IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON PRIVACY PRESERVATION FOR LARGE-SCALE USER DATA IN SOCIAL NETWORKS

Received December 19, 2017, accepted January 24, 2018, date of current version March 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2805464

Cognitive Approach for Location Privacy Protection

MENG HAN[1], (Member, IEEE), LEI LI[1], YING XIE[1], JINBAO WANG[2], ZHUOJUN DUAN[3], JI LI[3], AND MINGYUAN YAN[4], (Member, IEEE)

[1]Department of Information Technology, Kennesaw State University, Marietta, GA 30060, USA
[2]Academy of Fundamental and Interdisciplinary Sciences, Harbin Institute of Technology, Harbin 150000, China
[3]Department of Computer Science, Georgia State University, Atlanta, GA 30303, USA
[4]Computer Science and Information Systems, University of North Georgia, Dahlonega, GA 30533, USA

Corresponding author: Meng Han (mhan9@kennesaw.edu)

ABSTRACT While enjoying the convenience of location-based services (LBSs) in everyday life, wireless device users could also put their location privacy at risk. An untrusted LBS provider can store mobile users' data on its server, track users in various ways or share users location data to the third parties. To protect LBS users' privacy, many position confusion algorithms were proposed, but those algorithms often have difficulty balancing the utility-privacy tradeoffs. In this paper, we propose a new cognitive approach that enables near-complete privacy protection for LBS users by leveraging existing social network resources. We introduce a heterogeneous multi-server architecture that cuts off the direct connection between the LBS queries and the query issuers, and an auction-based incentive mechanism guaranteed user participation, which is critical for the success of the proposed architecture. A simulation system and a smartphone application were developed, and our evaluation results show that the proposed method can not only achieve the near-total privacy protection for LBS users, but also significantly improve the quality of the services.

INDEX TERMS Privacy, location, data, social, mobile.

I. INTRODUCTION

Nowadays, smart mobile devices (such as smart phones, tablets, wearable smart devices) play an important role in our life. Technology advances and fast development in smart devices enrich our daily life in various aspects. A lot of convenience has been brought by smart mobile devices and the rich applications available on smart mobile devices. Among which, one of the most important and popular services that being extensively explored are the services obtained from location based applications. We can find a large number of location based applications that can simply collect users' location information through the embedded GPS module on smart mobile devices. Because of that, users can use map applications to report or obtain road condition such as traffic and accident by a simple click. Based on the participation of a large group of users, road condition can be analyzed and the best route or alternative good routes will be recommended to users. Another example, it is pretty common to see that public transportation vehicles equipped with smart devices, which allow them to report their accurate location. Based on the report, a more accurate arriving time can be computed so that users can better schedule their trip. With the help of LBS, we can also get good recommendations on food, entertainment, hotels and so on. A report from MarketsandMarkets[1] shows that the market of location-based service is going to reach $54.95 billion by 2020. However, like every coin has two sides [1]. The benefits and convenience brought by LBS comes with a risk that users' private information which may include current and historical locations can no longer be preserved [2]–[5]. For example, based on a user's regular report of road condition, it is easy to figure out sensitive location information (such as home address, office address, and regular route) of a commuter. Such information could be compromised when a user submit a query with sensitive information to a LSB server. Privacy leakage may also happen when a LSB server contains sensitive information get hacked. The dilemma is: the more location data we share, the better service we may get from LBS. On the one hand, the more location data users share, the better service they may get from LBS. On the other hand, the more location data collected from users and the broader that those data being used, the higher possibility users

[1]http://www.marketsandmarkets.com/

privacy could get compromised. How to balance the expectation of obtaining better service from a LBS and achieving lower chance of privacy leakage attracts extensive interest recently [6]–[8].

During the past several years, many studies [9]–[11] focused on addressing how to protect privacy in LBS. One popular strategy is to employ well-known privacy metrics such as k-anonymity and differential privacy [12]–[14]. In k-anonymity, users send their queries to a trusted third-party server, after that, a centralized location anonymizer (most of time is the LBS server itself) is required to coordinate all the queries [15]–[18]. It protects location privacy from the LBS server by hiding user's location to other $k-1$ dummy locations. The differential privacy requires that the difference between the probabilities that two answers from a query on value v to a data base D_1 and that probability obtained from the adjacent data base D_2 should be within a bound e^{ϵ}. The effectiveness of those strategies highly relies on the trustiness of the LBS server. Overall, most of the up-to-date proposed technology could only provide privacy protection with a certain probability [19], [20]. If the adversary integrates and utilizes some side information, and digs into data correlation, certain privacy protection could be easily broken [21]–[23]. That is, if a LBS server got compromised, the adversary party has the chance to distinguish the real location from the $k-1$ dummy locations based on rich side information that kept at the server end.

The other challenges that we are facing on protecting sensitive location information in LBS applications include: 1) The risk of losing privacy is due to users' expectation for obtaining better services. In order to get a better service such as obtain accurate and good recommendations for the nearest restaurants, hotels, or shopping centers, you have to share your accurate location information with the server. To improve the query result, such as get a recommendation based on personal preferences, it is usually necessary to share more side information with the server. 2) The traditional privacy protection techniques can not totally hide the real location. Such as the technique which employs dummy locations or fake locations, the real location and the real query issuer have to be included in the queries so that the LBS server can observe enough information so that provide service. In this situation, it could be not difficult for the adversary to crack the protection with the help of side information. 3) The algorithms proposed in existing research articles often have high complexity which is either impractical or costly. Even though they may prove the effectiveness of the proposed solution on privacy protection theoretically. The frustration is that it is very difficult to apply their method to real life applications which hard to satisfy all required pre-defined assumptions.

In this work, we investigate how to balance the efficiency of the query and the privacy concern of the users in a more effective way. To be specific, the target is to develop a simple effective solution with low complexity. With all above mentioned concerns, a social based cognitive approach to achieve a near-complete privacy protection strategy is proposed. Different from existing approaches, the proposed solution aims at separating the LBS query issuer from the query itself. That is, the accurate query issuer's information will not be included in the query that sent to the LBS server. We try to take advantage of the extensively used existing social media to help the submission of LBS queries. A user will no longer directly send a query to the LBS server or third party. Instead, he/she will seek for help from his/her social friends to ask them to send the query to the LBS server. The query result will be returned to the social friends and then passed to the user through a trusted third-party (social networks). For a new product, you may doubt that establish a communication channel independently for a LBS application (app) is also a challenge. This concern can be easily resolved when existing popular social media, such as Facebook, Google+, etc. can be used. Popular social media (such as Google, Twitter, and Facebook, etc.) all capable of providing login interfaces to support user's login to a new app without extra required registered new account. Through existing accounts, the app could also access more authorized information to do more activities. A success example is the AR mobile game *Pokémon GO*,[2] which achieved more than 9.55 million total daily U.S. users after one month since its release. The convenience and trusted login system of Google contributes to this achievement.

Benefiting from the existing popular social media and APIs, we propose to employ the existing social media and account system to establish an independent communication channel for our LBS application in this paper. The idea is to let their social friends to help users submit the LBS query and receive the response. Since the query is not issued directly from the query issuer but from friends of that issuer, it breaks the connection among the queries, side information and the issuer identity. Furthermore, in order to handle the situation that the adversary might collect historical data and social information through the system as well, a practical differential privacy mechanism is proposed. This strategy guarantees that our approach could still limit the chance of privacy loss extremely low even when the social media release several information regarding the query issuer and her helps. It is hard to ensure the number of active friends of a query issues on the social media system is always greater than $k-1$. The k-anonymity privacy objective can not be reached in this case. As a compromise, we try to recruit strangers on the social media system to help. The major technical contributions of this paper are as follows.

- We propose a novel architecture for the location-based service to protect query issuers' privacy (such as locations and identities) against adversary. The major property of this architecture is to distribute the location based query and the query issuer to different servers.
- A differential privacy mechanism is proposed to handle the situation that if the LBS server knows can obtain the query issuer's history activities or social connections.

[2]http://pokemongo.nianticlabs.com/en/

The differential privacy mechanism could guarantee a quite good privacy level in case of side information leakage.
- To stimulate more user on social media system to participate in helping others to perform queries. A game-theory-based auction model followed by an incentive mechanism are proposed, which includes fair query task assignments and price calculation.
- The performance of the proposed methods are evaluated through comprehensive experiments. Besides that, a practical Android App is implemented to demonstrate the usage and effectiveness of our proposed architecture and mechanism.

The rest of the paper is organized as follows. The related work is summarized in Section II. Section III introduces preliminaries, including basic concepts, adversary model, motivation and the basic idea of our resolution. The detailed novel architecture and the implementation foundation are discussed in Section IV. Section VI demonstrates the evaluation results and introduces the Android App implementation. We discuss the conclusion in Section VII.

II. RELATED WORK

The investigation on privacy protection of location-based services is crucial to many related data privacy problems regarding data mining and analyzing in mobile social networks [24]–[26]. There existing literature can be classified into two categories. One category mainly focuses on the metrics of location privacy. It tries to evaluate how accurate an adversary could infer users' coordinate based on the collected data and side information. The other category interests in the investigation of location privacy protection, among which, two popular strategies are k-anonymity and differential privacy based privacy protection. In this section, we first discuss the exiting research work in-depth, and then extend the discussion to how our work contribute to the field.

A. LOCATION PRIVACY METRICS

To evaluate the effectiveness of a protection mechanism, it is very important for the researchers to get a clear idea that how accurate an adversary might infer the location based on collected information and side information. For this purpose, several location privacy metrics have been proposed. Most of the existing literatures are probability-based., They use a probability (between 0 to 1) to indicate the chance that privacy information may be compromised citeChow-1164, where the probability also reflects the privacy level [27]–[29]. To measure the adversary's ability on differentiating a real query issuer from other anonymity set, [30] proposed a very classical metrics. For example, the size of the anonymity set k is a straightforward parameter that can be used to evaluate the privacy level. On the other side, by incorporating social users' spatiotemporal data and semantic information, Yin *et al.* [31] proposed a community discovery approach [32].

B. LOCATION PRIVACY PROTECTION MECHANISM

1) k-ANONYMITY

Gruteser et al. introduced the k-anonymity into location privacy in the earlier days, which protected location privacy from the LBS server by hiding user's location to other $k-1$ dummy locations [30]. Then, [15] was proposed which allowed users to adjust the anonymity level in their protection model. To achieve [11] k-anonymity in privacy-aware LBS, Niu, Li, et al. proposed a method which choose dummy locations based on the entropy metric, and tried to enlarge the cloaking region while keeping a well privacy level [33].,

C. LOCATION PRIVACY PROTECTION MECHANISM

Unfortunately, most of these k-anonymity models are relying on a location anonymizer to enlarge the queried location into a more noised room, and the anonymizer becomes the bottleneck of the performance. Different from k-anonymity, which applied dummy locations and hide the real location in many candidates, our work use the social media being the bridge between the query processing and query issuer. The real query issuer will not communicate to the LBS server.

1) DIFFERENTIAL PRIVACY

In research area of statistical database, differential privacy is a classical notion [12]. Differential privacy limited the modification of a single query issuers data [7], [34], so that have a negligible effect on the query result. Specifically, differential privacy requires that the difference between the probabilities that two answers from a query on value v to a data base D_1 and that probability obtained from the adjacent data base D_2 should be within a bound e^{ϵ}. Reference [35] applied differential privacy to location privacy. The authors proposed a synthetic data generation techniques to publish statistical information related to commuting patterns. While a quadtree spatial decomposition technique proposed by [36] tried to ensure the differential privacy with location pattern mining capabilities. Reference [37] presented a protocol of interactions between the service and query issuers that has remarkable optimality properties. That is, no inference algorithm can be successfully used to infer a query issuers private attribute with a probability better than random guessing. No other privacy-preserving protocol improves rating prediction. It involves a minimal disclosure. However, only relying on the differential privacy cannot completely handle the adversarys referring by exhausted query since differential privacy only protects the data with a specific threshold probability [38], [39].

2) INCENTIVE MECHANISM

Auction model is a popular tool to make the task assignment and payment calculation in incentive mechanism design. Yang *et al.* [40] proposed two types of incentive mechanisms: platform-centric incentive mechanisms and user-centric incentive mechanisms. The platform-centric incentive mechanism is based on the Stackelberg game where the MCS

platform decides the budget as well as control the auction process and users can only adjust their strategies to maximize their utilizes [28], [41]. In user-centric incentive mechanism, each query issuer reports the lowest price for selling a service to the MCS platform. Duan *et al.* [43] designed a reward-based collaboration mechanism, in which the reward of a client is shared among collaborators. If there are enough query issuers' participating, the collaboration is successful. To attract query issuers' participating, [43] proposed a novel Reverse Auction-based Dynamic Price (RADP) incentive mechanism, in which query issuers can sell their sensing data to a service provider according the claimed cost. Singla and Krause [44] deigned a budget feasible auction.

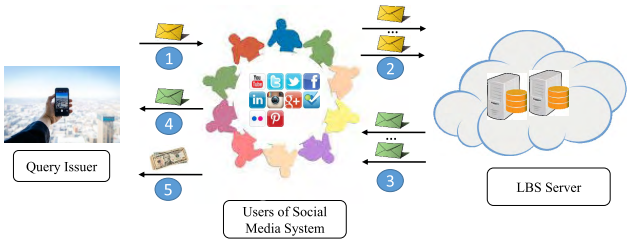


FIGURE 1. System model of our work.

Different from existing method, we take full advantage of existing social networks. The proposed approach could further protect the location and identity of the query issuer. Unlike the existing approaches, we take a lead in proposing the methodology and application to the best of our knowledge. Such methodology and application able to separate the utility and privacy, achieving a cognitive optimal resolution by employing the social network associated with a LBS. The system model of our work is illustrated in Figure 1, which proceeds in five steps:

- **Step 1:** The query issuer request the services through their social channel to their friends.
- **Step 2:** Social partners (the freinds who get the request) will send the query directly to the location service provide with their ID and the original query issuer's location.
- **Step 3:** The corresponding answer to the query return to multiple social partners.
- **Step 4:** The original query issuer get feedback from her/is social partners through the social channel.
- **Step 5:** According to all the data collected, the query issuer caculate the final location-based query's answer.

Table 1 lists frequently used notations.

III. PRELIMINARIES

In this section, the adversary model, background concepts, motivation, and basic idea of our approach are presented.

A. ADVERSARY MODEL

We assume that an adversary is targeting at obtaining sensitive information about a particular query issuer.

TABLE 1. Table of notations.

Notation	Description
k	parameter for privacy level
p_i	probability of a query to location i
S	uncertainty of identifying an individual location
D	database
$q(.)$	query function
Γ	set of users in social media system
Π,	set of queries
γ_j	query issuer i
π_i	task i
γ_j	user j
S_j, c_j	subset of tasks of γ_j, cost
x_{ij}	indicator of task assignment
p_j	received payment of γ_j

The adversary may be a general adversary or a positive adversary. If the adversary is a general adversary, he/she will try to obtain the query issuer's sensitive information through monitoring and eavesdroping on the communication channel between the LBS server and the query issuer. On the other hand, if the adversary is a positive adversary, he/she would not only monitor but also try to compromise the privacy based on collecting enough side information. Generally speaking, the positive adversary is more dangerous than general adversary. Because positive adversary usually collects a lot historical information and side information of all queries, which results in a potential to crack more sensitive information related to the query issuers in a LBS. In this work, we consider the privacy protection under both adversary models.

B. BASIC CONCEPTS

Based on the conclusion obtained in existing literature, we find out that: to evaluate the level of privacy, the measure of anonymity could be one of the straightforward ways. However, to measure the uncertainty, entropy is a more useful metric. Thus, entropy is chosen in this work to measure the anonymity which could be considered as the uncertainty of the probability on determining the real location from all candidate locations [17]. Assume each possible location of the query issuer has a probability denoted by p_i of being queried historically. Because the query issuer is the target user for the adversary, the probability that it will get monitored is 1. Thus, the summation of all probabilities p_i is equals to 1. The entropy S is defined as

$$S = -\sum_{i=1}^{k} p_i \cdot \log_2 p_i \tag{1}$$

where S represents the uncertainty for the adversary to identify the query issuer's accurate location from all the candidate locations. Equation 1 shows that, the larger the uncertainty, the better we can protect our privacy. Therefore, our target is to find out a solution that can maximize the entropy, which also represent the hardness for the adversary to refer our privacy.

C. MOTIVATION AND BASIC IDEA

Existing privacy protection mechanisms are all based on the idea that hides sensitive information among noisy data to make it is difficult for the adversary to identify the real sensitive information. However, since the real information is still included, the connection between a query issuer and the query itself is still exposed to the adversary no matter how good the protection mechanism design is. When referring to more side information, the adversary could have a certain probability to guess and compromise the privacy of a query issuer. That motivates us to think about this problem from a different direction. The basic idea in our work takes advantage of the social connection from social media, in which location queries and corresponding results are sent through social media. It can be summarized as follows.

In the proposed mechanism, we introduce a different architecture which introduce the friends of the query issuer to be the intermediary. The query issuer will not send the query to the LBS server but to one of its social friends instead. The friends from social networks of a query issuer then will help the issuer to submit a query to the LBS server. In this architecture, the original query issuer would not communicate with the LBS server directly at all. So that the actual query issuer's identification can be hidden from the LBS server.

In this way, the near-complete privacy protection can be achieved. However, the positive adversary may be able to track the historical data and social connections of our query issuer. It is possible for the positive adversary to analyze the regularity of a LBS query and compromise the identity. To avoid this, a differential privacy mechanism is further applied to incorporate the possibility of the participation of query issuer to further protect our query issuers.

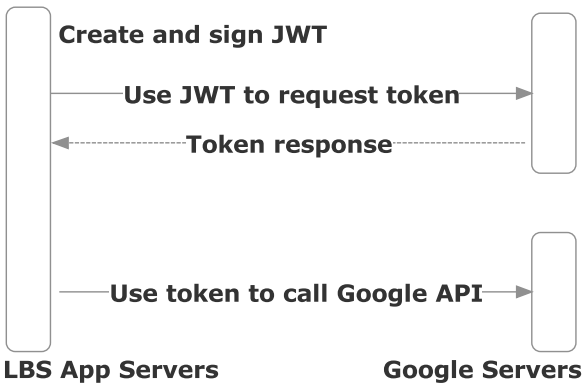


FIGURE 2. Verification mechanism of social network's API.

The implementation principle is based on the existing social media system and their open account APIs. These social media system could be employed as the foundation of our cognitive network independent to the LBS server. For example, as shown in Fig. 2, Google's service-account require applications to create and cryptographically sign JSON Web Tokens (JWTs).[3] Through Token, the application could directly call social media's API to do instant message, Email, and communication *etc.*

IV. COGNITIVE ARCHITECTURE AND DIFFERENTIAL PRIVACY MECHANISM

In this section, we discuss the cognitive architecture and differential privacy mechanism of our proposed privacy protection in detail.

A. COGNITIVE ARCHITECTURE FOR PRIVACY PROTECTION

The key idea of the cognitive architecture is to build a mechanism to let query issuer's friends help the query issuer to communicate with the LBS server. In this paper, we will try two different strategies on different scenarios. In one situation, the query issuer is completely hidden from the LBS server by not participating in the query interaction with the LBS server. In this case, the query issuer is not going to send the query to the LBS server but will send all queries to his/her social friends, instead. In the other situation, the query issuer will participates the query process and interactive with the LBS server with his/her social friends. The query issuer will also receive query result from the LBS server directly. Our objective is, to hide the query issuer among his/her social friends so that it can not be identified easily. To be specific, we aims to limit the probability that the real query issuer can be identified within $1/(2k)$ (k is the number of friends of the query issuer).

1) COMPLETE PROTECTION

The complete protection is achieved in the way that the real query issuer will not attempt to submit a query at all. Instead, his/her social will help her/him to interact with the LBS server, including submit queries and receive query results. For example, if a query issuer γ wants to get recommendation for the restaurant near location l. He will chose some of his/her social friends $\gamma_1, \gamma_2, \ldots$ from u's friend set $F(u)$ and let them know about his/her need. Then, those selected friends would send the query $Q(l, \text{“}restaurant\text{”})$ to the LBS server. During this process, for the LBS server, the query it received is from query issuer γ_1 and γ_2. Since the location information is very accurate and specific, the answer to this query could be ultimately optimized. On the other hand, because the actual query issuer is not involved in the location-based query process, the privacy is near-complete protected.

2) QUERY ISSUER INVOLVED PROTECTION

If the adversary is a positive adversary that interested in collecting query history data and side information related to all queries it monitored, the complete protection may not work as effective as we expect. For example, if the adversary can figure out the strategy and the relationships among the query issuers who obtained services from the LBS server based on its collected data. The adversary has the chance to

[3]https://developers.google.com/identity/protocols/OAuth2#libraries

check all query regarding the same location l from different query issuer γ_1, γ_2, etc. and find out the real query issuer u' by analyzing the common friend of those query issuers. In this case, there is a very high probability that real query issuer u' will be identified. What make the situation even worse is that all queries submitted to the LBS server contains accurate location information. If the adversary could compromise the query and corresponding identity, the accurate location privacy is going to be lost completely. Therefore, to provide a complete privacy protection system, we proposed the differential privacy mechanism for the situation that when the query issuer is involved in the query. It guarantees that under the case there is a positive adversary, and the adversary collects a lot of historical data and side information related to our query issuers, we solution still achieve a very good privacy protection level.

B. DIFFERENTIAL PRIVACY MECHANISM

The differential privacy mechanism is proposed to protect the situation that the adversary positively collects the query information and side information to analyze the identity of the query issuer. As illustrated, we actually do not need to worry if there is no or few social information leakage at the the LBS server end. For example, the LBS server does not keep query history or side information. In this case, our LBS query architecture could preserve a near-complete privacy protection. However, in reality, during the service life of the LBS, it is natural for the service provider to collect user's historical query and side information (for providing better or more customized recommendation for most of the time). Because of that, there is a certain probability for the adversary to break the real identity and location privacy of the query issuer. To address this issue, we develop a differential privacy mechanism to protect privacy with theoretical guarantees.

In order to more clearly introduce the proposed mechanism, the following definition is proposed.

Definition 1 (ϵ-Differential Privacy): Given a randomized function F*, it gives ϵ-differential privacy if and only if all data sets D_1 and D_2 differing on at most one element, and all $X \in Range$(*F*)*

$$Pr[\mathrm{F}(D_1) \in X] \leq exp(\epsilon) \times Pr[\mathrm{F}(D_2) \in X] \tag{2}$$

In Equation 2, parameter ϵ is a public parameter that usually obtained from experience or experiment in practice. Typically, the value of ϵ is selected from 0.01, 0.1, $ln2$ or $ln3$, etc. Which one is the best fit is not our focus in this work so the discussion on ϵ is beyond the scope of our work. Differential privacy model introduce a randomized function F to model users' behavior, which is independent of any other side information related to adversary or users. Thus, the privacy level of a mechanism considering if it satisfies this definition or not will not be influenced by the status of the adversary.

The key point of differential privacy mechanism is to add noise to the true answer so that could preserving the privacy. Let a query be a function $q(\cdot)$, the database stored at the LBS server is denoted as D, the corresponding query result returned from the server is denoted as a value of $q(D)$. In the differential privacy mechanism, a randomized function F is generated to add appropriately noise to the true answer to produce a final *response*. The following definition of sensitive function $q(\cdot)$ is introduced to evaluate the privacy protection degree.

Definition 2 (Sensitivity of $q(\cdot)$): For all adjacent database D_1, D_2 differing in at most one element, the sensitivity of $q(\cdot)$ is:

$$\bigtriangleup q = \max_{D_1, D_2} \parallel q(D_1) - q(D_2) \parallel_k \tag{3}$$

Specifically, if parameter k equals to 1, function $q(\cdot)$ actually achieve a maximum difference in the values that the function q could take on a pair of databases that differer in only one element.

V. INCENTIVE MECHANISM

To guarantee the k-anonymity of a query issuer, it requires the query issuer obtain help from at least $k-1$ social friends. However, it is possible that a query issuer can not find $k-1$ friends who would like to provide help at a specific time. There are two reasons: i) a query issuer may have few friends who own their account on existing social media system, it is hard to find $k-1$ friends of the query issuer to provide help; ii) at a specific time, like midnight, most of the friends' social media system of a query issuer is offline. Therefore, for each LBS query of a query issuer, we recruit both friends and strangers from the social media system to help to query. If a user of a social media system helps to query, the user should first install related app which supports the general interest query based on the search result on his or her device. Helping to query brings cost to users of a social media system such as battery resource, computational resource, and storage resource. Some users may reject participating in helping to query. To attract enough users of social media systems to participate in query, the query issuer should make monetary reward for them. We model this problem as an auction process, in which each query from a query issuer is regarded as a query task [21], [45], [46]. The query issuer acts as an auctioneer and a buyer to control the auction process and buy query service from users of social media systems. Besides, users of social media systems are sellers who can sell their query service to query issuers.

The auction process have five phases, which are briefly summarized in the following:

- **Phase 1: Publish task information.** In the beginning, the query issuer announces query task set on the platform.
- **Phase 2: Submit bidding information.** After obtaining the query tasks' information, each user on the social media system submits its cost and the set of query tasks to the query issuer.
- **Phase 3: Publish auction results.** The query issuer collects users' information, determine task assignments,

and calculate payment. The query issuer publish the auction results on the platform.

- **Phase 4: Help to query.** These winner users help to query each assigned task at the required time.
- **Phase 5: Make payments.** The query issuer makes the payments to the winning users.

The working process is shown in Figure 11. We proposed an auction-based incentive mechanism in Phase 3.

A. AUCTION MODEL FORMULATION

Generally, more than one query will be launched when a query issuer arrives at a new place. We use $\Pi = \{\pi_1, \pi_2, \ldots, \pi_m\}$ to denote the set of queries of a query issuer. Each query task $\pi_i \in \Pi$ has two attributes, which can be represented as

$$\pi_i = (t_i, k_i),$$

where t_i is the time the query launched and k_i points out that how many times the π_i should be queried by other users in the social media system. The value of k_i is related to the privacy target of the π_i. $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ represents the set of users from the social media systems who agree on helping to query. Each $\gamma_j \in \Gamma$'s attributes can be represented as

$$\gamma_j = (S_j, c_j),$$

where $S_j \subseteq \Pi$ denotes the subset of query tasks can be done by π_j. c_j is the cost of π_j helping to query all query tasks in S_j. Each user γ_j can help to query a task in S_j at most one time.

An binary variable x_{ij} is used to show the query task assignment results. If user γ_j is assigned to work for query task π_i, $x_{ij} = 1$. Otherwise, $x_{ij} = 0$. γ_j can help to query one or query tasks in S_i. p_j represents the payment of the γ_j from the query issuer. If γ_j is not assigned to any query task in Π, the cost of γ_j is 0 and $p_j = 0$. Otherwise, the cost of γ_j is c_j and the $p_j \geq 0$.

The objective of the query issuer is to recruit users in Γ which can complete the query tasks which can achieve k-anonymity as well as minimum cost. The task assignment and price calculation problem can be formalized as

$$\min \sum_{j=1}^{n} p_j, \tag{4a}$$

$$s.t. \sum_{j=1}^{n} x_{ij} \geq k_i, \quad \forall\, i \in [1, m], \tag{4b}$$

$$\sum_{i=1}^{m} x_{ij} \leq |S_j|, \quad \forall j \in [1, n], \tag{4c}$$

$$p_j \geq c_j \sum_{i=1}^{m} x_{ij}, \tag{4d}$$

$$x_{ij} \in \{0, 1\}, \tag{4e}$$

In Eq. 4, the query issuer aims to minimize the cost such that the following conditions should hold: (i) Eq. 4b indicates how many times a query should be helped by users in the social media system; (ii) Eq. 4c represents the number of queries assigned to any user γ_j of the social media system can not exceed the number of query tasks in S_j; (iii) Eq. 4d requires that the payment of of a user can not be smaller than his or her cost; (iv) Eq. 4e shows the range of assignment variable.

We consider three properties when designing incentive mechanism:

- **Individual rationality.** We define the utility of a user as the difference between received payment and the cost. No MUD obtains a negative utility.
- **Price truthfulness.** It indicates that no user can improve its received utility via lying on his or her cost.
- **Computational efficiency.** The results of the mechanism can be done in real time.

B. INCENTIVE MECHANISM DESIGN

Our objective is to design a mechanism that approximately minimize the cost while guaranteeing k-anonymity as well as the three properties. Generally, there are two phases in an auction-based incentive mechanisms: winner determination and payment calculation. The detailed algorithms are shown as follows.

Winner Determination: We use W as the winner set of users and initial value is empty.

Algorithm 1 Winner Determination

Input: Π, Γ
Output: W
Set $W = \emptyset$, $\{\delta_j\} = \{0\}$
Find the user with the largest marginal contribution
Set $\delta^* = 0, j^* = 0$
Winner determination
for Each $\gamma_j \in \Gamma / W$ **do**
  $\delta_j = \frac{|S_j|}{c_j}$
  if $\delta_j > \delta^*$ **then**
    $\delta^* = \delta_j /, j^* = j, W = W \cup \gamma_{j^*}$
  end if
end for
while $\exists\, \pi_i \in \Pi, \sum_{j':\gamma_{j'} \in W, \pi_i \in S_{j'}} 1 < k_i$ **do**
  Set $\delta^* = 0, j^* = 0$
  for Each $\gamma_j \in \Gamma / W$ **do**
    $\delta_j = |S_j|/c_j$
    if $\delta_j > \delta^*$ **then**
      $\delta^* = \delta_j, j^* = j, W = W \cup \gamma_{j^*}$
    end if
  end for
end while

In Algorithm 1, we greedily select winners according to the ratio of users' marginal contribution over costs.

Price Calculation: After winners are identified, query issuer calculates the payment for each winner $\gamma_j \in W$ via identifying γ_j's *critical neighbor*, which is defined to be the

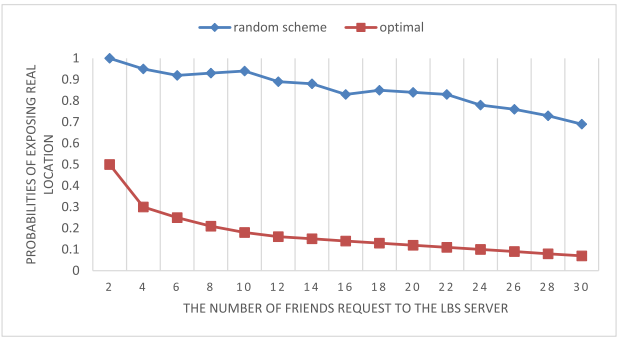


FIGURE 3. Probability of User's real location release.

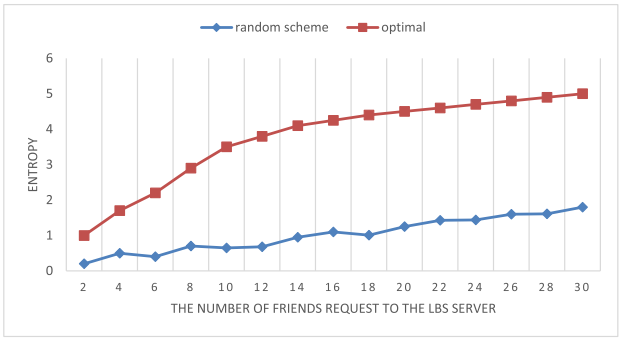


FIGURE 4. Entropy of our resolution VS random scheme.

user who could lead to the failure of the γ_j. Detailed way to calculate the payments is shown in Algorithm 2.

Algorithm 2 Price Calculation

Input: Π, Γ, W
Output: $\{p_j\}$
Set $\{p_j\} = \{0\}$
for Each winner $\gamma_w \in W$ **do**
  Set $\Gamma_{-\gamma_w} = \Gamma / \gamma_w$
end for
Set $\delta^* = 0, j^* = 0, W_{-\gamma_w} = \emptyset$
for Each $\gamma_w \in \Gamma_{-\gamma_w} / W_{-\gamma_w}$ **do**
  for Each $\pi_i \in \Pi$ **do**
    $\delta_j = \delta_j + \delta(i, j, W_{-\gamma_w})$
  end for
  if $\delta_j / c_j > \delta^*$ **then**
    $\delta^* = \delta_j / c_j, j^* = j, W_{-\gamma_w} = W_{-\gamma_w} \cup \gamma_{j^*}$
  end if
  if $\forall \pi_i \in S_w, \sum_{j':\gamma_{j'} \in W_{-\lambda_w}, \pi_i \in S_{j'}} 1 \geq k_i$ **then**
    $p_i = \frac{|S_w|}{|S_{j^*}|} c_{j^*}$
  end if
  while $\exists \pi_i \in \Pi, \sum_{j':\gamma_{j'} \in W, \pi_i \in S_{j'}} 1 < k_i$ **do**
    Set $\delta^* = 0, j^* = 0$
    for Each $\gamma_j \in \Gamma / W_{-\gamma_w}$ **do**
      $\delta_j = |S_j| / c_j$
      if $\delta_j > \delta^*$ **then**
        $\delta^* = \delta_j, j^* = j, W_{-\gamma_w} = W_{-\gamma_w} \cup \gamma_{j^*}$
      end if
    end for
  end while
  if $\forall \pi_i \in S_w, \sum_{j':\gamma_{j'} \in W_{-\lambda_w}, \pi_i \in S_{j'}} 1 \geq k_i$ **then**
    $p_i = \frac{|S_w|}{|S_{j^*}|} c_{j^*}$
  end if
end for

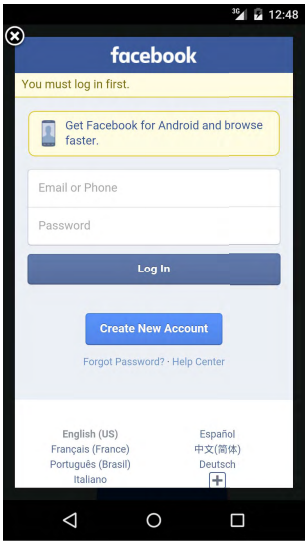


FIGURE 5. Login interface.

FIGURE 6. App login.

C. PROPERTIES ANALYSIS

Lemma 1: The winner MUDs set selection provided in Algorithm 1 is monotonic.

Proof: If γ_j is selected as a winner with c_j and S_j, its contribution is $\delta_j = \frac{|S_j|}{c_j}$. We set $c'_j \leq c_j$, we should prove

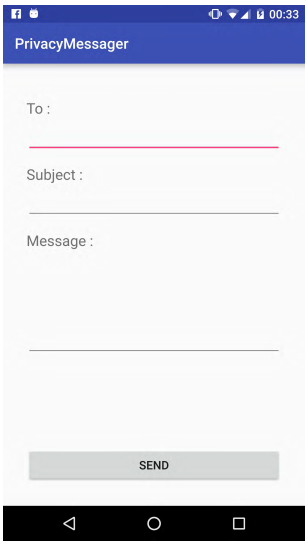


FIGURE 7. App message.

FIGURE 8. Welcome message.

that γ_j can still win with c'_j and S_j. The new contribution is $\delta'_j = \frac{|S_j|}{c'_j}$. Since $\delta'_j \leq \delta_j$, γ_j is still selected as winner Algorithm 1. Next, we can see that γ_j will become winner with c_j and S'_j, where $S'_j \supseteq S_j$. ■

Lemma 2: The payment p_j to each $\gamma_j \in W$ is the critical value.

Proof: Each winner γ_j's payment is $p_i = \frac{|S_w|}{|S_{j^*}|} c_{j^*}$, in which S_{j^*} and c_{j^*} are submiited by the the critical user of γ_j, if the $c_j > \frac{|S_w|}{|S_{j^*}|} c_{j^*}$, the γ_j would not be selected as winner. Thus, p_i is critical value. ■

Theorem 1: The incentive mechanism designed in this paper is truthful.

Theorem 2: The incentive mechanism designed in this paper is individual rational.

Proof: According to the theorem 2, a user γ_j would be loser if $c_j > \frac{|S_w|}{|S_{j^*}|} c_{j^*}$. For each winner γ_j, the payment is $p_i = \frac{|S_w|}{|S_{j^*}|} c_{j^*}$. Thus, individual rationality is guaranteed. ■

Theorem 3: The incentive mechanism designed in this paper is computationally efficient.

Proof: The time complexity of Algorithm 1 is n^2. The time complexity of Algorithm 2 is n^2. Thus, the incentive mechanism designed in this paper is computationally efficient. ■

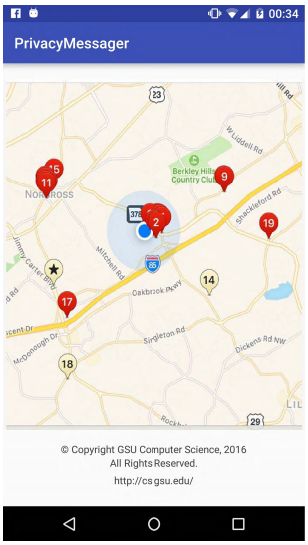


FIGURE 9. Result map.

VI. PERFORMANCE EVALUATIONS

A. EXPERIMENT SETUP

The general idea of our solution is to optimize the selection of friends of the query issuer, then to protect the adversary may exploit some side information to compromise the privacy of query issuer.

As shown in Fig. 3, it indicates the probability of finding the user's real location by the LBS server from all user's friends requests. The random scheme and the optimal scheme is significantly different. Next, we evaluate the entropy with a different number of user's friends evolved in the location-based request. In Fig. 4, the performance of the optimal scheme is much better than the random one which is because all friends who helped the query user have the same probability to be targeted as the real user's, which actually hidden the real target in a better way.

B. APPLICATION IMPLEMENTATION

To illustrate and verify our novel architecture for privacy preservation, we implemented one Android app PrivacyMessage(PM), which could support the general interest query based on the search result of Yelp,[4] and implement the communication through Facebook API. Yelp is one of the largest information integration provider includes both

[4]https://www.yelp.com/developers/documentation/v2/overview

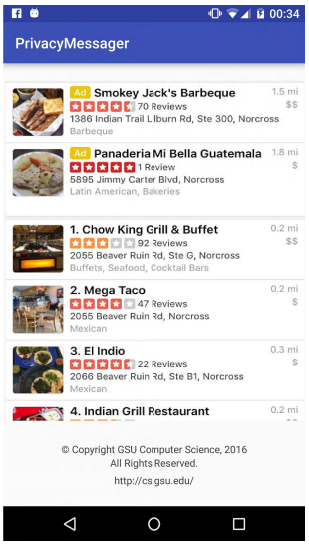


FIGURE 10. Result list.

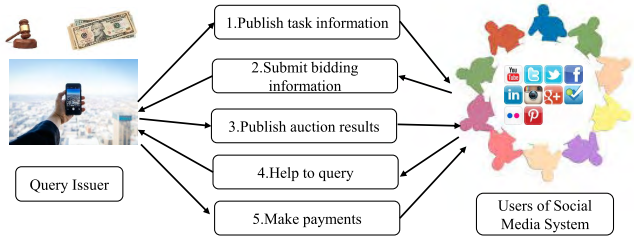


FIGURE 11. The auction process.

website and Android mobile App that connects people with the local business found in 2004. In the second quarter of 2016, the average monthly mobile App unique users have reached 23 million, and more than 72% search queries are coming from mobile devices users.[5] On another hand, Facebook as one of the world largest social media provides API for developers to implement their customized functions based on the authorization of each users.[6] Through the API provided by Facebook, we could let the user of our QuerySafer login through Facebook directly, and request all the location-based query from their facebook friends who are using the same service. And all query and answer data are transparently to the location-based services provide Yelp on this occasion.

As shown in Fig. 5 require the user to the login in our App through their Facebook account. Fig. 6 demonstrates the interface when the user login our App with their Facebook account. During the time they are logging into the system, our App could retrieve the user's friends and the basic profile under their authorization. Our prototype App sends the message through the Facebook message, as shown in Figure 7, and another user who gets the LBS query through the message could sent the query out to the LBS server in order to collect answer for the original query issuer. And this just provides the feasibility to implement our privacy safe architecture.

Fig. 8 is the welcome page after authorization. All message and location query is going to be sent through Facebook connection to one user's friends first, how many friends and messages need to sent out is according to the social activity of the social cycle for each users. Then Fig. 9 and Fig. 10 show the returned result of queries.

[5]https://www.yelp.com/factsheet

[6]https://developers.facebook.com/products/login

VII. CONCLUSION

In this paper, we proposed a novel architecture to achieve a near-complete location privacy protection. By employing the nature connection of popular social network, we are pursuing one resolution for location based services with separated query issuer and query itself. Since we cut off the connection the LBS query and the query issuer, untrusted LBS server or any other adversary could not get the location privacy anymore. We also proposed an enhanced differential privacy mechanism in case the social network releasing their users' behavior pattern. According to our mechanism, even the LBS or social network collect much side information to refer users' identity, the algorithm could still guarantee the leakage of privacy is quite few or even deflectable. Furthermore, we tested our architecture, mechanism with convincing data and developed an open source Android App as a practical application based on Yelp and Facebook APIs to practice our contribution in real mobile device App market.

REFERENCES

[1] D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2011, pp. 193–204.

[2] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: User movement in location-based social networks," in *Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2011, pp. 1082–1090.

[3] X. Chen and J. Pang, "Exploring dependency for query privacy protection in location-based services," in *Proc. 3rd ACM Conf. Data Appl. Secur. Privacy*, 2013, pp. 37–48.

[4] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 251–262.

[5] M. Han, M. Yan, Z. Cai, and Y. Li, "An exploration of broader influence maximization in timeliness networks with opportunistic selection," *J. Netw. Comput. Appl.*, vol. 63, pp. 39–49, Mar. 2016.

[6] B. Yang, I. Sato, and H. Nakagawa, "Bayesian differential privacy on correlated data," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2015, pp. 747–762.

[7] E. Fung, G. Kellaris, and D. Papadias, "Combining differential privacy and pir for efficient strong location privacy," in *Proc. Int. Symp. Spatial Temporal Databases*, 2015, pp. 295–312.

[8] M. Han, Y. Liang, Z. Duan, and Y. Wang, "Mining public business knowledge: A case study in SEC's EDGAR," in *Proc. IEEE Int. Conf. Big Data Cloud Comput. (BDCloud), Social Comput. Netw. (SocialCom), Sustain. Comput. Commun. (SustainCom)(BDCloud-SocialCom-SustainCom)*, Oct. 2016, pp. 393–400.

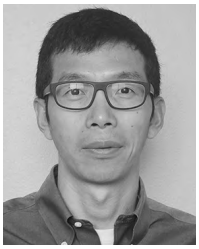
[9] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 617–627.

[10] B. Niu, Z. Zhang, X. Li, and H. Li, "Privacy-area aware dummy generation algorithms for location-based services," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 957–962.

[11] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2015, pp. 1017–1025.

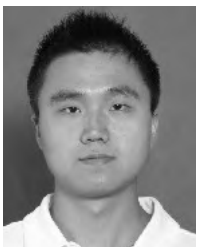
[12] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.*, 2008, pp. 1–19.
[13] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 901–914.
[14] M. Han, M. Yan, Z. Cai, Y. Li, X. Cai, and J. Yu, "Influence maximization by probing partial communities in dynamic online social networks," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 4, p. e3054, 2017.
[15] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1–18, Jan. 2008.
[16] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discovery Data*, vol. 1, no. 1, p. 3, 2007.
[17] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proc. Int. Workshop Privacy Enhancing Technol.*, 2002, pp. 41–53.
[18] T. Shi, S. Cheng, Z. Cai, Y. Li, and J. Li, "Retrieving the maximal time-bounded positive influence set from social networks," *Pers. Ubiquitous Comput.*, vol. 20, no. 5, pp. 717–730, 2016.
[19] W. Tong, E. Miyano, R. Goebel, and G. Lin, "A PTAS for the multiple parallel identical multi-stage flow-shops to minimize the makespan," in *Proc. FAW*, 2016, pp. 227–237.
[20] W. Tong, R. Goebel, and G. Lin, "Smoothed heights of tries and patricia tries," *Theor. Comput. Sci.*, vol. 609, pp. 620–626, Jan. 2016.
[21] Z. Duan, W. Li, and Z. Cai, "Distributed auctions for task assignment and scheduling in mobile crowdsensing systems," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 635–644.
[22] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2789–2800, Mar. 2017.
[23] Z. He, Z. Cai, and X. Wang, "Modeling propagation dynamics and developing optimized countermeasures for rumor spreading in online social networks," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2015, pp. 205–214.
[24] M. Han, W. Zhang, and J.-Z. Li, "RAKING: An efficient K-maximal frequent pattern mining algorithm on uncertain graph database," *Chin. J. Comput.*, vol. 33, no. 8, pp. 1387–1395, 2010.
[25] H. Albinali, M. Han, J. Wang, H. Gao, and Y. Li, "The roles of social network mavens," in *Proc. 12th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Dec. 2016, pp. 1–12.
[26] M. Han, M. Yan, J. Li, S. Ji, and Y. Li, "Neighborhood-based uncertainty generation in social networks," *J. Combinat. Optim.*, vol. 28, no. 3, pp. 561–576, 2014.
[27] M. Han, L. Li, X. Peng, Z. Hong, and M. Li, "Information privacy of cyber transportation system: Opportunities and challenges," in *Proc. 6th Annu. Conf. Res. Inf. Technol. (RIIT)*, New York, NY, USA, 2017, pp. 23–28. [Online]. Available: http://doi.acm.org/10.1145/3125649.3125652
[28] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Comput. Netw.*, vol. 102, pp. 157–171, Jun. 2016.
[29] M. Han, Z. Duan, and Y. Li, "Privacy issues for transportation cyber physical systems," in *Secure and Trustworthy Transportation Cyber-Physical Systems*. Singapore: Springer, 2017, pp. 67–86.
[30] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Syst., Appl. Services*, 2003, pp. 31–42.
[31] H. Yin *et al.*, "Discovering interpretable geo-social communities for user behavior prediction," in *Proc. IEEE 32nd Int. Conf. Data Eng. (ICDE)*, May 2016, pp. 942–953.
[32] M. Han, Q. Han, L. Li, J. Li, and Y. Li, "Maximizing influence in sensed heterogenous social network with privacy preservation," *Int. J. Sensor Netw.*, vol. 1, pp. 1–11, Jan. 2017.
[33] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in *Proc. Int. Symp. Spatial Temporal Databases*, 2007, pp. 239–257.
[34] M. Hay, A. Machanavajjhala, G. Miklau, Y. Chen, and D. Zhang, "Principled evaluation of differentially private algorithms using dpbench," in *Proc. Int. Conf. Manage. Data*, 2016, pp. 139–154.
[35] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *Proc. IEEE 24th Int. Conf. Data Eng. (ICDE)*, Apr. 2008, pp. 277–286.
[36] S.-S. Ho and S. Ruan, "Differential privacy for location pattern mining," in *Proc. 4th ACM SIGSPATIAL Int. Workshop Secur. Privacy GIS LBS*, 2011, pp. 17–24.
[37] S. Ioannidis, A. Montanari, U. Weinsberg, S. Bhagat, N. Fawaz, and N. Taft, "Privacy tradeoffs in predictive analytics," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 1, pp. 57–69, 2014.
[38] Q. Xiao, M. K. Reiter, and Y. Zhang, "Mitigating storage side channels using statistical privacy mechanisms," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 1582–1594.
[39] J. Zhang, X. Xiao, and X. Xie, "PrivTree: A differentially private algorithm for hierarchical decompositions," in *Proc. Int. Conf. Manage. Data*, 2016, pp. 155–170.
[40] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *Biological*, vol. 24, no. 3, pp. 1732–1744, 2016.
[41] Z. Chi, Y. Wang, Y. Huang, and X. Tong, "The novel location privacy-preserving CKD for mobile crowdsourcing systems," *IEEE Access*, vol. 6, pp. 5678–5687, 2018, doi: 10.1109/ACCESS.2017.2783322.
[42] L. Duan, T. Kubo, K. Sugiyama, J. Huang, T. Hasegawa, and J. Walrand, "Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1701–1709.
[43] J.-S. Lee and B. Hoh, "Sell your experiences: A market mechanism based incentive for participatory sensing," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2010, pp. 60–68.
[44] A. Singla and A. Krause, "Truthful incentives in crowdsourcing tasks using regret minimization mechanisms," in *Proc. 22nd Int. Conf. World Wide Web*, 2013, pp. 1167–1178.
[45] Z. Duan, M. Yan, Z. Cai, X. Wang, M. Han, and Y. Li, "Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems," *Sensors*, vol. 16, no. 4, p. 481, 2016.
[46] Z. Duan, L. Tian, M. Yan, Z. Cai, Q. Han, and G. Yin, "Practical incentive mechanisms for IoT-based mobile crowdsensing systems," *IEEE Access*, vol. 5, pp. 20383–20392, 2017.

MENG HAN (M'13) received the Ph.D. degree in computer science from Georgia State University. He is currently an Assistant Professor with the College of Computing and Software Engineering, Kennesaw State University. His research interests include big social data mining, cyber data security and privacy, and data-driven intelligence. He is currently an ACM Member and an IEEE COMSOC Member.



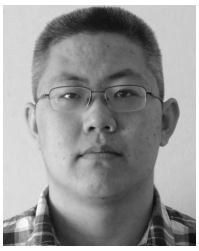
LEI LI received the Ph.D. degree in computer information systems from Georgia State University. He is currently a Professor of information technology with the College of Computing and Software Engineering, Kennesaw State University. His current research interests include social media data analytics, information security, Web information management, and IT education. His research has appeared in the *Journal of Systems and Software*, the *Journal of Information Systems Education*, the *Journal of Universal Computer Science*, the *Journal of Management Information and Decision Science*, and various IEEE and ACM conferences.

YING XIE is currently a Professor of information technology and the Director of the Equifax Data Science Research Lab, Kennesaw State University. His research was sponsored by several U.S. companies and the National Science Foundation. He holds two U.S. patents on data analytics and a couple of pending U.S. patents as co-inventor. His current research interests include data science and machine learning and their applications in different domains. He has been involved in organizing several international conferences and workshops on data mining. He has served in the Editorial Board of the *Journal of Big Data Research* (Elsevier).



JINBAO WANG received the master's and Ph.D. degrees from the School of Computer Science and Technology, Harbin Institute of Technology, China, in 2008 and 2013, respectively. He is currently a Lecturer with the Academy of Fundamental and Interdisciplinary Sciences, Harbin Institute of Technology. His main research interests include big data analytics and data privacy.

ZHUOJUN DUAN received the M.S. degree from Shaanxi Normal University in 2011. She is currently pursuing the Ph.D. degree with the Department of Computer Science, Georgia State University. Her research interests include truthful auction in the Internet of Things, game theory, social network, and data analytics.



JI LI received the B.S. degree from the School of Computer Science and Technology, Heilongjiang University, China. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Georgia State University. His research interests include mobile crowdsensing.

MINGYUAN YAN (M'13) received the B.S. degree in computer science and technology and the M.S. degree in information security from Wuhan University, Wuhan, China, in 2008 and 2010, respectively, the M.S. degree in computer science from Georgia State University, in 2012, and the Ph.D. degree from the Department of Computer Science, Georgia State University, in 2015. She is currently an Assistant Professor in computer science with the University of North Georgia. Her research interests include data management and protocol design in wireless networks, influence maximization, information dissemination in mobile social networks, information security, and big data management. She is an IEEE COMSOC Member.