International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

LOCATION PRIVACY PROTECTION MECHANISMS USING ORDER-RETRIEVABLE ENCRYPTION FOR SOCIAL NETWORK

*1Ms. Shalini P, *2 Ms. Abarna N.

*1M.Phil Research Scholar, PG & Research Department of Computer Science & Information Technology, Arcot Sri Mahalakshmi Women's College, Villapakkam, Tamil Nadu, India.
*2.Assistant Professor, PG & Research Department of Computer Science & Information Technology, Arcot Sri Mahalakshmi Women's College, Villapakkam, Tamil Nadu, India.

---***---

Abstract: A common functionality of many location-based social networking applications is a location sharing service that allows a group of friends to share their locations. With a potentially untrusted server, such a location sharing service may threaten the privacy of users. Existing solutions for Privacy-Preserving Location Sharing Services (PPLSS) require a trusted third party that has access to the exact location of all users in the system or rely on expensive algorithms or protocols in terms of computational or communication overhead. Other solutions can only provide approximate query answers. To overcome these limitations, we propose a new encryption notion, called Order-Retrievable Encryption (ORE), for PPLSS for social networking applications. The distinguishing characteristics of our PPLSS are that it (1) allows a group of friends to share their exact locations without the need of any third party or leaking any location information to any server or users outside the group, (2) achieves low computational and communication cost by allowing users to receive the exact location of their friends without requiring any direct communication between users or multiple rounds of communication between a user and a server, (3) provides efficient query processing by designing an index structure for our ORE scheme, (4) supports dynamic location updates, and (5) provides personalized privacy protection within a group of friends by specifying a maximum distance where a user is willing to be located by his/her friends. Experimental results show that the computational and communication cost of our PPLSS is much better than the state-of-the-art solution.

Keywords: Location privacy, location sharing services, order-retrievable encryption, location-based social networking, spatio-temporal query processing

I. INTRODUCTION

Recently people have been receiving more and more digitized information from Internet, and the volume of information is larger than any other point in time, reaching a point of information overload. To solve this problem, the recommender system has been created in response to the need to disseminate so much information. It does not only filter the noise, but also help to select attractive and useful information. Recommender system has achieved initial success based on a survey that shows at least 20 percent of sales on Amazon's website come from the recommender system.Social networks gather volumes of information contributed by users around the world. This information is versatile. It always contains item/services descriptions (including textual descriptions, logos and pictures), users' comments, moods and users' social circles, prices, and locations. It is very popular for recommending users' favorite services from crowd-source contributed information.

However, with the rapid increase in number of registered Internet users and more and more new products available for purchase online, the issue of cold start for users and sparsity of datasets has become increasingly intractable. Fortunately, with the popularity and rapid development of social networks, more and more users enjoy sharing their experiences, such as reviews, ratings, photos and moods. The interpersonal relationships have become transparent and opened up as more and more users share this information on social media websites such as Facebook, Twitter, Yelp, Douban, Epinions, etc. The circles of friends also bring opportunities and challenges for a recommender system to solve the issues of cold start and sparsity.

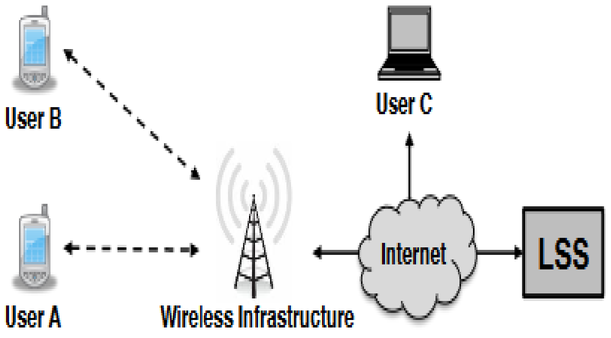


Fig : Location based Services

For the scope of this thesis we focus on Location-Based Service (LBS). In these services the user's location is processed in order to deliver a service, such as finding a nearby Point-of-Interest (POI) or getting directions. Due to their usefulness, LBS are being used by most mobile device users. Some services require the users to reveal their location either sporadically or continuously. The difference between the two is that in the sporadic case two consecutive queries to the LBS of the same user happen with sufficient time in between so that they do not correlate. We shall understand LBSs from a broader prospect than only from a technology perspective. Instead, we consider processing location data as a new socio-technical practice, having impact on technology, society and legislation. We adopt an interdisciplinary approach in order to understand the threats on privacy from engineering, ethical and legal perspectives**.**

For the domain of obfuscation-based location privacy protection we first propose a framework that allows the computation of optimal LPPMs for users who sporadically engage in LBSs. Our framework accounts for resource constraints of mobile devices with which LBSs are typically being accessed. This makes our framework suitable to compute optimal dummy and precision-based obfuscation strategies. An analysis of several optimal obfuscation strategies further shows the trilateral trade-off of privacy, Quality Loss (QL) and bandwidth overhead

- A concept of the rating schedule to represent user daily rating behavior.
- The factor of interpersonal rating behavior diffusion to deep understand users' rating behaviors.
- The main factors are, personal interest, interpersonal interest similarity, interpersonal rating behavior similarity, and interpersonal rating behavior diffusion, into matrix factorization with fully exploring user rating behaviors to predict user-service ratings.

II. BACK GROUND

Privacy assessment of LBSs from engineering, an ethical and a legal perspective. Scholars from every of the involved disciplines obtain an added value for their own field and additionally obtain an insight in how the topic is addressed in other disciplines. For example, the detail provided by the legal perspective serves as a valuable reference for legal scholars. However, scholars from other disciplines may find the provided information especially valuable, because works in their discipline typically lack this kind of legal detail. Also, the combination of the engineering, ethical and legal discipline to assess privacy implications in LBS contributes towards a better understanding of privacy issues from a broader perspective.

It apply the CI heuristic in a novel way. Typically, the CI heuristic is used to analyze how a new socio-technical practice impacts the CI in very specific situations. For example, consider a library that provides a paper-based repository of all available books that can be used by visitors to locate the books in which they are interested. If the library would replace this paper-based system by a computer-based search system, then the situation for the visitors would fundamentally change. While consulting the paper-based repository leaves no digital trace, any action on the computer-based system can be recorded. Finding the prevailing context of the CI heuristic is in this scenario relatively straight forward, because visitors use the system only in the library. This is different with LBSs as they are employed in numerous situations and contexts. In our work we analyze the impact of the new socio-technical practice on CI independent of a particular scenario. Instead, we employ the context of travelling for our analysis.

Location Data

It presents the necessary background on location data. We provide a detailed explanation on apps that are the most important tools for people to utilize the capabilities of their mobile devices, such as their location data. This also includes a description of the prevailing business model of the app-eco system and its privacy issues, as well as the users' attitude towards this business model. We continue with the explanation of the legal protection of location data and outline users' attitude towards LBSs. Finally, we provide a summary of the threats to user privacy when location data is misused.

Mobile Device Eco-System

Mobile devices are nowadays ubiquitous companions. More than two billion people worldwide are using smartphones and more than 1.2 billion people are using tablet computers. Smartphones are intuitive to use and they are equipped with a wide variety of communication modules, such as WiFi, Bluetooth and 4G/LTE, allowing their users to be connected in ways never possible before. Another reason for the success of smartphones is their platform, i.e. the Mobile Operating System (MOS) and the app-store that are maintained by the Platform Operator (PO). More traditional mobile phones usually run a MOS developed by the phone manufacturer and offered only a very limited number of additional applications, which typically have also been implemented by the phone manufacturer. The software of modern mobile devices, however, is much more sophisticated.

Legal Protection of Location Data

There are several directives in place for the protection of location data of which we discuss in detail the DPD, the ePrivacy Directive (2002/58/EC, as amended by 2009/136/EC) (ePrivacy Directive) directive and the recently published GDPR. The Data Protection Directive (95/46/EC) (DPD) [190] defines the legal rules for processing personal data. The term processing is very broad and can be anything from recording, handling and deleting data. The term personal data refers to "any information relating to an identified or identifiable natural person (data subject)", whereas the identification can be direct or indirect. Direct means to identify an individual without third party data sourcesMany models based on social networks have been proposed to improve recommender system performance. The concept of 'inferred trust circle' based on circles of friends. To recommend favorite and useful items to users. Their approach, called the Circle on Model, not only reduces the load of big data and computation complexity, but also defines the interpersonal trust in the complex social networks.

The similarity between users or items according to the number of common ratings. An item-based CF combined with a condition-based probability similarity and Cosine Similarity. Collaborative filtering-based recommendation approaches can be viewed as the first generation of recommender system.

III. DESIGN OF PRIVATE LOCATION-BASED

Most LBSs for mobile devices are privacy invasive, because the service provider learns the user's location data. A variety of services have been proposed that make this privacy invasion impossible. Such services employ cryptographic primitives that allow them to provide the necessary privacy guarantees. One of the most commonly used cryptographic primitives is homomorphic encryption that allows computations to be carried out on ciphertext. There exists several cryptosystems that provide this homomorphic property. Cryptosystem possess the *additive homomorphic property.* Given two plaintexts *m1* and *m2* and their respective encryptions *E(m1)* and *E(m2),* the following equation holds:

$$E.(mi) \copyright E.(m2) = E(mi + m2) \text{ -----(1)}$$

Geo-Social Networks

It proposes a private location-sharing service and employs hybrid encryption to protect the user's privacy. Every user is assumed to have a public/private key pair and users can exchange their public keys either out-of-band or with the help of the service provider. If Alice wants to inform Bob about her current location, she chooses a secret key, encrypts her location with the secret key, encrypts the secret key with the public key of Bob and sends both to Bob. The receiver Bob uses his private key to decrypt the symmetric key, enabling him to decrypt Alice's location. The data being sent between Alice and Bob could be transferred with the help of a central service provider, but if the service provider is reluctant to store and forward encrypted data, Alice and Bob could exchange their information with the help of a Distributed Hash Table (DHT),

POI Finder

One of the most commonly used LBSs allows users to find Point-of-Interest (POI) around their location. Therefore, the user submits a query to the service provider along with her location and, optionally, some additional information on what kind of POIs the user is interested in. Private Information Retrieval (PIR) is suited to implement a POI finder in a privacy-preserving way. PIR is a mechanism that allows users to query a database without the database server learning what information the user requested. It propose two protocols based on PIR. The first protocol works with a single PIR request at the cost of providing only approximate results. The second protocol has a higher computational and communication overhead but provides more accurate query results. Both protocols are built on a data structure based on Hilbert curves and search trees that convert the map coordinates of POIs into 1-dimensional coordinates preserving the proximity of POIs. This allows to apply PIR on originally two-dimensional data.

Traffic Monitoring

The idea of traffic monitoring is that cars on the road are equipped with tracking devices and report to a LBS additional data, such as their current speed. This allows the LBS to compute statistics, such as current road utilization, that can be used to navigate cars in a more efficient way. Clearly, such a system can provide considerable advantages, including the detection of traffic jams and the subsequent redirection of other cars to a faster route. However, if cars constantly reveal their locations, any observer would be able to learn private information about the users

Formally define the Sybil detection problem. Specifically, we first introduce the social Network model. Then we introduce a few design goals.

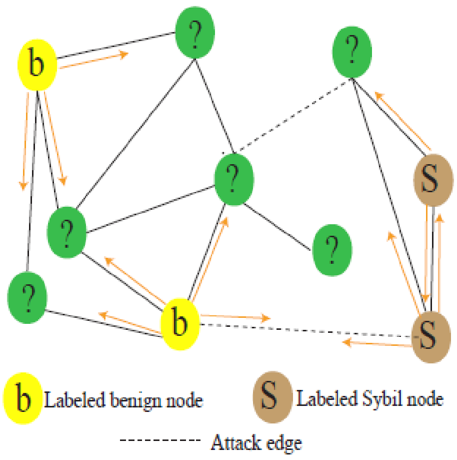


Fig : The propagation in Sybil

Let us consider an undirected social network G = (V;E), where a node v 2 V represents a user in the system and an edge (u; v) 2 E indicates that the users u 2 V and v 2 V are socially connected. In an ideal setting, G represents a weighted network of trust relationships between Users, where the edge weights represent the levels of trust between users [92]. Each node is either benign or Sybil.
Figure 3.1 illustrates a Sybil attack. We denote the sub network including the benign nodes and the edges between them as the benign region, denote the sub network including the Sybil's and edges between them as the Sybil region, and denote the edges between the two regions as attack edges. Note that the benign region could consist of multiple communities and we will evaluate their impact on Sybil detections

IV. PROPOSED ANALYSIS

In our research, user, item and tag are three fundamental entities of data. For the three basic entities, we define {a/, b/ and *T* as disjoint non-empty finite sets. We use set symbols in lower case with indices in the subscripts to denote individual elements of a set, for example, u_2 denotes the second user in the user set {c/. We use symbols of individual set elements, i.e., user , item iy, or tag t_p, in the subscripts or superscripts of the set symbols, as conditions imposed onto the sets to denote subsets. For example, denotes the item set in which each item was used by the vth user u„ 6 *U*.

- Users. *U* = u_2, — , u^, — ,U|y|} contains all users in a social tagging system. denotes the vth user, $u_5$6 0, 1 <*v* < |a[a/b|.
- Items. / = (t_1,t_2, —, ty, —, $t_{|7|}$} contains all items used by the users in the system. iy denotes the y'th item, iy 6 /, 1 < _/' < |a/b|.
- Tags. *T* = (t_1, t_2, —, t_p, —, $t_{|T|}$} contains all tags used by the users in the system. t_p denotes the pth tag, t_p 6 *T*, 1 < p < |T|.
- Tag assignments. The basic tagging behaviour, namely tag assignment, is defined as a 3-tuple e: *U* x / x *T* 6 {0,1}. If a user collected item $t_;$ with tag t„, then e„ $_t$ =1, otherwise e„ $_t$ =0.

User Profiling Based On Multidimensional Singular Value Decomposition

Traditionally some two-dimensional CF approaches apply SVD on a user-item matrix to compute user or item profiles and identify similar users/items (Symeonidis et al., 2006; Mi Zhang & Hurley, 2009). In these approaches, user-item matrix M 6 R't/'x'7' is decomposed and approximated by the truncated SVD:

Taking user-based CF, for example, <W|[/|XFC 1 £fcxfc is used to project each user's data from an |/|-dimensional space to a k-dimensional space, where k principal components of the data are preserved. Thus the user profile matrix in the SVD-based user profiling is computed as:

Recall that we have a social network G = (V, E) of the nodes in the system. Each node can have two states, i.e., benign or Sybil. Thus, we associate a binary random variable $xv \in \{-1,1\}$1g with each node. xv = +1 means that node v is a benign node and xv = ⍰1 indicates that node vis Sybil. In the following, we use xA to represent the set of random variables associated with the nodes in the set A. Moreover, we use _xA to denote the observed values of these random variables. There might exist some prior information about a node v independently from all other nodes in the system. Such prior information could be the content generated by v or its behavior. We model the prior belief of v being benign as follows:

$$P(xv = +1) = \frac{1}{1+\exp(-hv)},$$

Where hv quantities the prior information about v. More specifically, hv> 0 encodes the scenario in which v is more likely to be benign; hv< 0 encodes the opposite scenario; hv = 0 means prior information is not helpful to determine v's state. here now introduce $= \{u|(u,v)€E\}$, the set of v's neighbors in the social network, and their respective states _x€v . When these states are known, the probability of v to be benign is modeled as

$$P(xv = +1|xTv) = \frac{1}{1 + \exp(-\sum u€TvJuvXu - hv},$$

A Pair wise Markov Random Field

We find that the probabilistic local rule introduced in the previous section can be applied by modeling the social network as a pair wise Markov Random Field (MRF). A MRF defines a joint probability distribution for binary random variables associated with all the nodes in the network. Specifically, a MRF is specified with a node potential for each node v, which incorporates prior knowledge about v, and with an edge potential for each edge (u; v), which represents correlations between u and v. In the context of Sybil detection, we define a node potential _v(xv) for the node v as

$$u(xv) := \begin{cases} \theta vifxv = 1 \\ 1 - \theta vifxv = -1 \end{cases}$$

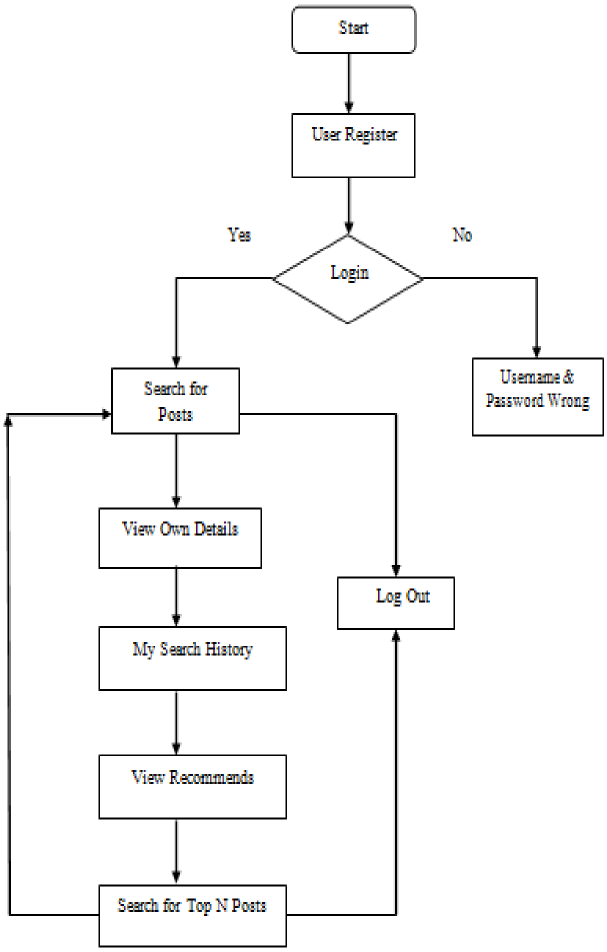


Fig : Markov Random Model Implementation

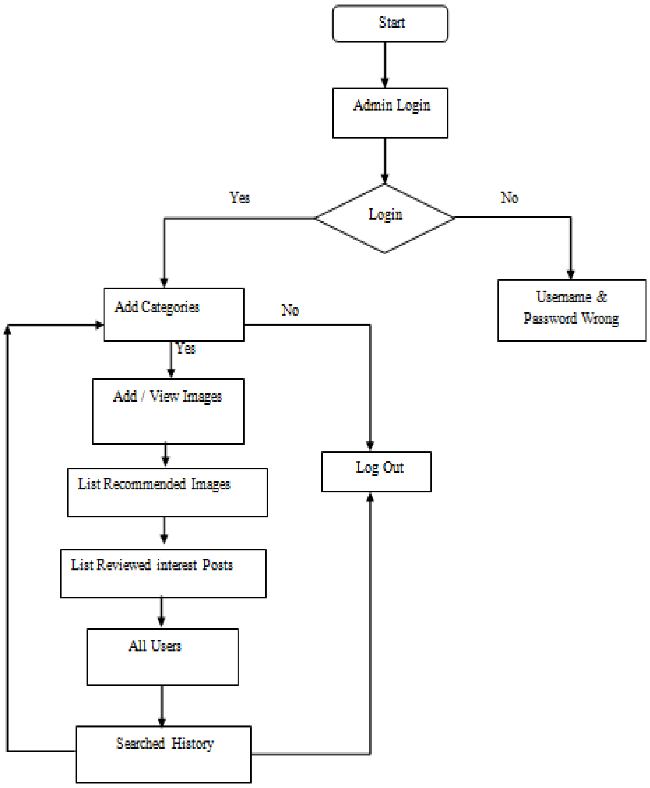


Fig : Order Retrieve Encryption Work Process

As mentioned above, user locations (i.e., points) in the database server are always in encrypted form. When an "encrypted" query location of Q1 for a group of friends is received by the database server, the database server should determine for any two friends' encrypted locations within the group which of them is closer to the encrypted query location. To achieve this, we use our proposed encryption notion ORE for geographical data. An ORE scheme is a symmetric key encryption scheme with two additional functions: one is for generating encrypted query locations and the other one is for the database server to determine which one between two encrypted user locations is closer to an encrypted query location. The scheme is called ORE because the order of the encrypted user locations in terms of their distances from any given encrypted query location can be retrieved. Note that the actual distance information is not retrievable.

Algorithm Implementation

1. Rating scale of individual users
2. Popularity of individual items
3. User preferences

$r_{ui}(t)=\mu+b_u(t)+b_i(t)+q^T{}_i p_u(t)$

Parameterizing the model

$r_{ui}(t)=\mu+b_u(t)+b_i(t)+q^T{}_i p_u(t)$

- Use functional forms: $b_u(t)=f(u,t)$, $b_i(t)=g(i,t)$, $p_u^{(t)}=h(u,t)$
- Need to find adequate f(), g(), h()
- General guidelines:
  – Items show slower temporal changes
  – Users exhibit frequent and sudden changes
  – Factors –$p_u(t)$– are expensive to model
  – Gain flexibility by heavily parametering the functions

1. User Rating Behavior Exploration

The factors of interpersonal interest similarity W∗u,v and personal interest Q∗u,i proposed in have been proved effective. Thus, in this subsection, we turn to the details of our proposed interpersonal rating behavior similarity and interpersonal rating behavior diffusion.

2. Interpersonal Rating Behavior Similarity:

The behavior habit is essential. It could not be separated from temporal information. Thus, we define rating behavior in this paper as what the user has done and when it happened. This kind of behavior presentation arouses us to the curriculum schedule. The schedule arranges which course would we take and when we should go to class.

3. Interpersonal Rating Behavior Diffusion:

We consider the factor of social users' rating behavior diffusions. We explore the diffusion of user rating behavior by combining the scope of user's social network and the temporal information of rating behaviors. For a user, we split his/her social network into three components, direct friends, mutual friends, and the indirect friends.

4. Impact of Predicted Integer Ratings:

The predicted ratings are decimal; we discuss the impact of predicted integer ratings on performance. The ratings user rated are all discrete values ranging from 1 to 5. But the predicted results of matrix factorization model are all decimals. Thus, it is necessary to discuss the impact of integer predicted ratings. We round decimal ratings we predicted into discrete integers.

5. Yelp Dataset:

Yelp is a local directory service with social networks and user reviews. It is the largest review site in America. Users rate the businesses, submit comments, communicate experience, etc. It combines local reviews and social networking functionality to create a local online community. Yelp dataset4 contains eight categories, including Active Life, Beauty & Spas, Home Services, Hotels & Travel, Night Life, Pets, Restaurants, and Shopping.

LOCAL TRUSTEE SELECTION STRATEGIES

For a user u, a local trustee selection strategy essentially computes a score s(v, u) for each friend v of u and then selects my friends with the highest scores as u's trustees.

T-Random: As a baseline, T-Random assigns a random number ranging from 0 to 1 as the score s(v, u).

T-CF: As was shown by the number of common friends of two users is an informative indicator about the level of trust between them. Thus, one speculation is that a user might select friends with which he or she shares many common friends as trustees. To quantify the security of this speculation, we design the strategy T-CF (i.e.,T-Common Friends), which uses the number of common friends shared by u and his or her friend v as the scores

$$(v,u) = [T(v) \bigcap T(u)].$$

However, there are two drawbacks of T-CF. First, the fact that u shares many friends with a popular user v doesn't necessarily mean that u and v have a high level of trust because it is normal for many friends of u to be in v's friend list. Second, if a common friend of u and v is a popular user, then sharing him or her doesn'tnecessarily indicate a high level of trust between u and v. Next, we introduce two strategies to overcome the two drawbacks, respectively.

T-JC: To overcome the first drawback of T-CF, we design the trustee selection strategy T-JC (i.e., T-Jacquard Coefficient), which uses the Jacquard Coefficient [61] of the two sets T(u) and T(v) as the scores$s(v,u)$, i.e.,

$$s(v,u) = T(v) = \frac{\mathrm{T(v)\cap T(u)}}{\mathrm{T(v)\cup T(u).}}\text{. ...(2)}$$

T-AA: To overcome the second drawback, we design the T-AA (i.e., T-Adamic Ada) strategy, which uses Adamic-Ada similarity between u and v as the score s(v,u). Adamic-Ada similarity penalizes each common friend by its popularity (i.e., the number of friends). Formally, we have

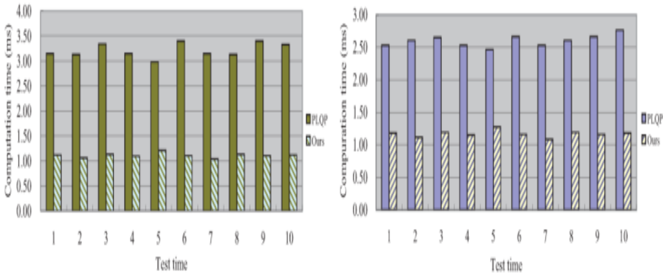
$$s(v,u) = \sum w€T(v) \cap T(u) \ldots (3)$$

T-Degree:, users could be those having large out degrees in the trustee network, and they could enable an attacker to compromise many other users. Thus, we propose the T-Degree strategy to minimize the maximum out degree in the trustee network. Intuitively, T-Degree constrains that no users are selected as trustees by too many other users.

Algorithm 2 shows our T-Degree strategy. T-Degree selects trustees for users one by one. For each user u that has adopted the trustee-based social authentication service, T-Degree selects his or her $m_u$friends who's current out degrees in the trustee network are the smallest as u's trustees; ties are broken uniform at random.

V. EVALUATION RESULT

The PLQP is a suit of protocols supporting privacy-preserving LBS in mobile application. It has high efficiency and achieves fine-grained control by exerting the CP-ABE scheme, which is similar to our work. Thus, in this section, we will compare our scheme with the PLQP scheme for evaluating the performance of our proposed scheme. The algorithms are implemented using the Big Integer library on a Windows 8.1 system with Intel CORE i7-4500U CPU@2.40 GHz and 8.00 G RAM. We have 10 tests in this experiment. Additionally, in each test, we use 1000 pairs of random locations for the publisher and the querier, respectively. We present the average results for each test in the following figures.It shows the detailed time cost for once location distance compute and location distance compare, respectively. It is obvious that the time cost at the publisher is always zero,

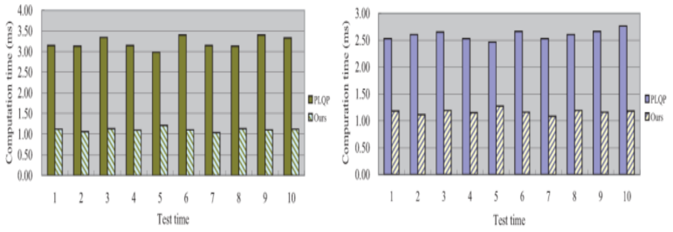


(a) Location distance compute (b) Location distance compare

Fig : distance compute and location distance compare

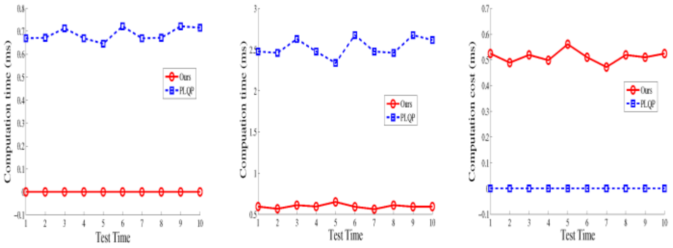
The comparison results of the total time cost for the aforementioned two operations, respectively. It can be seen that our scheme is much more efficient than PLQP. shows the comparison results of the detailed time cost for the aforementioned two operations at the publisher, querier and mobile cloud, respectively. To be more clear, we also present the comparison results in. From these figures, we get three points:

- At the querier, the time cost in our scheme is much less that that in PLQP.
- At the publisher, the time cost in our scheme is zero.
- At the mobile cloud, the time cost in PLQP is zero



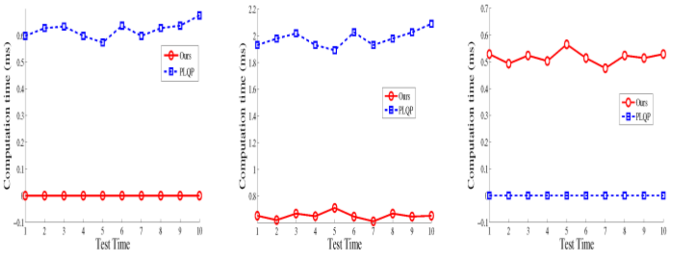
(a) Location distance compute (b) Location distance compare

Fig : The comparison of each entity's time cost between our scheme and PLQP



(a) At the publisher (b) At the querier (c) At the cloud

Fig: The time comparison of performing location distance compute between our scheme and PLQP



(a) At publisher (b) At querier (c) At cloud

Fig: The time comparison of performing location distance compare between our scheme and PLQP

In our system, the publisher can authorize the queries that he/she knows or not, such as his/her friends or someone who has similar interests. Hence, the queries may include attackers. If so, it is easy for the attacker to get a certain plaintext/ciphertext pair. Thus, our scheme has to be secure against the chosen plaintext attack. Next, we will prove it

Conclusion

In this Paper , here propose a user-service rating prediction approach by exploring users' rating behaviors with considering four social network factors: user personal interest (related to user and the item's topics), interpersonal interest similarity (related to user interest), interpersonal rating behavior similarity (related to users' rating habits), and interpersonal rating behavior diffusion (related to users' behavior diffusions). A concept of the rating schedule is proposed to represent user daily rating behavior. The similarity between user rating schedules is utilized to represent interpersonal rating behavior similarity. The factor of interpersonal rating behavior diffusion is proposed to deep understand users' rating behaviors. We explore the user's social circle, and split the social network into three components, direct friends, mutual friends, and the indirect friends, to deep understand social users' rating behavior diffusions. These factors are fused together to improve the accuracy and applicability of predictions. We conduct a series of experiments in Yelp and Douban Movie datasets. The experimental results of our model show significant improvement.

Future work

To further enhance the recommendation, check-in behaviors of users will be deeply explored by considering the factor of their multi-activity centers and the attribute of POIs.

REFERENCES

1. K. Mao, L. Shou, J. Fan, G. Chen, and M. Kankanhalli, "Competencebased song recommendation: Matching songs to one's singing skill," IEEE Trans. Multimedia, vol. 17, no. 3, pp. 396–408, Mar. 2015.
2. R. Keshavan, A. Montanari, and S. Oh, "Matrix completion from noisy entries," J. Mach. Learn. Res., vol. 11, pp. 2057–2078, 2010.
3. Q. Liu, E. Chen, H. Xiong, C. Ding, and J. Chen, "Enhancing collaborative filtering by user interest expansion via personalized ranking," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 42, no. 1, pp. 218–233, Feb. 2012.
4. Y. Chen and J. Canny, "Recommending ephemeral items at web scale," in Proc. SIGIR, 2011, pp. 1013–1022.
5. M. Harvey, M. J. Carman, I. Ruthven, and F. Crestani, "Bayesian latent variable models for collaborative item rating prediction," in Proc. CIKM, 2011, pp. 699–708.
6. X.-W.Yang, H. Steck, andY. Liu, "Circle-based recommendation in online social networks," in Proc. KDD, 2012, pp. 1267–1275.
7. Y. Zhou and L. Liu, "Social influence based clustering of heterogeneous information networks," in Proc. KDD, 2013, pp. 338–346.
8. H. Gao, J. Tang, X. Hu, and H. Liu, "Exploring temporal effects for location recommendation on location-based social networks," in Proc. RecSys, 2013, pp. 93–100.
9. X. Qian, H. Feng, G. Zhao, and T. Mei, "Personalized recommendation combining user interest and social circle," IEEE Trans. Knowl. Data Eng., vol. 26, no. 7, pp. 1763–1777, Jul. 2014.
10. K. Lee and K. Lee, "Using dynamically promoted experts for music recommendation," IEEE Trans. Multimedia, vol. 16, no. 5, pp. 1201–1210, Aug. 2014.
11. Z. Wang et al., "Joint social and content recommendation for user generated videos in online social network," IEEE Trans. Multimedia, vol. 15, no. 3, pp. 698–709, Apr. 2013.