Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

TRACING PRIVACY PRESERVING SERVICE LOCATION RECOMMENDATIONS BASED ON USAGE HISTORY FACTORIZATION

[1]k.Selvarani [1], [2]Dr.A.Annadhason
Department Of Computer Applications,
Alagappa University,
Karaikudi, Sivagangai (District),
Tamilnadu, India

Abstract

With the depth study and extensive application are social networks location-based (LBSNs), The new platform social to promote their services and products they are utilizing more businesses, In this paper, The distributing items with business information or the leaflets are explore an important technique that can help business to promote their locations of the business at some locations. Although CF-based Web service QoS prediction methods performs significant improvement. QoS methods seldom consider personalized influence of users and services when measuring the similarity between users and between services. Secondly, QoS factors, response time and throughput, usually depends on the locations of Web services and users. In the location promotion benefit is an order to maximize , this paper defines is a location-based social on network scope maximization problem in location influence , i.e., given a target business and an LBSN, the problem is set of K are find the locations, where the business distributes small promotional gifts or leaflets on, such that people who visited these locations can successfully propagate the advertisement information to most other locations for attracting most people to visit the target location. The existing related researches neglect location influences studies on location promotion (outdoor marketing). And it is challenging more to derive the influence between locations and the spatial influence scope of each location, since location influence depends on user's mobility and the target location. In this paper, provide a new approach (called as Loup) to location promotion between exploit influence locations. The First, lope correlations incrementally mines between instruct to the location graph (LG). Then centrality betweenness based on scope and lope predicts each location's its influence and influence on others, Finally, the lazy algorithm provide to efficiently a top-K find set of influential locations for the business. The datasets two real LBSN is an Extensive experiments based have verified, the effectiveness superior location promotion are our proposed method.

Keywords: QoS (Quality of Service), Web service recommendations, Location Graph (LG), Collaborative Filtering (CF), User Filtering, Privacy Preserving Protocol, and Cryptographic Framework.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

I. INTRODUCTION

With the wireless communication is a rapid developments, mobile devices and positioning technologies, gaining tremendous in Location-Based Services they are popularity , past few years are mobile user [1],[2],[3],[4].In LBS, users can obtain his current location by his Smartphone with GPS quilted in, then they send the query with his location to LBS server. With the help of LBS server, users can find Points of Interests (POIs) nearby, such as finding nearest restaurant, asking for taxi service, obtaining just-in-time coupons.

Collaborative Filtering (CF) is widely employed to recommend high quality Web services to service users. Based on the fact that a service user may only have invoked a small number of Web services, CF-based Web service recommendation technique focuses on predicting missing QoS values of Web services for the user [9]. Employing CF technologies, Web services with optimal QoS can be identified and recommended to the user. The effectiveness of CF-based Web service recommendation is usually represented by the prediction accuracy, which measures the deviation of the real QoS value and the predicted QoS value of a Web service.

However, when users enjoy the great convenience and entertainment from LBSs, they may confront privacy risks of sensitive information leakage. By collecting the queries submitted, such as his home location, health condition and even behavior pattern [5]. What's worse, LBS server may disclose users' private information to third party for pecuniary advantage, which may become the serious threat. Therefore, the privacy problem in LBSs is becoming increasingly prominent and needs to be solved. To the risk reduce of privacy disclosure. For example, et al. in [9] proposed using the third party trusted-fully model are using spatial cloaking algorithm. Figure 1 system architecture are depicts of TTP. The TTP main task is a the exact location are track of blurring a user's querying and all users, exact location in cloaked region, so that the cloaked region including other users $(K-1)$ at least can satisfy K-anonymity [10],[11],[12] ,their exact location information are all users report to the TTP, which becomes attackers are an attractive target. If the TTP server is compromised on attacker, it will pose the jeopardy on user information. (2) The TTP server will be the the

[1]K.SELVARANI [1], [2]Dr.A.ANNADHASON

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

performance bottleneck and failure in central point, because go through the all submitted queries. (3) It is difficult to find a third party that can be fully trusted.

Figure 1. The Architecture of TTP

To overcome the defects of TTP, some approaches are proposed for preserving location privacy LBSs based on centralized architecture. Peng et al. [13] proposed a scheme Location- Enhanced Privacy-Preserving (ELPP) for protection of users' location privacy in LBS. in [14] proposed a dynamic privacy grid system for preserving privacy in continuous LBS. Their scheme only third party semi-trusted are requires that responsible in carrying out some matching operations, and the user exact location are doesn't know the third party. However, user's query when the is too small spatial region and only one user includes, the LSP may the true user deduce, which will increase the user's privacy exposure. Inspired by the work in [14], we propose an enhanced location privacy through User-Defined Grid (DG) scheme in LBSs to the above-mentioned problems solve. The technology K-anonymity are our scheme adopts, combines with the user defined grid that improves user's location privacy. When service is a query request are sends a user, he firstly looks X other users for $(K - 1)$ in his surroundings. Then they specify query spatial region respectively, and two coordinates, which can determine every specified query spatial region, are encrypted by OPSE. Finally, the service user forwards it to anonymizer which cloaked region a forms, and sends to tell server for query. In the process of query, the anonymizer only some simple carries out comparison and matching operations,

1.1. THE SYSTEM MODEL AND DEFINITION

In this section, we first depict the location privacy preserving framework based on user-defined grid, then we provide the attack model. Finally, we define some basic notions. System Architecture Figure 1. The architecture of DG In this paper, an privacy preserving enhanced location approach through grid in

user-defined LBS, which combines the improve the user's privacy are OPSE. The DG scheme supports snapshot or queries continuous range for user. The architecture are made up of three main entities: service user, anonymizer and LBS server, which is shown (see Figure 1) and works as follows:

(1) The service user firstly specifies a query area, which is divided into equal-sized grid cells based on the grid structure specified by him. Then he specifies the range gets the grid cell identifiers of the spatial region query. At the same time, the service user looks for (K − 1) other users around him, and specify the query spatial region respectively, and two coordinates, which can determine every specify query spatial region, are encrypted by OPSE. Then the service user puts it into the request message .Finally, the service user sends the encrypted identifiers and query request to anonymizer.

(2) The anonymizer compares then cryptic coordinates and forms cloaking region based on K-anonymity, then the two encrypted coordinates which can determine this cloaking region are updated to request message, and anonymizer forwards the query request to LBS server.

(3) The LBS server searches the POIs of the service user within the cloaking region from its database, which can the encrypted identifiers of this candidate POIs and return it to anonymizer.

(4) The anonymizer matches the encrypted identifiers along with the POIs with the service user needs, and returns it to the user side. Finally, the service user filters the candidate result set and gets the accurate result.

1.2. THREAT MODELS

The threat model, the service user the communication channel between and the anonymizer is assumed to be secured. The existing security and solutions conventional (e.g., cryptography and hashing) can be used to protect the secrecy and integrity of the information through network [15], [16]. A common adversary can be thought that eavesdrops on as an entity wireless channel between the anonymizer and LBS server, or a who has attacker compromised the anonymizer or LSP.

1.3. WEAK ADVERSARY ATTACK MODEL

The weak adversary has little knowledge about the service user. It is only an adversary that can wiretap the insecure wireless channel. Eavesdroppers are usually local, short-term and passive because of their status features and limited resources.

1.3.1. Strong Adversary Attack Model

The strong adversary has more power than the weak adversary. At the worst case, the LSP or anonymizer may be compromised by the making profits, so they are considered as strong adversary.

1.3.2. Order-Preserving Symmetric Encryption

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

An OPSE is a deterministic symmetric encryption scheme whose encryption algorithm produces cipher texts that preserve numerical ordering of the plaintexts [17]. The concept of OPSE was proposed in the database community by Agrawal et al. [18], which supports efficient encrypted data on range queries. However, the first formal cryptographic treatment of OPSE did not appear until recently. In the paper by Boldyreva et al. [19], the authors give the first cryptographic study of OPSE primitive and provide a construction that is provably secure under the security framework of pseudorandom function or pseudorandom permutation, and the OPSE scheme from [19] has received attention from the applied community.

II.METHODOLIGIES

2.1. OVERVIEW

The only focus spatial queries on range. For example, the service users query the hotels, restaurants or them within 1 kilometer cinemas around. The summary of used notations in the architecture of UDG is shown in Table Before the service in the grid-based solution, the query area is divided the equalized grid cells. The shape of the grid cell can be either a square or a rectangle but all of them must cover the whole query area. The area query is assumed to be a rectangular areas server on user query requests, query area the system specifies a, larger area is usually, such as the city of size. The service user is not required to be at the center of the query area necessarily. Instead, its location can be anywhere in the area. .

2.2. THE QUERY REQUEST

After the service user defines the grid structure, he specifies the query range with the radius of *R* on it, and we can get the spatial region query that is the spatial region of grid cells in the grid structure is a defined- user that intersect the query range. Then obtain the identifiers of grid cells in query spatial region.

2.3. SEARCH

The LBS server obtains the request message *MSGA*2*S* and decrypts the *EPKS* (*Query*, *Key*, *Grid structure*) with its private key *SKS*, which can get the *Query*, *Key* and *Grid structure*. The same time, he decrypts the *C Region* with the key *KOPSE*, then the cloaking region in the user-defined grid structure is established. And gets *t* POIs. If the location of the *j*et POI is (*Xu, in*) ($1 \leq j \leq t$), the LBS server computers

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

the identifier of the grid cell in the cloaking region and the LBS server computes the following: where *H* () is a hash function, and *Enki* () is a symmetric encryption function under the *Key*.

2.4. COORDINATE COMPARISON

When anonymizer receives the query request message *MSGU2A* from the service user, it firstly stores the set of encrypted identifiers *Se*. Then it will obtain the encrypted coordinate pairs *RI* from the *Region* and compare this encrypted coordinates respectively, coordinate values, *Encase*(*xi*1)*min*, *Encase*(*yj*1)*min*, *Encase*(*xm*2)*max* and *Encase*(*yn*2)*max* (*is, j, m, n* ∈(0, (*K* − 1))) from the axis X and the axis Y respectively, comparing In the process , the does not anonymizer specific location recognize of the encrypted e users, by OPSE.

2.5. IDENTIFIER MATCHING

When receiving the POIs along with their encrypted identifiers, the anonymizer determines the matching POIs set of by the encrypted are comparing identifiers *job*($1 \le j \le t$) of the received POIs with the encrypted set of identifiers *Se* received previously from the service user. If *job* matches the *qi* in *Se*, it indicates that the *Poi* in the grid cells is required by the service user. Thus, the anonymizer forwards every matching *Poi* to the service user. The message forwarded *MSGA2U* to the service user by anonymizer.

III.RESULT COMPUTATION

The service user receives the query results information *MSGA2U* forwarded from anonymizer. For each of these matched *Poi* = (*job, elk, job*), the service user decrypts *elk* using the *KL* and gets access to the exact location (*Xu, in*) of the POIs. For the (*Xu, in*) and *job*, he verifies *job* by recalculating the hash value of *job* and *elk* and compares it against *job*

If they are matched, it indicates that the location of POIs has tampered in transition. Then the service user gets the results, which the POI whose location includes is within a distance of *R* of the service user's current position (*x*0, *y*0).

3.1. PERFORMANCE ANALYSIS

We have conducted to evaluate the set of experiments performance of our protocol. Since is a PPP (privacy preserving protocol) is mostly on our focus, we present the performance in- terms of running the computations on cipher texts, decryption and size of data transmitted among different parties. However, since a new-found way of grouping users present by computing their geographical separation, we show enough experimental evidence that users who are similar based on QoS experiences, are actually closely located. Our experimental analysis as follows organized. First, we analyze the communication complexity and computation for each stage of our protocol. The latitude and longitude is a locations provided important: that, in our experiment, we only use RTT (response time) to test the performance of our protocol. Finally, we present the correlation between QoS similarity and user proximity. More specifically, we address and analyze the following points.

- The computation and communication complexity of the overall protocol
- Correlation between users' geographical locations and their similarity based on QoS values.
- Performance evaluation of the protocol in-computation of terms and communication costs and impact of T, n, n`, m and m`on performance.

The experiments to conduct , Java 2 SE 8 we use including libraries cryptographic on a hardware platform with windows 7 OS 3.6 GHz- core i7 , 64 bit and and 8GB CPU unit. For the performance measurement, the metrices we considered in our experiment are shown.

3.1. Computation Complexity

In below we present the computation cost of our protocol in terms of user filtering, initialization, similarity computation on filtered users and Web Service recommendations. Represents the complexities in terms of user filtering and the complexities of initialization, similarity and recommendation protocols respectively

3.2. User Filtering

Filtering nearby users two stages is a consists: firstly, distance computation between QU and other n users and secondly, the distance threshold based on nearby users filtering.

3.3. Web Service Recommendations

In the initialization of generating Web Service recommendations, all users including QU encrypt their QoS experiences and more related information. According to step 1 of algorithm 3, the users from set n encrypt four different information for all Web Services m, which takes 4m (e) seconds.

3.4. Communication Complexity

3.4.1. User filtering

In step 1 of algorithm 1, the QU broadcasts three different cipher texts which are 3l bits in size to user k. However, user k is just one user from set of n users and the cipher texts are need to be sent to all of them to compute their distances.

3.4.2. Web Service Recommendations

According to step 2 of algorithm 3, all users n send four different cipher texts for m Web Services to RS which are of 4lm bits. The QU also sends two cipher texts for m number of webs services to RS. Therefore, the complexity communication of QU, all users and RS becomes 2lm, 4lm and 4lmn + 2lmn bits respectively.

3.4.3. Correlation between Geographical Locations and QoS based Similarities

That there exists a correlation between users' locations and their QoS based similarity. However, location their assumptions unlike, we use users' experimentally and geographical locations the evidence also provide enough that users' geographical locations are indeed related with their QoS based similarities. To evaluate this relationship we group the based on their distances by user with QU based on different distance thresholds.

3.4.4. Efficiency

To check the efficiency of our protocol in terms of different stages, we randomly chose one user as the query user (QU) and find the time required to filter the nearby users, initialization, similarity computation and, finally, predicting missing QoS values in a privacy-preserving manner. We also present the required time to perform a discrete logarithm for decryption. More specifically, we choose one user who is located in USA according to its geographical location. Note that we need to provide a threshold TXs for user filtering. That we need to provide a threshold T×s for user filtering. In our experiment, we choose the distance threshold T ×s as 8:5 ×105, where T = 85 and s=104 and found that there are 102 users located within this threshold region. Based on these parameters, we discuss the performance of our methods in below. The computation and communication costs of the target user and all other users in terms of distance computation and filtering nearby users.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

Table 3.1. Computation and Communication Cost

		Initialization	***Similarity***	***Recommendation***
Computation Cost	*QU*	*0.47s*	*15.26s*	*n/a*
	Other users	*0.23s*	*n/a*	*n/a*
	PS	*n/a*	*n/a*	*100s*
	RS	*n/a*	*n/a*	*0.08s*
Communication Cost	*QU*	*1.5MB*	*252.7MB*	*0.3MB*
	Other users	*2.9MB*	*n /a*	*n/a*
	PS	*10^3MB*	*76MB*	*0.125MB*
	RS	*n/a*	*n/a*	*0.125MB*

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 13,January 2023

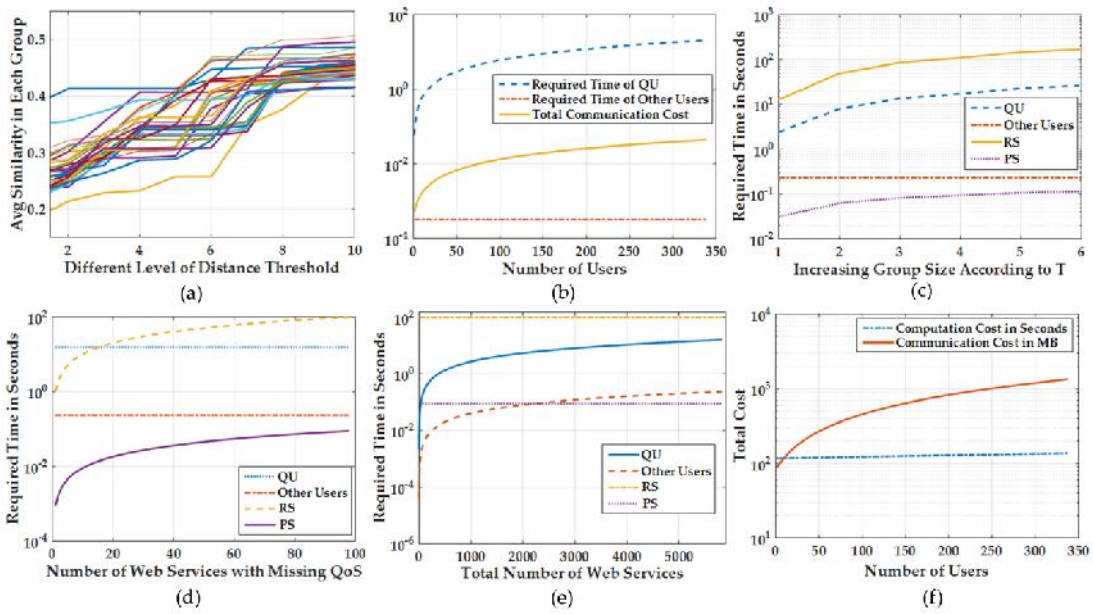

Fig. 3. (a) Correlation between QoS based similarity and user locations. (b) Computational cost in-terms of number of total users n = 338. (c) Impact of distance threshold T on computational cost. (d) Impact of the number of Web Services with missing QoS m0 on the performance. (e) Impact of total number of Web Services in the system m on performance. (e) Overall scalability of the system while n = 338, m = 5825, n n0 = 102 and m0 = 98

In this setting, the number of total users for initialization and similarity computation is n = 338, the number of total web services is m = 5825 and the number of nearby filtered users is n-n0 = 102. For predicting the missing QoS values, we found that there are m0 = 98 web services for the chosen QU, who has not previously invoked the 98 Web Services. At the initialization phase, only the users participate and perform some encryption operations locally where the QU and the user k take 0:47 seconds and 0:23 seconds respectively. Here the cost of user k is shown only for one user from n set, since they can compute the operations in parallel. During the similarity computation, only QU participates and computes the similarity with other nearby users based on encrypted QoS values (n - n0 = 102), which takes 15:2 seconds. To predict one missing QoS, the RS takes about 1:02 which results 100 seconds to predict 98 Web Services. The PS takes about 0.08 seconds to decrypt the 98 resultant cipher texts of QoS predictions. The memory size required for users is very small for both QU and other users, which are 1:5 MB and 2:9MB respectively. To predict one missing QoS, the RS

takes about 1:02 which results 100 seconds to predict 98 Web Services. The PS takes about 0.08 seconds to decrypt the 98 resultant cipher texts of QoS predictions. The computation does not affect cost of other users. Figure 3(b) presents the scalability of user filtering protocol in terms of computation and communication cost with increasing the total number of users n in the system.

IV. CONCULSION

The paper propose a cryptographic framework to preserve users privacy while predicting QoS values missing and web service recommendations are providing. And never propose a new protocol to efficiently compute the distances among the users and sorting a subset of users based on their encrypted locations. Unlike existing works, we conduct the experimental analysis on user's geographical locations for the first time the field of Web Service recommendations. Our privacy and experimental analyses show the effectiveness of our protocol. In future, we are interested in analyzing and solving more privacy issues in Web Service recommendations and improving the efficiency by developing this research through distributed and parallel recommendation system.

REFERENCES

[1] L.-J. Zhang, H. Cai, and J. Zhang, Services computing. Springer, 2007.

[2] V. Nikolaenko, S. Ioannidis, U. Weinsberg, M. Joye, N. Taft, and D. Boneh, "Privacy-preserving matrix factorization," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 801–812.

[3] S. Badsha, X. Yi, I. Khalil, and E. Bertino, "Privacy preserving user based recommender system," in Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017, pp. 1074–1083.

[4] G. Kang, J. Liu, M. Tang, X. Liu, B. Cao, and Y. Xu, "Awsr: Active web service recommendation based on usage history," in Web
Services (ICWS), 2012 IEEE 19th International Conference on. IEEE, 2012, pp. 186–193.

[5] L. Liu, F. Lecue, and N. Mehandjiev, "Semantic content-based recommendation of software services using context," ACM Transactions on the Web (TWEB), vol. 7, no. 3, p. 17, 2013.

[6] L. Shao, J. Zhang, Y.Wei, J. Zhao, B. Xie, and H. Mei, "Personalized qos prediction for web services via collaborative filtering," in Web Services, 2007. ICWS 2007. IEEE International Conference on. IEEE, 2007, pp. 439–446.

[7] Z. Zheng, H. Ma, M. R. Lyu, and I. King, "Wsrec: A collaborative filtering based web service recommender system," in Web Services, 2009. ICWS 2009. IEEE International Conference on. IEEE, 2009, pp. 437–444.

[8] "Qos-aware web service recommendation by collaborative filtering," IEEE Transactions on services computing, vol. 4, no. 2, pp. 140–152, 2011.

[9] "Collaborative web service qos prediction via neighborhood integrated matrix factorization," IEEE Transactions on Services Computing, vol. 6, no. 3, pp. 289–299, 2013.

[10] Q. Yu, Z. Zheng, and H. Wang, "Trace norm regularized matrix factorization for service recommendation," in Web Services (ICWS) 2013 IEEE 20th International Conference on. IEEE, 2013, pp. 34–41.

[11] J. Liu, M. Tang, Z. Zheng, X. F. Liu, and S. Lyu, "Location aware and personalized collaborative filtering for web service recommendation," IEEE Transactions on Services Computing, vol. 9,. 5, pp. 686–699, 2016.

[12] X. Chen, Z. Zheng, Q. Yu, and M. R. Lyu, "Web service recommendation via exploiting location and qos information," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1913–1924, 2014.

[13] M. Tang, Y. Jiang, J. Liu, and X. Liu, "Location-aware collaborative filtering for qos-based service recommendation," in Web Services (ICWS), 2012 IEEE 19th International Conference on. IEEE, 2012, pp. 202–209.

[14] W. Xu, V. Venkatakrishnan, R. Sekar, and I. Ramakrishnan, "A framework for building privacy-conscious composite web services," in Web Services, 2006. ICWS'06. International Conference on. IEEE, 2006, pp. 655–662.

[15] A. Squicciarini, B. Carminati, and S. Karumanchi, "A privacy preserving approach for web service selection and provisioning," in Web Services (ICWS), 2011 IEEE International Conference on. IEEE, 2011, pp. 33–40.

[16] S.-E. Tbahriti, M. Mrissa, B. Medjahed, C. Ghedira, M. Barhamgi, and J. Fayn, "Privacy-aware daas services composition," in International Conference on Database and Expert Systems Applications. Springer, 2011, pp. 202–216.

[17] S.-E. Tbahriti, C. Ghedira, B. Medjahed, and M. Mrissa, "Privacy enhanced web service composition," IEEE Transactions on Services Computing, vol. 7, no. 2, pp. 210–222, 2014.

[18] J. Zhu, P. He, Z. Zheng, and M. R. Lyu, "A privacy-preserving qos prediction framework for web service recommendation," in Web Services (ICWS), 2015 IEEE International Conference on. IEEE, 2015, pp. 241–248.

[19] S. Badsha, X. Yi, and I. Khalil, "A practical privacy-preserving recommender system," Data Science and Engineering, vol. 1, no. 3, pp. 161–177, 2016.

[20] S. Badsha, X. Yi, I. Khalil, and A. Kelarev, "Private recommendations generation for vertically partitioned datasets," 2017.

[21] S. Badsha, X. Yi, I. Khalil, D. Liu, S. Nepal, and E. Bertino, "Privacy preserving location recommendations," in International Conference on Web Information Systems Engineering. Springer, 2017, pp. 502– 516.

[22] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1053–1066, 2012.

[23] P. Paillier et al., "Public-key cryptosystems based on composite degree residuosity classes," in Euro crypt, vol. 99. Springer, 1999, pp. 223–238.

[24] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on cipher texts," in Theory of Cryptography Conference. Springer, 2005, pp. 325–341.

[25] X.-Y. Li and T. Jung, "Search me if you can: privacy-preserving location query service," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2760–2768.

[26] Z. Zheng, Y. Zhang, and M. R. Lyu, "Distributed qos evaluation for real-world web services," in Web Services (ICWS), 2010 IEEE International Conference on. IEEE, 2010, pp. 83–90.