Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Generating Location Aware Recommendations Using Homomorphic Encryption and Spatial Queries

[1]A. Indhumathi, [2]J. Sudha
[1]PG Student, Department of CSE, [2]Associate Professor, Department of CSE
[1, 2] AVC College of Engineering, Mayiladuthurai, Tamil Nadu, India

Abstract--- People use social networks to get in contact with further people, and create and distribute content that includes personal information, images, and videos. The service providers have right of access to the content provided by their users and have the right to process collected data and allocate them to third parties. A very regular service provided in social networks is to generate recommendations for ruling new product using collaborative filtering techniques. The data essential for the collaborative filtering algorithm is composed from various property including users' profiles and behaviours. To find services and products appropriate to a particular customer, the service provider processes collected user data like user preferences and click logs. In all of the above services and in many others, recommender systems based on collaborative filtering techniques that collect and process personal user data constitute an essential part of the service. Recent studies show that the privacy considerations in online services appear to be one of the most important factors that threaten the healthy growth of e- business. Therefore, it is important to maintain the privacy of the users of online services for the assistance of both individuals and business. Recommender systems have become an important tool for personalization of online services. Generating recommendations in online services depends on privacy-sensitive data collected from the users. Generating location aware recommendation, do not consider spatial properties of user nor items. Location aware recommender system uses location based rating to produce recommendation. Location aware recommendation exploits user rating locations through user partitioning, a technique that influences recommendations with ratings spatially close to querying users in a manner that maximizes system scalability while not sacrificing recommendation quality. Recommender system exploits item locations, a technique that favours recommendation candidates closer in travel distance to querying users in a way that avoids extensive access to all spatial items.

Keywords---Recommender system, spatial, Privacy, Service provider, Collaborative filtering, Homomorphic encryption.

I. INTRODUCTION

In the last decade, we have practiced unique progress in information and communication technologies. Cheaper, more powerful, less power consuming devices and high bandwidth communication lines enabled us to create a new virtual world in which people mimic behaviour from their daily lives without the restrictions imposed by the physical world. As a result, online applications have become very popular for millions of people. Personalization is a common approach to further improve online services and attract more users. Instead of making general suggestions for the users of the system, the system can suggest personalized services targeting only a particular user based on his preferences. Since the personalization of the services offers high profits to the service providers and poses exciting research challenges, research for generating recommendations, also known as collaborative filtering, attracts attention both from academia and industry. The techniques to generate recommendations for users powerfully rely on information gathered from the user. This information can be provided by the user himself as in profiles or the service provider can observe users' actions, such as click logs. On one hand, more customer information helps the system to improve the accuracy of the recommendations. On the other hand, the information on the users creates a strict confidentiality risk since there is no solid guarantee for the service provider not to misuse the users' data. It is often seen that whenever a user enters the system, the service provider claims the tenure of the information provided by the user and authorizes itself to issue the data to third parties for its own benefits. The need for privacy protection for online services, particularly those using collaborative filtering techniques[1], triggered research efforts in the past years. Among many different approaches, two main directions, which are based on data perturbation and cryptography. It means privacy-preserving collaborative forecasting[9] and benchmarking to enlarge the consistency of local forecasts and data correlations using cryptographic techniques.

In this paper, in addition to privacy preserving data [4] from service provider, recommender system also recommend location based rating to produce recommendation. It propose three types of location based rating in a single framework (1) Spatial ratings for non-spatial items, represented as a four-tuple (user, ulocation, rating, item), where ulocation represents a user location, for example, a user located at home rating a book; (2) non-spatial ratings for spatial items, represented as a four-tuple (user, rating, item, ilocation), where ilocation represents an item location, for example, a user

with unknown location rating a restaurant; (3) spatial ratings for spatial items, represented as a five-tuple (user, ulocation, rating, item, ilocation), for example, a user at his/her office rating a restaurant visited for lunch. Traditional rating triples can be classified as non-spatial ratings for non-spatial items and do not fit this taxonomy.

Recommender systems are usually classified into the following category, based on how recommendations are made:

1. Content-based recommendations: In Content-based recommendations, the user will be recommended items similar to the ones the user preferred in the past.
2. Collaborative recommendations: In this recommendation technique, the user will be recommended items that people with similar tastes and preferences liked in the past.
3. Hybrid approaches: In Hybrid approaches, collaborative and content-based methods are combined.

II. RELATED WORK

Location aware recommender system uses item –based collaborative filtering [7] as its primary recommendation technique, chosen due to its popularity and widespread adoption in commercial system.

A. Collaborative Filtering:

Collaborative Filtering (CF) [1] is frequently used in the E- Commerce area for producing recommendation for diverse products. CF is based on the statement that people with similar tastes prefer the same items. In order to generate a recommendation, CF firstly creates a neighbourhood of users with the top similarity to the user whose preferences are to be predicted. Then, it generates a prediction by calculating a normalized and weighted average of the ratings of the users in the neighbourhood. In CF, user profile is a feature- vector containing information about user preferences with respect to a set of item the user rated. For quite some time CF has been applied in E-Commerce and express recommendations of various kinds. Personalized information delivery in general and purchase recommendations (that applies collaborative filtering) in particular can increase the possibility of a customer making a purchase, compared to non-personalized approaches. However, personalization brings with it the issue of privacy.

B. Privacy Enhanced Recommender System:

Recommender systems are broadly used in online applications since they facilitate personalized service to the users. The primary collaborative filtering techniques job on user‘s data which are mostly privacy sensitive and can be misused by the service provider. To protect the privacy of the users, encrypt the privacy aware[2] data and generate recommendations by processing them under encryption. With this approach, the service provider learns no information on any user‘s preferences or the recommendations made. The method is based on homomorphic encryption schemes and secure multiparty computation (MPC) techniques.

C. Location Aware Recommendations:

Recommender system suggests k items personalized for a querying user u. However, capability to produce location-aware recommendations [6] using each of the three types of location-based rating within a single framework. Recommender system produce recommendations using spatial ratings for non-spatial items, i.e., the tuple (user, ulocation, rating, item), by employing a user partitioning technique that exploits preference locality. This technique uses an adaptive pyramid structure to partition ratings by their user location attribute into spatial regions of varying sizes at different hierarchies. Recommender system produces recommendations using non-spatial ratings for spatial items, i.e., the tuple (user, rating, item, ilocation), by using travel penalty, a technique that exploits travel locality. This technique penalizes recommendation candidates the further they are in travel distance to a querying user. The challenge here is to avoid computing the travel distance for all spatial items to produce the list of k recommendations, as this will really consume system resources. Travelling distance can be calculated by using latitude and longitude in google map based on the location of querying user. To produce recommendations using spatial ratings for spatial items, i.e., the tuple (user, ulocation, rating, item, ilocation) ,recommender system employs both the user partitioning and travel penalty techniques to address the user and item locations associated with the ratings.

III. PRIVACY-PRESERVING LOCATION BASED RECOMMENDER SYSTEM

Techniques for privacy preserving sensitive data of user from service provider is based on following method

A. Homomorphic Paillier:

- Retrieve messages.
- Generate public and secret key.
- Compute product of two large prime numbers.
- Generate a subgroup of order and random number.
- Apply paillier to encrypt the privacy sensitive data.

B. Homomorphic DGK:

- Generate the product of two large prime numbers.
- Check another pair of prime which are divisible
- Choose random integer.

- Perform look-up table operation.

C. Collaborative filtering:

- Select similar users.
- Compare with threshold value.
- Compute average rating of most similar users
- Apply rating for the users.

D. Generating recommendation:

- Service provider and PSP compute the similarity values
- Compare each similarity values with a public known threshold.
- Check the number of users with a similarity value above the threshold.
- Sum the ratings for users.

IV. IMPLEMENTATION DETAILS

Recent systems need active participation of user which becomes privacy risk. To conquer this problem eliminate the need for active participation of users using a semi trusted third party, that is the Privacy Service Provider (PSP), who is trusted to perform the assigned tasks properly, but is not allowed to examine the private data. Encryption and Decryption are doing using additive Homomorphic encryption algorithm such as paillier and DGK algorithm. Using this PSP users upload their encrypted data to the service provider and the recommendations are generated by using a collaborative filtering technique[4] between the service provider and the PSP, without interconnect with the users.

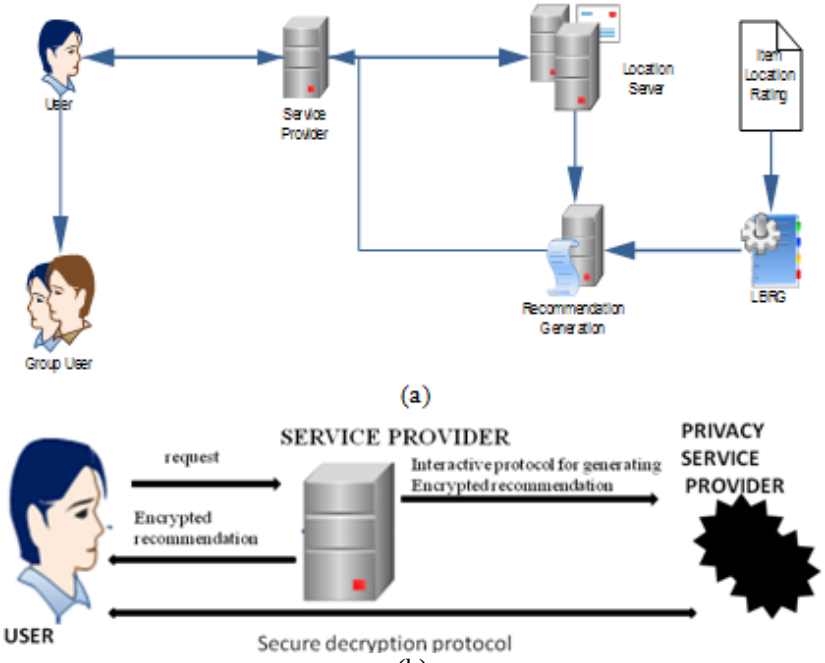

Fig. 1.System Model for Generating Recommendations. (a) Location Aware Recommender System, (b) Database Construction

A. Database Construction:

Before constructing database, system is computing the similarities between particular user and all other user. This similarity stored in vector V. To construct the encrypted database, the users encrypt their data before distribution them to the service provider using pailliar algorithm.

B. Service Provider Processing:

To find services and products suitable to a particular customer, the service provider processes collected user data like user preferences. Recommender systems based on collaborative filtering techniques that collect and process personal user data constitute an essential part of the service. The service provider receives the encrypted inputs of all parties. In this process, user send the query to the service provider (SP), SP forward the encrypted data to the privacy service provider.

C. Privacy Service Provider Processing:

The Privacy Service Provider (PSP) [2] is a semi trusted third party who has a business interest in providing processing power and privacy functionality. Privacy service provider receives the forwarded query and gets the key value pair. During the secure multiplication protocol, the service provider adds random values that are (the security parameter) bits longer than the actual ones. Finally PSP generate the decrypted number and decrypted query according to the user preference.

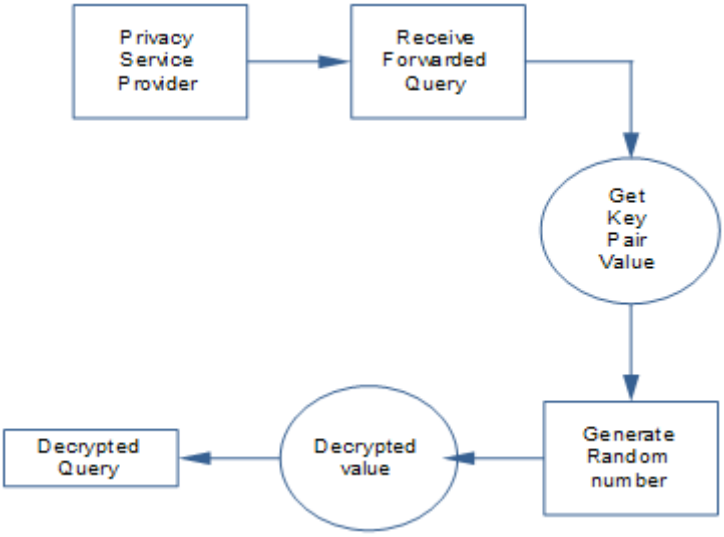

Fig. 2.Privacy Service Provider

D. User Query Processing:

Users are the customers of the service provider. Based on their preferences, in the form of ratings, the service provider generates recommendations for them. The goal of our protocol is to hide any piece of information that may harm the privacy of users. User does not learn any information other than the desired result, even if he colludes with the service provider or PSP. First, note that before the execution of the secure decryption protocol with the PSP in the end, user is no different from any other user (except for the role of its input). In particular, user has received no messages so he cannot know inputs of other users. User receives a fresh encryption from the service provider.

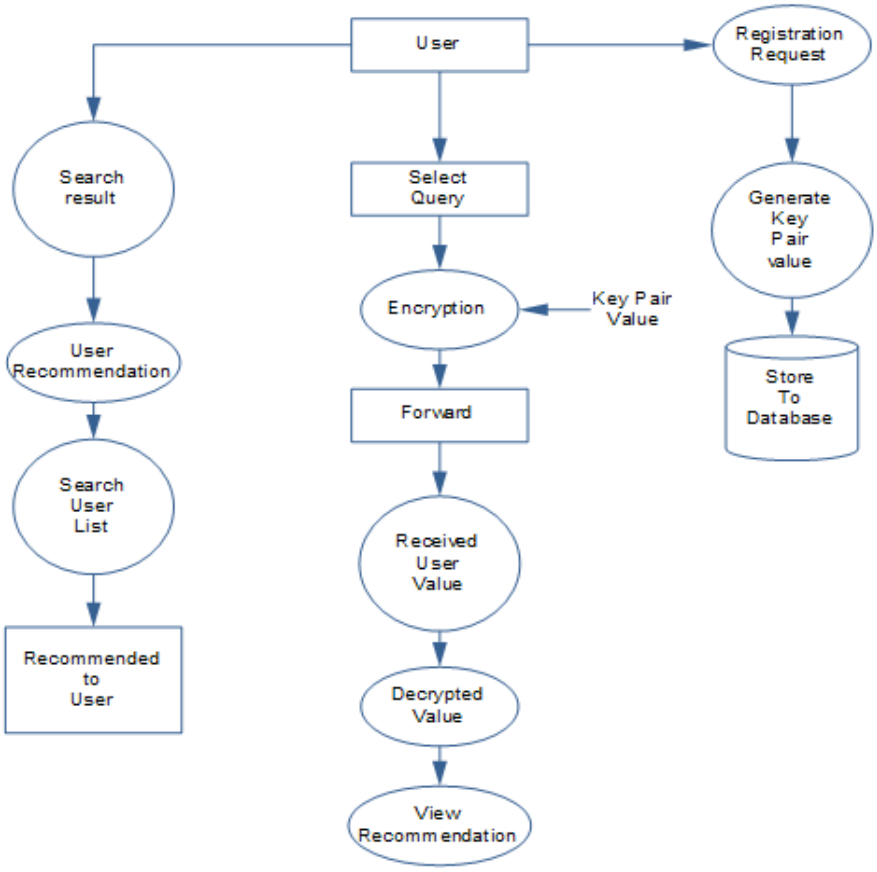

Fig. 3. User Data Processing

E. Generate Private Recommendation Based on Location:

To generate recommendations for a specific user, the PSP and the service provider initiate a cryptographic protocol using only the encrypted vectors received by the users. The service provider and the PSP compute the encrypted similarity values between user and all other users.PSP then generate recommendation by decrypting the received vector and apply collaborative filtering approach for finding similarity between that particular user and all other user based and also recommend item based on spatial queries.

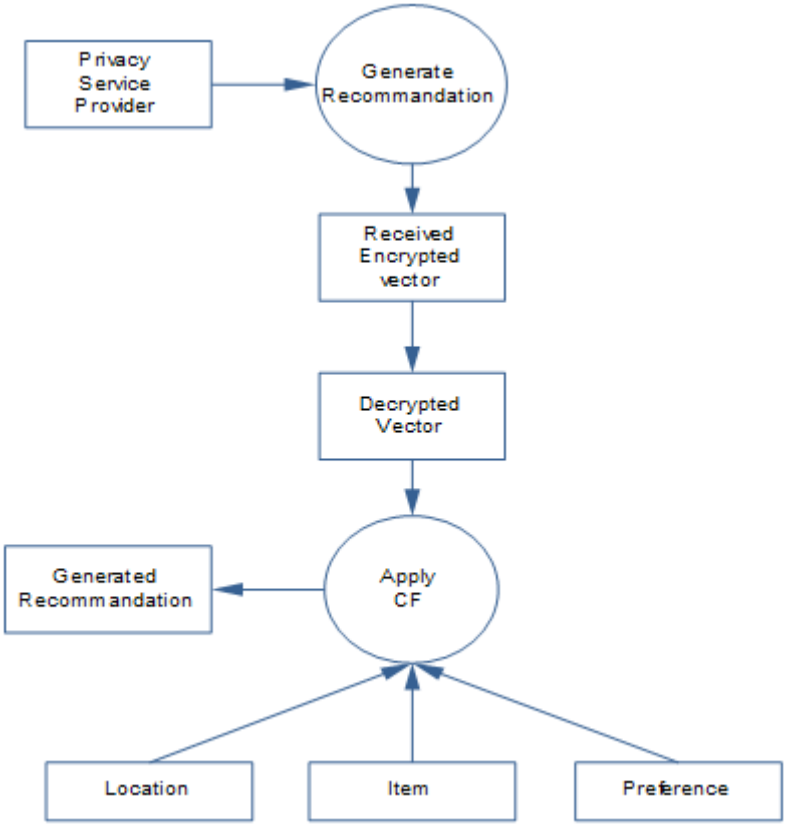

Fig. 4.Location Aware Recommendations

Algorithm:

1. Data from user
2. Encrypt the data using paillier encryption
   a. Choose a large prime s with 150 digits
   b. Choose two random integers $1 \leq g, x < s$
   c. Calculate $u = g^x \bmod s$
   d. Public key: s, g, u; private key: x
   e. Encryption of a data R : choose a random t and compute $a = g^t \bmod s$, $b = u^t R \bmod s$
   f. Cipher Text c= (c1, c2)
3. Send cipher text to service provider
4. Calculate Similarities between particular user with all other user
5. Send similarities to privacy service provider
6. Decrypt similarities

$$R = \frac{c_2}{c_1{}^x} \; mod \; s = c_2 \, c_1{}^{-x} \; mod \; s$$

7. Compute recommendation
   a. Finding similar users
   b. Computing the number L and sum of ratings of most similar users
   c. Computing Recommendation
8. Send recommendation to user.

V. CONCLUSIONS

To protect the privacy of the users, encrypt the privacy sensitive data and generate recommendations by processing them under encryption. With this approach, the service provider learns no information on any user's preferences or the recommendations made. The method is based on homomorphic encryption scheme. The system makes it possible for servers to collect private data from users for CF purposes without compromising users' privacy requirements. As a final point, provide recommendation of product based on location to the group of user. In future, proposed system can be expanded to a dynamic recommender system for various categories in real time environment

REFERENCES

[1] Casino, F. Domingo-Ferrer, J.; Patsakis, C.; Puig, D.; Solanas, A., "*Privacy Preserving Collaborative Filtering with k-Anonymity through Microaggregation*", e-Business Engineering (ICEBE), 2013 IEEE 10th International Conference on 11-13 Sept.

[2] Erkin, M. Beye, T. Veugen and R. L. Lagendijk, "*Privacy enhanced recommender system*," in Proc. Thirty-

First Symp. Information Theory in the Benelux, Rotterdam, 2010, pp. 35–42.

[3] F.McSherry and I. Mironov, "*Differentially private recommender systems: Building privacy into the net*," in Proc. 15th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining (KDD'09), New York,NY, 2009, pp. 627–636, ACM.

[4] H. Polat and W. Du, "*Privacy-preserving collaborative filtering using randomized perturbation techniques*," in Proc. ICDM, 2003, pp. 625–628.

[5] Hao Ji, Jinfeng Li, Changrui Ren, Miao He He "*Hybrid Collaborative Filtering Model for improved Recommendation*" 2013 IEEE.

[6] J. J. Levandoski, M. Sarwat, A. Eldawy, and M. F. Mokbel, "*LARS: A location-aware recommender system*," in Proc. ICDE, Washington, DC, USA, 2012.

[7] J. Konstan ,B. Sarwar, G. Karypis,, and J. Riedl, "*Item-based collaborative filtering recommendation algorithms*," in Proc. Int. Conf. WWW, Hong Kong, China, 2001.

[8] J. Bao, C.-Y. Chow, M. F. Mokbel, and W.-S. Ku, "*Efficient evaluation of k-range nearest neighbour queries in road networks*," in Proc. Int. Conf. MDM, Kansas City, MO, USA, 2010.

[9] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and J.-P. Hubaux, "*Preserving privacy in collaborative filtering through distributed aggregation of offline profiles*," in Proc. Third ACM Conf. Recommender Systems (RecSys'09), New York, NY, 2009, pp. 157–164, ACM.

[10] Z. Erkin, M. Beye, T. Veugen, and R. L. Lagendijk, "*Efficiently computing private recommendations*," in Proc. Int. Conf. Acoustic, Speech and Signal Processing (ICASSP), Prague, Czech Republic, May 2011, , pp. 5864–5867, 2011.

