3.1.3 Optimal game strategy

To enhance location privacy, we use fuzzy technique [33] for the query $o = \{u, s\}$. The computational and communication resources required to perform query fuzzing operations can be abstracted as a cost function $c(o', o)$. Based on the cost function, the collaboration cost can be concretely calculated as (9) at the top of the next page.

The goal of an attacker is to minimize user privacy, that is, to minimize the error between the estimated value $\hat{o}$ and the original content o, where the distortion-privacy measures the error. The attacker's inference is optimal when (8) takes the minimum value. Thus, the optimal inference attack scheme is expressed as (10) at the top of the next page.

From (4) and (5), the attack function is determined by p_1 and p_2. The mobility privacy is guaranteed if p_1 and p_2 satisfies

$$\frac{q(\hat{o}|{o'}_t, {o'}_{t-1}, {o'}_{t-2}, ..., {o'}_{t-n})}{q(\hat{o}|{o'}_t)} \leq \exp(\alpha). \tag{11}$$

Let β be the minimum-desired distortion privacy level. The user's average distortion privacy is guaranteed if the obfuscation mechanisms p_1 and p_2 satisfy (12) at the top of the next page.

$$\sum_{o \in O} \pi(o) \sum_{u' \in U} p_1(u'|o) \sum_{s' \in S'} p_2(s'|u', o) \sum_{\hat{o} \in O} q^*(\hat{o}|o') d(\hat{o}, o) \leq \beta \tag{12}$$

In contrast to the attacker, group collaboration aims to minimize the collaborative cost (9) under privacy constraints (11) and (12), i.e., find probability distribution functions ${p_1}^*$ and ${p_2}^*$ that is defined to minimize the collaborative cost under multiple privacy constraints. Accordingly, the collaborative privacy game problem is formulated as

$$\mathcal{P}1 : \min_{p_1,p_2} \sum_{o\in O} \pi(o) \sum_{u'\in U} p_1(u'|o) \sum_{s'\in S'} p_2(s'|u',o)c(o',o)$$

s.t. (11), (12).

The essence of $\mathcal{P}1$ is to output an optimal pair of p_1 and p_2 from a decision space to minimize collaboration cost under privacy constraints.

3.2 On- and Off-chain interaction

As described in Subsection 3.1, CPGM generation relies on user profiles stored off-chain due to their large size. This motivates us to design an on-chain and off-chain secure interaction scheme to achieve trusted data retrieval and model generation.

Oracle [10] is a programmable computing platform that can be connected to the blockchain through smart contracts, and it can fetch off-chain data by calling APIs interfaces of external systems. Oracle contracts can be performed to verify the authenticity, accuracy, and integrity of acquired data. The verified data is uploaded to the chain by the oracle contract. ChainLink [34] and Witnet [35] are two types of oracle mechanisms. The former can achieve secure off-chain data retrieval, and the latter is good at trusted model generation and verification. They are integrated into the proposed framework to improve privacy protection and distributed trust. Figure 3 shows the implementation details of our designed scheme based on the two oracles.

The virtual account of the collaboration group sends members' off-chain profile addresses to the smart contract. Smart contracts further forward the addresses to ChainLink contracts. ChainLink nodes are triggered to extract user profile data from corresponding sources by calling APIs. After obtaining the profile, ChainLink contracts perform source validation, consistency checking, and data integrity verification. Legal data is sent to WitnetBridge contracts.

With the profiles filtered by ChainLink, WitnetBridge contracts select trusted nodes to generate a CPGM. Given α and β, the Witnet nodes utilize off-chain resources to compute the optimal protection mechanisms, p_1 and p_2, and obtain its corresponding optimal attack q by solving $\mathcal{P}1$ using linear programming solver. During generation, nodes embed tamper-resistant watermarks [36] into the model and upload intermediate data and logs on-chain for full traceability. After generating a CPGM, Witnet nodes submit p_1 and p_2 to WitnetBridge contracts for integrity verification. Upon verification, this contract returns p_1 and p_2 to the requesting smart contract. Smart contracts calculate digests of the protection function parameters and only record the digests on the chain. In contrast, embedded validity period details in the functions are transmitted to the collaborative group's virtual account to avoid long-term abuse.

This way, a dual-verification mechanism with two oracles is constructed to enable on- and off-chain trusted data retrieval and model generation.

4 Incentive mechanisms

As mentioned earlier, a prerequisite for the effectiveness of CMPG is the adherence of group members to the collaboration rules. A reward and punishment mechanism for

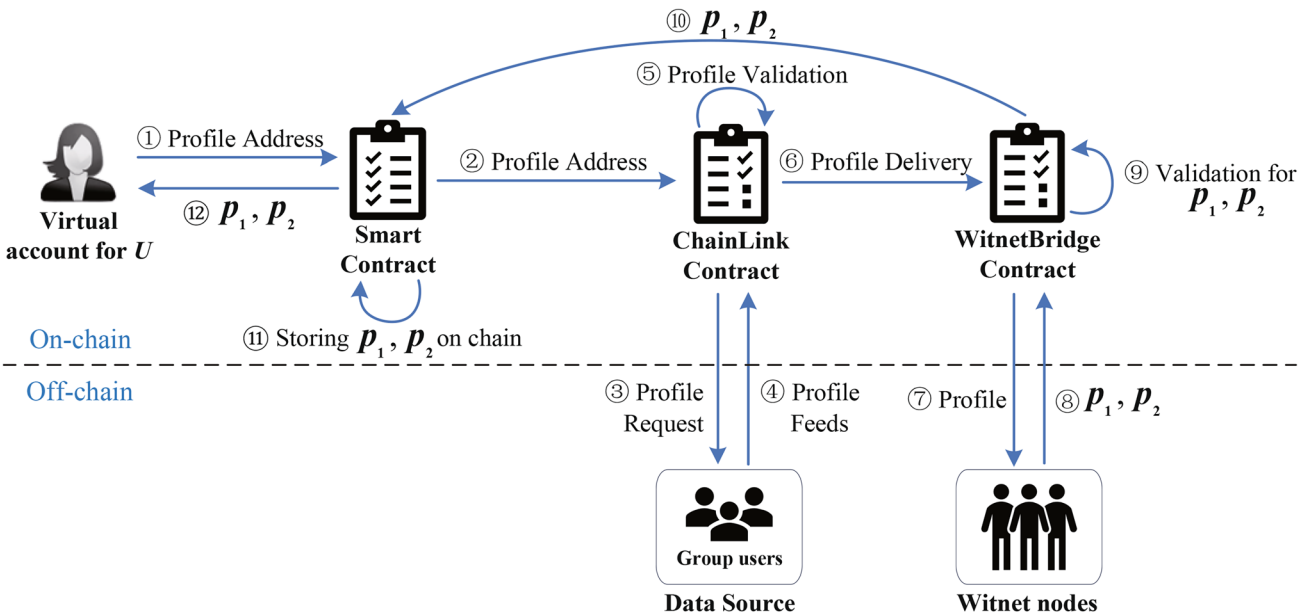


Fig. 3 On- and off-chain interaction

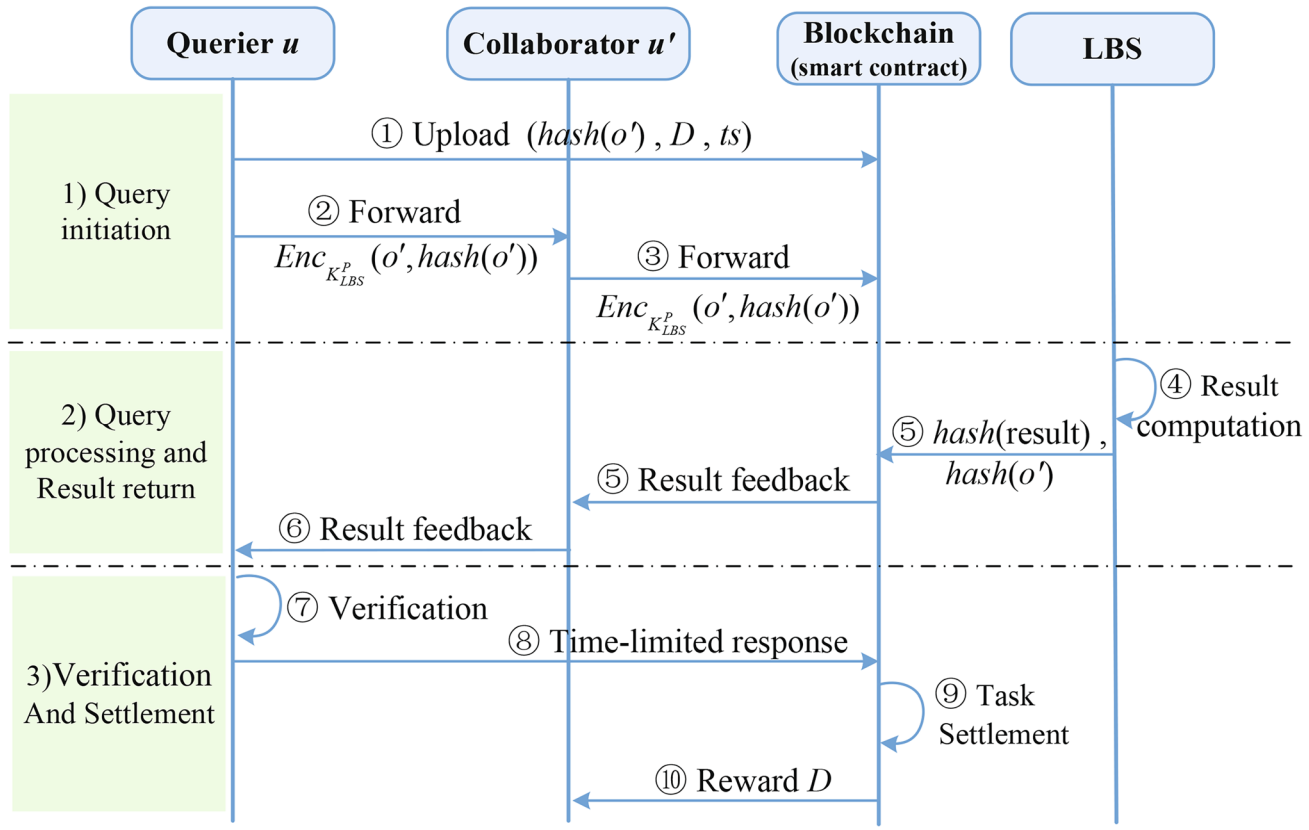


Fig. 4 Intra-group collaboration workflow

collaboration is designed to regulate users' behavior during privacy gaming by integrating token incentives and black-listing mechanisms.

4.1 Token-based reward mechanism

Figure 4 shows the intra-group collaboration, consisting of three phases: query initiation, query processing, result return, and verification and settlement. For the peer-to-peer collaboration, we achieve the verifiability of user behavior and query results by behavioral evidence and incentives, as described below.

1. **Query initiation:** Querier u needs to deposit a certain number of tokens (denoted as D) in the smart contract as a bond, and submit the query hash and timestamp, $hash(o')$ and ts, to the blockchain (see step ①), to prevent duplicate queries and controlling the number of queries. Then u encrypts o' and $hash(o')$ using the public key K^P_{LBS} of the LBS and forwards them together to collaborators u' (see step ②), ensuring query content is not stolen.
2. **Query processing and result return:** The LBS decrypts o' and verifies the uniqueness of it, then relays $hash(result), hash(o')$ back to the blockchain (see steps ④ and ⑤), for later verification. The smart contract incentivizes the LBS by rewarding from u's deposited D, for its correct and proactive evidence provision.
3. **Verification and settlement:** u verifies result completeness by retrieving the on-chain $hash(result)$ (see step ⑦). If complete, u submits confirmation to the contract within a time limit (see step ⑧). The contract then checks the consistency of $hash(o')$ submitted earlier by u and LBS to confirm if u' has legitimately completed the query submission. After confirming u' has legitimately completed query submission and relay, the contract settles the task and pays u's deposited D to u' (see steps ⑨ and ⑩)). The uniqueness of $hash(o')$ also prevents collaborators from duplicate reward claims.

This framework can deter malicious behaviors of querier u. If u does not submit confirmation in time, D is deducted from his deposit to compensate u'. Preset timestamps determine valid queries. Timed-out tasks are auto-settled to avoid delays.

4.2 Blacklisting mechanism

The account information of the offending users is recorded in a public blacklist on the blockchain. Before forming a collaborative group, the smart contract verifies the identity of the users who want to join the group, and the users on the blacklist are prohibited from entering the collaborative group. In this case, users who cannot participate in the collaboration can only join the degraded single-player game, and the privacy protection effect is significantly reduced. Smart contracts verify the behavior evidence submitted by the collaborating parties after completion. Once a violation is found, the user account is immediately blacklisted and temporarily stripped of its right to collaborate. The smart contract sets the corresponding lock time according to the number of violations by the user. During the penalty period, the blacklisted users are not allowed to participate in any collaboration and will not be removed from the blacklist until the punishment period expires. Users who frequently violate collaboration rules may permanently lose collaboration opportunities. At the same time, the proposed token incentive mechanism can be set up to reward long-term compliance users and stimulate their willingness to participate in compliance and collaboration. Due to the ease of access to publicly stored data on the chain, retrieving the blacklist does not incur additional communication and latency burdens.

5 Security analysis

We theoretically analyze whether the proposed solution can achieve the design goals.

- **Enhanced privacy protection via collaboration:** When a user plays a single-user game, his collaborator can be regarded as himself. In this case, forwarding function $p_1(u' \mid o) = 1$, and then $p(o' \mid o)$ and $q(\hat{o} \mid o')$ reach their maximum value, meaning the attacker's inference achieves the optimal value. When collaborative queries are adopted, $p_1(u' \mid o)$ is less than 1. The value of $q(\hat{o} \mid o')$ under a collaborative query is smaller than that under a single-user game, weakening the attacker's inference.
- **Resistance to model leakage:** The game allows attackers and defenders to reach an equilibrium point at which the optimal defense and attack are simultaneously obtained. Even if the protection model or algorithm logic is compromised, users do not have to worry about the failure of the protection policy.
- **Identity non-correlatability:** Since the observed $o' = (u', s')$ is ambiguous and anonymized, it is difficult for an attacker to infer the true identity and secret information of inquirer u based on o'.
- **Identity invisibility:** At the CPGM generation phase, interactions between the collaborative group and smart contracts are executed by virtual accounts, making the real identities of group members untraceable externally.
- **Non-falsifiability:** 1) A tamper-resistant watermark is embedded in the protection functions. Smart contracts can verify the watermark to detect if the functions are altered; 2) A querier has no reason to forge his obfuscated location and cannot accurately predict p_2.
- **Resistance to DDoS attack:** Each initiated query corresponds to a query hash, which is non-collisional. Smart contracts can determine whether a query has been processed before based on the hash of each query, thus preventing DDoS attacks.
- **Resistance to reward repeat claim:** When settling the query tasks, smart contracts label each task ID as "Settle". When a user repeatedly claims rewards, smart contracts reject those requests according to task status.
- **Traceability:** Oracle contracts can trace and verify the user profile's source and CPGM generation, while smart contracts check and track key results and evidence retained on-chain.

6 Performance evaluation

In this section, we simulated multi-user game scenarios by generating random user datasets on a Beijing map containing various POIs to study the privacy preservation effectiveness of the proposed method under different geographical environments. The attacker inferred users' precise locations based on the maximum mobility speed limit and anonymous locations in consecutive queries. We developed a smartphone trajectory tracking software to collect mobile user trajectories for experiments to evaluate feasibility in real-world environments. The simulation experiments focused on performance metrics, including privacy level and collaboration cost. All models were implemented in Matlab and Python.

6.1 Single- vs. multi-user game

The proposed CPGM was classified into CPGM-1 and CPGM-2. The former considered both mobile privacy constraint (11) and distorted privacy constraint (12), while the latter omitted mobile privacy. The benchmark methods were two single-user privacy game schemes, SUPG-1 and SUPG-2, improved by [5, 37]. Similar to CPGM-1 and CPGM-2, the difference was that SUPG-2 ignored mobility privacy. The single-user game means a user can only use the obfuscation mechanism to interfere with the attacker's observation without the cover of a group. Compared with the single-user privacy game, the advantage of the multi-user collaborative

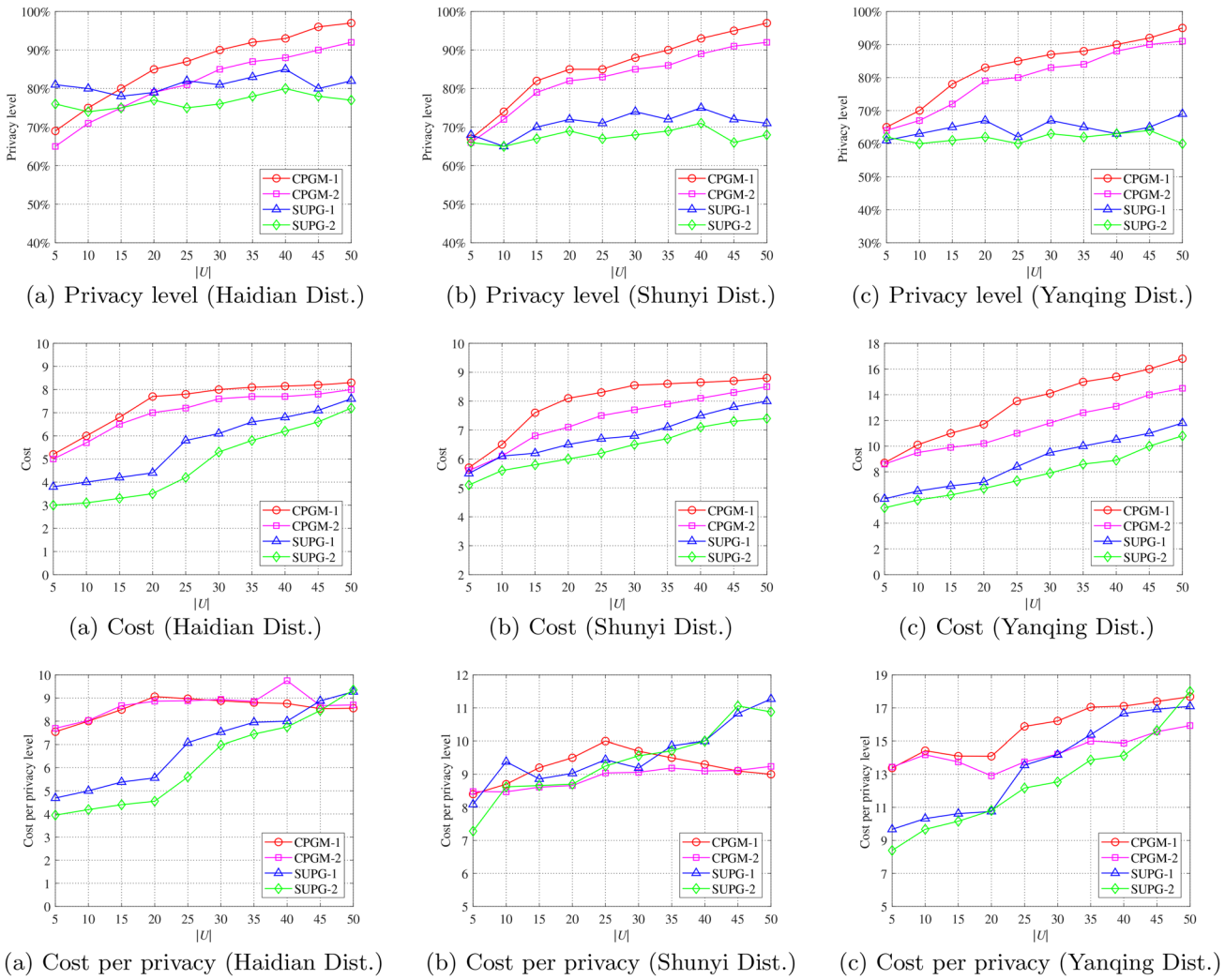


Fig. 5 Impact of urban areas and group size on CPGM

game is that the individual's behavior is hidden in the group, which reduces the risk of exposing identity privacy and query privacy.

Figure 5 gives the comparison when $\alpha = 0.1$ km, $\beta = 0.4$. Although the time consumption of the group-based game was higher, the level of expected privacy was significantly higher. The level of privacy protection positively correlates with the group size. The proposed multi-user game model takes advantage of user correlation, which can hide the identity of users and reduce the risk of exposing their privacy. In contrast, privacy protection will be weakened when the multi-user game model degenerates into a single-user game. In a single-user game, the user alone faces potentially malicious entities. Due to the lack of cover from other users, a user's privacy is more likely to be inferred and obtained by malicious entities, with a higher risk of privacy exposure. In particular, for a collaborative group of 20 people, the privacy level obtained through the group game has shown a clear increasing trend, the privacy level can reach 85%, while the cost increases slowly, showing good performance; however, as the group size increased, the privacy level flattened out while the time consumption increased rapidly. While larger group sizes are theoretically conducive to better camouflage, this result suggests that simply increasing group size is not a good option. The best trade-off between privacy protection and execution efficiency is achieved when the group size reaches 20 people. Further reductions in completion time can be achieved with efficient computational techniques.

6.2 Impact of POI density

We examined the impact of POI density on privacy protection. Twenty users were set to experience LBS in three

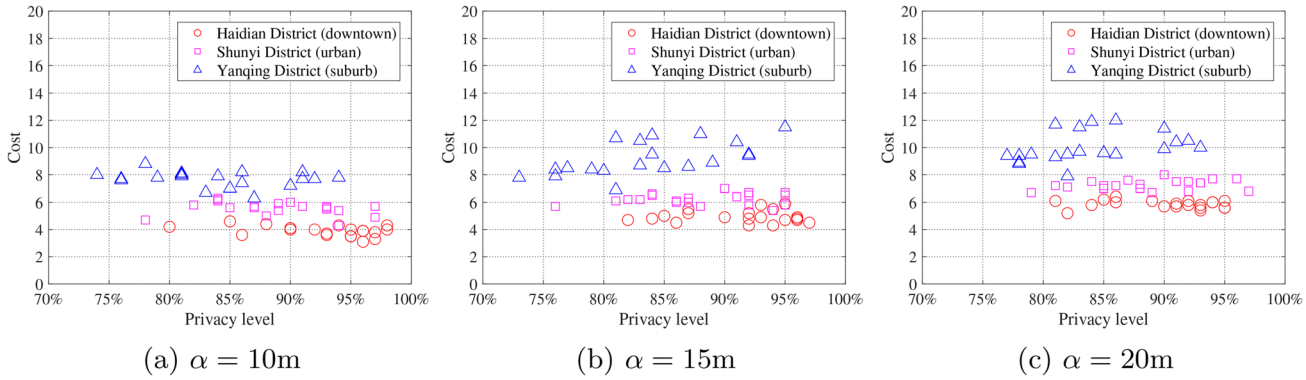


Fig. 6 Impact of average distance among users on CPGM

Beijing areas with different POI densities, where the city center Haidian had the highest density and suburban Yanqing the lowest.

Figure 6 provides the level of privacy protection for CPGM-1 in the three regions and the corresponding cost of collaboration. Users in the Haidian district can achieve a higher level of privacy at a lower cost. However, there is a higher cost of cooperation to achieve the same level of privacy in the Yanqing District. CPGM-1 achieves satisfactory privacy protection in areas with high POI density, and even in suburban areas, it still protects at least 74% of privacy. The difference between the three sub-figures in Fig. 6 shows that as the average distance between users increases, the collaboration cost consumed by CPGM-1 to achieve the same level of privacy protection increases, but the overall fluctuation range is insignificant. In general, CPGM can help users better hide in areas with high POI density and dense membership and achieve higher privacy protection with low collaboration costs.

We developed a software tool to collect real trajectory data from 50 mobile devices instead of simulated data. Under the settings of $\alpha = 0.1$km and $\beta = 0.4$, Fig. 7 shows the game cost increase accompanying elevated privacy levels under different mechanisms in different regions. Results intuitively demonstrated that incorporating mobility privacy helped defend against mobility pattern attacks, especially in consecutive query scenarios. CPGM-1 played a very positive role in satisfying at least 80% of users' privacy needs. By introducing mobility privacy metrics, CPGM-1 improved the average privacy level by about 7%. One device in Haidian reached a 98% privacy level, indicating CPGM could provide better protection in areas with high POI density. For SUPG, the combination of mobility privacy can also improve protection. SUPG-1 increases the average privacy level by about 10% compared to SUPG-2. Although introducing mobility privacy into a single-user privacy game can improve protection, its privacy protection level is not as good as CPGM. In Yanqing District, the privacy protection level of devices deployed with CPGM-1 is 20% higher than those deployed with SUPG-1.

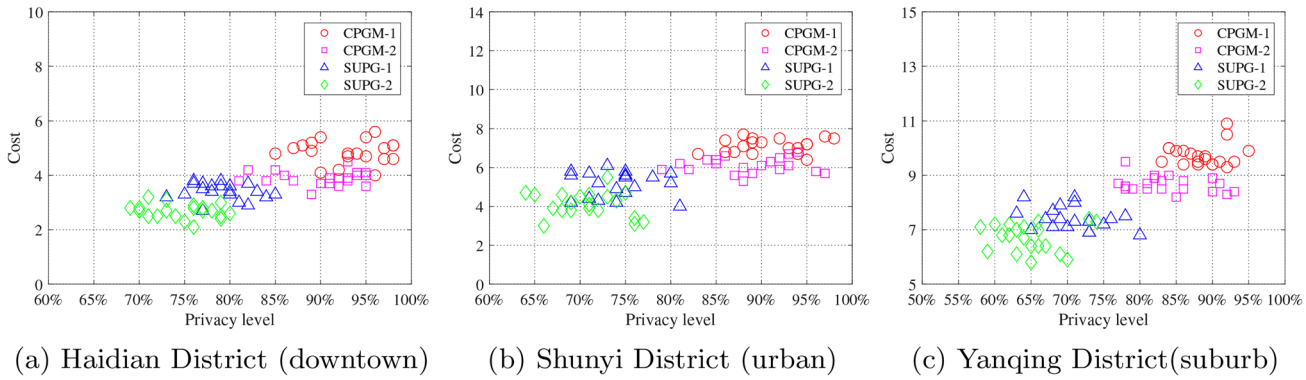


Fig. 7 Impact of POI density in urban areas on CPGM

7 Conclusion

A blockchain-enabled peer-to-peer collaborative framework is proposed to enable users to achieve their privacy protection in extreme environments and to allow the collaboration of groups that initially lacked trust to collaborate efficiently. A multi-user collaborative privacy game model is constructed for privacy inference attacks, and the oracle mechanism guarantees security. To ensure privacy games' safety and effectiveness, a blockchain-based token incentive and blacklisting mechanism are designed to achieve the verifiability and traceability of user behaviors. The evaluation results show that the designed privacy game can meet the privacy requirements at an acceptable cost, and the effect is better in the densely distributed POI areas. Follow-up work will study the construction of an architecture that integrates interplanetary file systems and blockchain to support large-scale mobile user scenarios.

Acknowledgements The authors gratefully acknowledge the financial assistance provided by the National Natural Science Foundation of China and the Natural Science Foundation of Jiangsu Province.

Author contributions Beining Zhang and Hang Shen wrote the main manuscript text. Tianjing Wang and Guangwei Bai provided guiding ideas and suggestions. All authors reviewed the manuscript.

Funding This work was supported in part by the National Natural Science Foundation of China under Grants 61502230 and 61501224, the Natural Science Foundation of Jiangsu Province under Grant BK20201357, and the Six Talent Peaks Project in Jiangsu Province under Grant RJFW-020.

Availibility of supportig data Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declarations

Ethical approval and consent to participate This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication All authors agree to publish the paper and related research results of the paper.

Competing interests We declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. We declare that there is no financial interest/personal relationship which may be considered as potential competing interests.

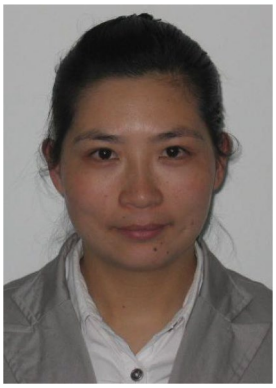
References

1. Jiang H, Li J, Zhao P, Zeng F, Xiao Z, Iyengar A (2021) Location privacy-preserving mechanisms in location-based services: A comprehensive survey. ACM Comput Surv 54(1)
2. Pawlick J, Colbert E, Zhu Q (2020) A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. ACM Comput Surv 52(4)
3. Do CT, Tran NH, Hong C, Kamhoua CA, Kwiat KA, Blasch E, Ren S, Pissinou N, Iyengar SS (2018) Game theory for cyber security and privacy. ACM Comput Surv 50(2)
4. Hong S, Duan L, Huang J (2022) Protecting location privacy by multiquery: A dynamic bayesian game theoretic approach. IEEE Trans Inf Forensics Secur 17:2569–2584
5. Shokri R, Theodorakopoulos G, Troncoso C (2016) Privacy games along location traces: A game-theoretic framework for optimizing location privacy. ACM Trans Priv Secur 19(4):1–31
6. Xue L, Liu D, Huang C, Shen X, Zhuang W, Sun R, Ying B (2022) Blockchain-based data sharing with key update for future networks. IEEE J Sel Areas Commun 40(12):3437–3451
7. Jiang H, Wang M, Zhao P, Xiao Z, Dustdar S (2021) A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs. IEEE/ACM Trans Netw 29(5):2228–2241
8. Backes M, Humbert M, Pang J, Zhang Y (2017) Walk2Friends: Inferring social links from mobility profiles. In Proc ACM SIGSAC CCS 1943–1957
9. Eyal I, Gencer AE, Sirer EG, Van Renesse R (2016) Bitcoin-ng: A scalable blockchain protocol. In Proc. of USENIX NSDI, pages 45–59
10. Pasdar A, Lee YC, Dong Z (2023) Connect api with blockchain: A survey on blockchain oracle implementation. ACM Comput Surv 55(10):1–39
11. Shokri R, Theodorakopoulos G, Papadimitratos P, Kazemi E, Hubaux J-P (2013) Hiding in the mobile crowd: Location privacy through collaboration. IEEE Trans Depend Sec Comput 11(3):266–279
12. Peng T, Liu Q, Meng D, Wang G (2017) Collaborative trajectory privacy preserving scheme in location-based services. Inf. Sci. 387:165–179
13. Niu B, Zhu X, Li W, Li H (2014) Epcloak: An efficient and privacy-preserving spatial cloaking scheme for LBSs. In IEEE MASS pp. 398–406
14. Chow C-Y, Mokbel MF, Liu X (2006) A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In Proc ACM SIGSPATIAL GIS, pp. 171–178
15. Niu B, Zhu X, Li Q, Chen J, Li H (2015) A novel attack to spatial cloaking schemes in location-based services. Future Gener. Comput. Syst. 49:125–132
16. Ghaffari M, Ghadiri N, Manshaei MH, Lahijani MS (2017) P^4QS: A peer-to-peer privacy preserving query service for location-based mobile applications. IEEE Trans Veh Technol 66(10):9458–9469
17. Jin H, Papadimitratos P (2019) Resilient privacy protection for location-based services through decentralization. ACM Trans Priv Secur 22(4)
18. Shokri R, Theodorakopoulos G, Troncoso C, Hubaux J-P, Le Boudec J-Y (2012) Protecting location privacy: Optimal strategy against localization attacks. In Proc ACM SIGSAC CCS, pp. 617–627
19. Shen H, Bai G, Yang M, Wang Z (2017) Protecting trajectory privacy: A user-centric analysis. J Netw Comput Appl 82:128–139
20. Shokri R (2015) Privacy games: Optimal user-centric data obfuscation. Proc Priv Enh Technol 2015(2):299–315
21. Ding K, Zhang J (2020) Multi-party privacy conflict management in online social networks: A network game perspective. IEEE/ACM Trans Netw 28(6):2685–2698
22. Hong S, Duan L (2022) Multi-user privacy cooperation game by leveraging users service flexibility. In IEEE Int Symp Info Theory pp. 637–642
23. Li B, Liang R, Zhu D, Chen W, Lin Q (2020) Blockchain-based trust management model for location privacy preserving in vanet. IEEE Trans Intell Transp Syst 22(6):3765–3775
24. Feng J, Wang Y, Wang J, Ren F (2020) Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular networks. IEEE Internet Things J 8(4):2087–2101

25. Li B, Liang R, Zhou W, Yin H, Gao H, Cai K (2021) LBS meets blockchain: an efficient method with security preserving trust in sagin. IEEE Internet Things J 9(8):5932–5942
26. Chaudhary B, Singh K (2021) A blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. Peer-to-Peer Netw Appl 14:3198–3212
27. Li H, Pei L, Liao D, Sun G, Du X (2019) Blockchain meets vanet: An architecture for identity and location privacy protection in vanet. Peer-to-Peer Netw Appl 12:1178–1193
28. Huang C, Wang W, Liu D, Rongxing L, Shen X (2022) Blockchain-assisted personalized car insurance with privacy preservation and fraud resistance. IEEE Trans Veh Technol 72(3):3777–3792
29. Xue L, Ni J, Liu D, Lin X, Shen X (2023) Blockchain-based fair and fine-grained data trading with privacy preservation. IEEE Trans Comput
30. Niu B, Chen Y, Wang Z, Li F, Wang B, Li H (2022) Eclipse: Preserving differential location privacy against long-term observation attacks. IEEE Trans Mobile Comput 21(1):125–138
31. Jiang H, Zhao P, Wang C (2018) RobLoP: Towards robust privacy preserving against location dependent attacks in continuous LBS queries. IEEE/ACM Trans Netw 26(2):1018–1032
32. Zhao Y, Chen J (2024) Vector-indistinguishability: Location dependency based privacy protection for successive location data. IEEE Trans Comput 73(4):970–979
33. Benarous L, Kadri B (2022) Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles. Peer-to-Peer Netw Appl 15(1):461–472
34. Breidenbach L, Cachin C, Chan B, Coventry A, Ellis S, Juels A, Koushanfar F, Miller A, Magauran B, Moroz D et al (2021) Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. Chainlink Labs 1:1–136
35. De Pedro AS, Levi D, Cuende LI (2017) Witnet: A decentralized oracle network protocol. arXiv preprint arXiv:1711.09756
36. Bhalerao S, Ansari IA, Kumar A (2021) A secure image watermarking for tamper detection and localization. J Ambient Intell Humaniz Comput 12(1):1057–1068
37. Shen H, Bai G, Yujia H, Wang T (2019) P2TA: Privacy-preserving task allocation for edge computing enhanced mobile crowdsensing. J Syst Archit 97:130–141

Beining Zhang received the BS degree in Xi'an University of Posts and Telecommunications, Xi'an, China. She is currently an MS student at the Department of Computer Science and Technology, Nanjing Tech University, Nanjing, China. Her research interests include blockchain-based privacy preservation in location-based services.

Hang Shen is currently an Associate Professor with the Department of Computer Science and Technology, Nanjing Tech University, Nanjing, China. He received the Ph.D. degree (with honors) in Computer Science from the Nanjing University of Science and Technology. He worked as a Full-Time Postdoctoral Fellow with the Broadband Communications Research (BBCR) Lab, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2018 to 2019. His research interests involve space-air-ground integrated vehicular networks, network security, and privacy computing. He serves as an Associate Editor for the IEEE Access and *Journal of Information Processing Systems*.



Tianjing Wang holds a BSc. (2000) in Mathematics at the Nanjing Normal University, an MSc. in Mathematics at the Nanjing University in 2005, and a Ph.D. in Signal and Information Processing at the Nanjing University of Posts and Telecommunications in 2009. From 2011 to 2013, she was a postdoctoral fellow with the School of Electronic Science and Engineering, Nanjing University of Posts and Telecommunications. From 2013 to 2014, she was a visiting scholar with the Department of Electrical and Computer Engineering, State University of New York at Stony Brook. She is now an Associate Professor with the Department of Computer Science and Technology at Nanjing Tech University. Her research interests include integrated sensing and communications for V2X, and artificial intelligence and machine learning for future networking.

Guangwei Bai received the B.Eng. and M.Eng. degrees in computer engineering from Xi'an Jiaotong University, Xi'an, China, in 1983 and 1986, respectively, and the Ph.D. degree in Computer Science from the University of Hamburg, Hamburg, Germany, in 1999. From 1999 to 2001, he worked at the German National Research Center for Information Technology, Germany, as a Research Scientist. In 2001, he joined the University of Calgary, Calgary, AB, Canada, as a Research Associate. Since 2005, he has been working at Nanjing Tech University, Nanjing, China, as a Professor in Computer Science. From October to December 2010, he was a Visiting Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research interests include architecture and protocol design for communication networks, multimedia networking, network security, and location-based services. He is a member of the ACM and a Distinguished Member of CCF.