Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Private Recommendation Based On Elgamal Homomorphic Encryption Scheme

Sapana Borole[*]
PG Student,
Department of Computer Engineering
Rajashri Shahu College of Engineering Tathawade
Pune , India

Prof. S. B. Javheri
Assistant Professor
Department of Computer Engineering
Rajashri Shahu College of Engineering Tathawade,
Pune ,India

Abstract— In recommender systems, online services access the user's profiles in order to generate useful recommendations. Depends on privacy perceptive data collected from the users, it generates recommendation in online services. Protecting the privacy of all participants is an essential requirement of the basic Information Filtering architectures, because the organize Recommender Systems have to be accepted by privacy-aware users as well as information and service providers. Data protection systems focus on access control and secure transmission which provide security against malicious third parties, but not the service provider. This produces a major privacy risk for the users. In this system, we aim to protect the confidential data of user against the service provider while protecting the functionality of the system. We recommend encrypting private data and process encrypted data to generate recommendations. In this paper, construct an extremely efficient system that does not require the active participation of the user by using a semi trusted third party. Existing private recommendation system uses Paillier encryption algorithm but system is more complex and inefficient. To overcome this drawback proposed system uses ElGamal algorithm. This system is efficient to generate private recommendations in a privacy-preserving manner.

Keywords— Collaborative filtering, Homomorphic encryption, Privacy, Privacy Service Provider (PSP), Recommender system.

I. INTRODUCTION

Many of people are accessing online services for daily activities which involve sharing personal information with the service provider. The example of such online services are social networks, online shopping, IP-TV. In social networks, people acquire in touch with other people, and also create as well as share data which includes personal information, images and videos. The provided contents of the user can be access by service providers and they have the right to build up the collected data and issue them to third parties. Collaborative filtering technique is to generate recommendations in social networks, a very common service is provided for finding groups, new friends and events. The techniques for generating recommendations for users strongly rely on the information gathered from the user. Collaborative filtering algorithm is collected data from different resources such as users' profiles and its behaviors. Also in online shopping, to find services and products appropriate for a particular user, collected user data similar to user preferences and click logs process by service provider.

It increases the possibility of a purchase by providing personalized suggestions to their customers. In web-based activities such as e-commerce, electronic retailers and product providers always offer a large number of products or content items which users are often enforced to choose from. The most important challenge in web based activity is matching consumers with most appropriate products and helps them in decision making process. It is helpful for recommendation system. A modified recommendation for products that suit a user's taste can not only enhance user satisfaction and loyalty, but also increase conversions and profits for electronic retailers. Internet leaders are increasingly adopting product recommendation engine for personalized recommendation, such as Amazon, Google, Netflix, TiVo and Yahoo. Recommender systems are flattering an extensive technology used to promote cross-selling. Collaborative filtering is the standards employed to offer users recommendations. Though most collaborative filtering methods require explicit user feedback, such as ratings, it is an entrenched fact that users rate only a small portion of all available products. Consequently, the rating system often acquires insufficient precise feedback which leading to disappointing recommendations.

Moreover, 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.[11]

II. Literature Survey

Polat use randomized perturbation (RP) technique which protects users' privacy during producing accurate recommendations. Anonymous techniques allow users to reveal their personal information without disclosing their identities but the major problem is that there is no guarantee on the quality of the dataset. so it propose a new scheme, in which each user first disguises his/her personal data, and then sends to a central place where as the data collector cannot derive the truthful information about a user's private information.[4] Distributed method for users to enhance their profiles and protect from an entrusted server, with minimum loss on the accuracy of the recommender system. It addressed the problem of protecting the users' privacy in the existence of an entrusted central server, where the server has direct access to users' profiles. To avoid privacy risk, it proposed a mechanism where users store an offline profile on their own side which hidden from the server and an online profile on the server from which the server generates the recommendations. The online profiles of different users are frequently synchronized with their offline versions in an independent and distributed way. [9] Erkin introduce Homomorphic encryption schemes and secure multiparty computation (MPC) techniques for privacy enhanced recommender system. The cryptographic protocol for generating recommendations to the users within online applications. The complexity analysis, the overhead initiate by working in the encrypted domain is reduced significantly by packing data and using the DGK cryptosystem. Proposed system cannot compare with previous system because of space problem [2].The distributed generation of an RSA private key required by a Threshold Paillier Cryptosystems much more complex than the simple independent partial private key generation possible with the ElGamal encryption algorithm. The private key is a factorization secret in Paillier encryption where as the distributed key generation is extremely inefficient as in ElGamal is much more efficient in voting scheme. In Paillier, each multiplication is performed modulo N^2 where N is the product of two large primes. In comparison with ElGamal, each multiplication is performed modulo p a large prime. If N and p should have same length then multiplication in Paillier is more costly than ElGamal. In private recommendation the privacy sensitive data such as user preferences and similarity values between users were to be encrypted and generate recommendation by processing those data. As the Homomorphic property permit us to realize linear operations in the encrypted data. Efficiency plays a important role in the success of cryptographic protocols. But because of large data system becomes costly. Multiparty computation is used to keep secret everything which is not to be public, all parties can agree on this security policy, but the multiparty computation is time-consuming as well as expensive.

III. Implementation Details

Current systems need active participation of user which becomes privacy risk. To overcome 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 ElGamal 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 between the service provider and the PSP, without interrelate with the users.

3.1 *Construction of the encrypted database:*

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 sending them to the service provider using ElGamal algorithm.

3.2 *Generating recommendations:*

To generate recommendations, we need two inputs from each user: the densely rated vector to compute the similarity values between users, and the partly rated vector to generate recommendations as the average rating of the top most similar users.

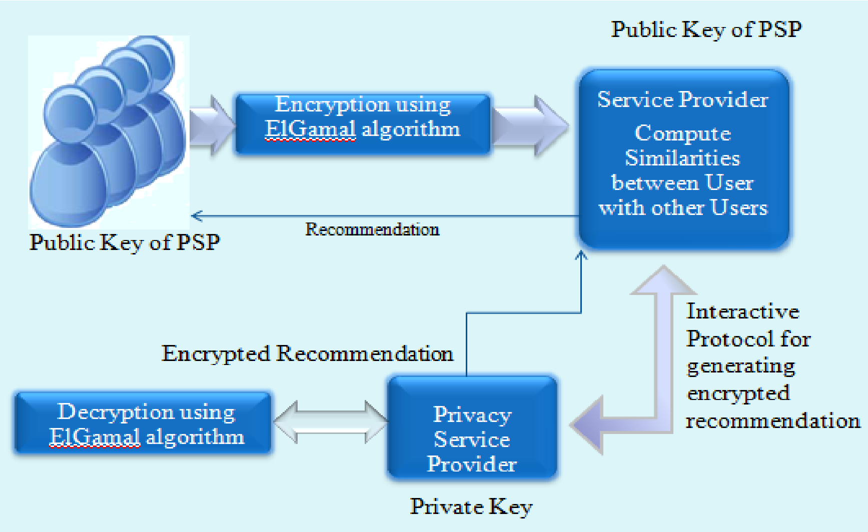
Public Key of PSP
Encryption using ElGamal algorithm
Service Provider
Compute Similarities between User with other Users
Public Key of PSP
Recommendation
Interactive Protocol for generating encrypted recommendation
Encrypted Recommendation
Decryption using ElGamal algorithm
Privacy Service Provider
Private Key

Fig. 1 System Architecture

These vectors are highly privacy-sensitive and thus, they will be stored in the encrypted form by the service provider. The service provider does not have the decryption key, thus preventing it from accessing the users' private data.

To generate recommendations, the service provider and the PSP run a cryptographic protocol without interacting with the users. Recommendations can be generated in a privacy-preserving way during the idle time of the service provider and the PSP even before any user asks for recommendations. This means that a user will receive recommendations soon after user's request without any delays.

3.3 Algorithm:

1. Data from user
2. Encrypt the data using ElGamal algorithm
    a. Choose a large prime p with 150 digit
    b. choose two random integers $1 \leq q, x < p$
    c. Calculate $y = q^x \bmod p$
    d. Public key: p, q, y; private key: x
    e. Encryption of a data R : choose a random t and compute $a = q^t \bmod p,\ b = y^t R \bmod p$
    f. Cipher Text $c=(c_1,c_2)$
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

$$R = \frac{c_2}{{c_1}^x} \bmod p = c_2 {c_1}^{-x} \bmod p$$

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.

3.4. Mathematical Model:

U= (U1, U2 …) set of users, I= (I1, I2……..) Set of items, R= (R1, R2…..) Set of densely rated items

a. Encryption of data R_i

$E_{p,q,t}$: $q^t \bmod p \rightarrow c_1$, $E_{p,q,t} : y^t \times R_i \rightarrow c_2$

C1= (c1, c2…), C = {C1, C_2, C_3……..}

b. SP ← C

c. Similarities

$$\text{Sim}\,{}_{(}C_1, C2{}_{)} = \frac{\sum_{i=0}^{I-1}(v(c1,i).v(c2,i))}{\sqrt{\sum_{i=0}^{I-1} v^2(c1,i) \sum_{i=0}^{I-1} v^2(c2,i)}}$$

$$= \sum_{i=0}^{I-1} \vartheta(c1,i)\vartheta(c2,i)$$

d. SP:C⟶ PSP

e. D_x : C1 × C2 ⟶ R_i

f. Find Similar user Us_i

g. Compute UR_s

h. If User ⟶ Request then SP $\xrightarrow{UR_s}$ User

IV. RESULT

4.1 Data set:

U= (U1, U2 …) set of users, I= (I1, I2……..)Set of items, R= (R1, R2…..) Set of densely rated items
Output: UR_s

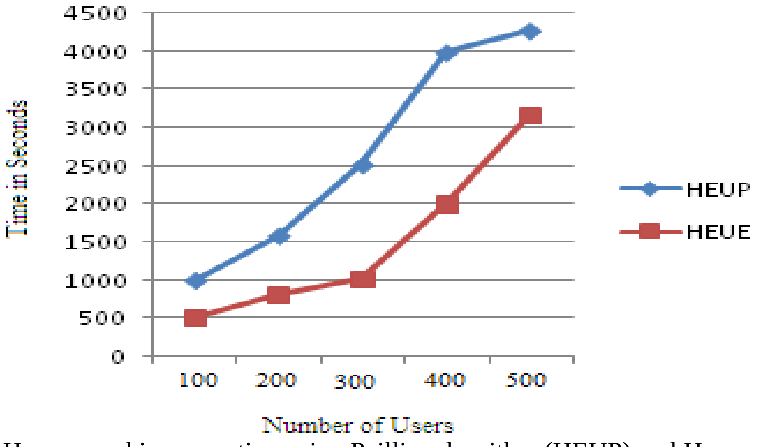

Fig.2 Average runtime of Homomorphic encryption using Paillier algorithm (HEUP) and Homomorphic encryption using ElGamal algorithm (HEUE) to generate recommendation.

4.1 Result: Graph shown below gives the comparison between the proposed system and existing system.

V. CONCLUSIONS

Propose system is protecting the privacy of the users against the service provider through Homomorphism encryption based on ElGamal scheme. Compared to the existing private recommendation system which uses Paillier techniques, this system is secure, much more efficient and inexpensive. The system makes it possible for servers to collect private data from users for CF purposes without compromising users' privacy requirements. 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. L. Herlocker, J. A. Konstan, A. Borchers, and J. Riedl, "An algorithmic framework for performing collaborative filtering," in Proc.22nd Ann. Int. ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR'99), New York, NY, 1999, pp. 230–237, ACM.

[7] P.Bogetoft, D. L.Christensen, I. Damgård, M. Geisler, T. P. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. I. Schwartzbach, and T. Toft, "Secure multiparty computation goes live," in Proc. Financial Cryptography, 2009, pp. 325–343.

[8] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. Advances in Cryptology (EUROCRYPT' 99), ser. LNCS, J. Stern, Ed., May 2–6, 1999, vol. 1592, pp. 223–238, Springer.

[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] R. Cramer, I. Damgård, and J. B. Nielsen, "Multiparty computation from threshold homomorphic encryption," in Proc. Int. Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT'01), London, U.K., 2001, pp. 280–299, Springer-Verlag.

[11] Z. Erkin, M. Beye, T. Veugen, and R. L. Lagendijk , " Generating Private Recommendations Efficiently Using Homomorphic Encryption and Data Packing", IEEE Transaction on Information Forensics and Security", Vol. 7,No. 3, JUNE 2012.

[12] 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.