Protective Approach to User Secrecy and Recommendation Using Homomorphic Scheme

Tejashree A. Malshikare[1], Amrit Priyadarshi[2]
[1, 2]Computer Engineering, Dattakala Faculty of Engineering, Swami Chincholi, Daund, Pune, India
Email address: [1]tejashri.malshikare@gmail.com

Abstract— *In the recommended systems, online service accesses users proles and generating valuable dynamic recommendations. Relay on the privacy info collect from users, it is generating recommendations in online services. To secure privacy of user it is important obligations of Information architecture. The Recommendation System has to identify by privacy of users and info and service providers. The information protection systems mainly provide security from malicious users like control access to malicious users and also provide secure transmissions, but does not provide security against the service provider. This produces main risk for user. We are protecting private info of user against services provider when protecting functionality of system. We are recommending encrypted personal data and process encrypted info to generate the recommendation. Here construct efficient systems and does not required active participation of users by semi trusted third party. Existing private recommendations system is consisting of Paillier system but system is difficult and an inefficient. We solve the problem by using ElGamal algorithm.*

Keywords— *Homomorphic encryption, recommender systems, privacy service provider, customer relational management*.

I. Introduction

Many are retrieving online service for activities which involves sharing personal info with the service providers. Example of online service is social networking, web shopping. In social networking, persons obtain in contact with other persons, and creating sharing info which comprises personal info. Provided content of consumer can be accessible by service provider and have permission to look up collected information and hand over them to third party. It does not provide security to users data. The opportunity of buying products is increased by providing suggestions to customers. In web based events like e-commerce which provide number of goods or items from which consumers can select. The important process in web activity is to provide identical customers with recommendation of goods which they like and help them to purchase appropriate good. It is helpful for recommendation system. Modified recommendation for product that suits consumers flavor cant only improve consumer satisfaction and faithfulness, also upsurge conversion and incomes for retailers. Internet are progressively adopting products recommendation engine for personalized recommendations, like Amazon, Google and Yahoo. Recommender system is gratifying extensive Knowledge used to endorse cross selling. The ratings obtaining adequate exact feedback which foremost to unsatisfactory recommendations.

Recommender system is classified in below category:

1) Content based recommendation: In such recommendation consumer will recommend item same to ones consumer favored in past.
2) Collaborative recommendation: In such recommendations techniques, consumer will recommend item that person with same tastes and predilections alike in past.
3) Hybrid Recommendations: In Hybrid recommendations, collaborative and content-based recommendation methods are combined.

To protect privacy of users is vital obligation of basic Information architectures. The organize Recommendation Systems have to recognized by privacy aware user and also information and service provider. The data protection system focuses on the access controls and secured transmission which provide the security in contradiction of the malicious parties, but not from the service providers. This yields major risk for users. Here, we are going to protect private data of users against service providers when protecting functionalities of systems. We are going to recommend encrypted private data and will process encrypted information to generating the 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. The existing private recommendation system consists of Paillier encryption system but system is more difficult and inefficient. We solve this problem by using ElGamal algorithm

A. Problem Statement

The main aim in this work is to focus on the customer churning process and develop some efficient techniques to overcome the customer churning using data mining techniques. Our algorithm does not depend only on prediction, but also on classification and probability estimation. User information is available from decision trees Also we have to protect the confidential data of user against the service provider while protecting the functionality of the system. This system is efficient to generate dynamic recommendations in a privacy preserving manner.

II. Liturature Survey

Privacy-preserving collaborative filtering using randomized perturbation techniques
Author: H. Polat and W. Du
polat uses randomized perturbation techniques that provide consumers confidentiality during creating accurate

recommendation. Anonymous technique has problem that there is no guarantee of quality of data this technique allow consumer to open up their private information without revealing their individualities. It provide new system, where every consumer provide personal facts, and send to other place where the data collector cannot retrieve honest information about a users private information [4].

Preserving privacy in collaborative filtering through distributed aggregation of offline profiles
Author: R. Shokri, P. Pedarsani
With minimum loss on accurateness of system, It provides the Distributed method for users to enhance their profiles and provide protection from an entrusted server. The server having direct entry to consumer profiles because of this It has problems of exploring consumers confidentiality in existence of entrusted central server. To remove confidentiality risk, it suggested mechanisms where consumer store off-line summary on own side and secreted from server and online profile on servers from the servers generate recommendation. The profiles of consumers are synchronized with off line forms in distributed ways [8].

Privacy enhanced recommender system
Author: Erkin, M. Beye, T. Veugen
Erkin presents Homomorphic schemes and protected computation techniques for privacy recommender system. The difficulty study, inductee by functioning in encryption domain is summary meaningfully by data packing. Propose work cannot equate with preceding system since of space problems [3].

Generating Private Recommendation
Efficiently Using Homomorphic Encryption and Data Packing
Author: Zekeriya Erkin
The thresholds of Paillier require distributed generations of RSA private key which is more difficult than partial private key generations probable with ElGamal algorithm. The private key kept secret in Paillier system. The Erkin introduced encrypting private data and processing them under encryption to generate recommendations. By introducing a semi trusted third party and using data packing, that constructs a highly efficient system that does not require the active participation of the user [1].

Privacy Preserving Collaborative Filtering
with k-Anonymity through Micro aggregation
Author: Casino, F. Domingo-Ferrer
Casino presents that Collaborative Filtering (CF) is a recommender system which is highly relevant for the industry. It focuses on Privacy Preserving Collaborative Filtering (PPCF), whose aim is to solve the privacy issues caused by the systematic collection of private information. It propose a new micro aggregation-based PPCF method that distorts data to provide k-anonymity, while simultaneously making accurate recommendations [10].

III. Proposed System

A. *System Architecture*

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. 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 tha t a user will receive recommendations soon after user's request without any delays.

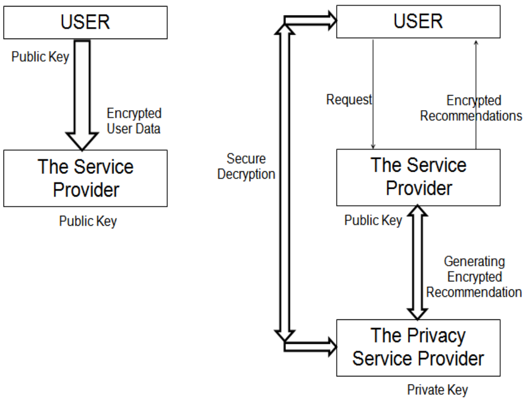


Fig. 1. System architecture

The recommendation will get generate in two modes namely
static and dynamic:

1) *Static recommendation*

In this type, recommendation will get generate according to the product only regardless of purchase of users. Consider user 1 purchased the software A then system defines the recommended product B for the product A.

2) *Dynamic recommendation*

In this type of recommendation the system will generate the recommendation according to products purchased by users. In this case consider five users purchased the product A. Out of five three will purchase product B along with product A and remaining two will purchased product C. So on the basis of maximum frequency, the system will recommend the product B for the product A for the new users. To produce recommendation, service providers and PSP run cryptographic algorithm without cooperating with consumers. Recommendations generated in privacy preserving manner during idle period of service providers and PSP even before user requests for recommendation. This means consumer will obtain recommendations quickly after consumer's request come without any delay.

B. *Algorithm*

The EIGamal algorithm is used for encryption.
ElGamal Algorithm is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and Signature algorithms. ElGamal encryption consists of three

components: the key generator, the encryption algorithm, and the decryption algorithm. In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography. This is the algorithm we are using to generate recommendation.

1. Information From Consumer
2. Encrypting the info by ElGamal
a. Select large prime p through 150 digit
b. Select two random integers 1 = q, x < p
c. Compute y = qx mod p
d. Public key: p, q, y, private key: x
e. Encryption of info R:Select random t and calculate a = qt mod p, b = yR mod p
f. Cipher Text c= (c1,c2t)
3. Send cipher text to service provider
4.Calculate Resemblances between specific consumers with all other consumer
5. Send resemblances to privacy service provider
6. Decrypt resemblances
7. Calculate recommendation
a. Discovery similar consumers
b. Calculating number L and sum of rating of most alike consumers
c. Calculating Recommendation
8. Direct recommendation to consumer.

IV. Implementation Details

A. System Model

In proposed system, we focus on the output of decision tree algorithms as the input to our post processing algorithms. Our algorithms rely on not only a security, but also a probability estimation of the classification, such as the probability of being loyal. Such information is available from decision trees. 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 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.

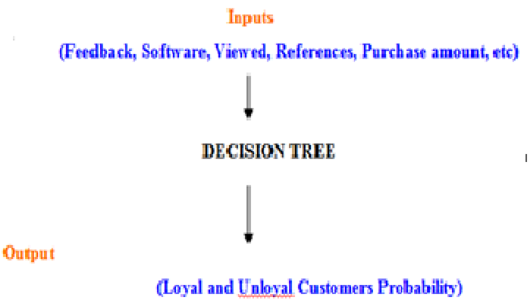

Inputs
(Feedback, Software, Viewed, References, Purchase amount, etc)
DECISION TREE
Output
(Loyal and Unloyal Customers Probability)

Fig. 2. System model

B. Creation of Encrypted Data

Beforehand creating data, systems are calculating resemblances between specific consumer and other consumer. This resemblance kept in vector. To make encrypted data, the consumers encrypt data before transfer them to service providers using ElGamal algorithm.

C. Generating Recommendations

To produce recommendation, system take essential inputs from user: densely vector to calculate similarity values among consumers, and partially evaluated vector to make recommendation as average evaluation of top similar consumers. Such vectors are extremely privacy sensitive and they will keep in encrypted format by service providers. The service providers don't have decryption keys, so stopping it from retrieving the consumer's private information.

D. Mathematical Model

Input:
U= (U1, U2) set of users, I= (I1, I2..) Set of items,
R= (R1, R2..) Set of densely rated items.
Processing:
1) Encryption of data Ri.
Ep,q,t : qt mod p → c1 , Ep,q,t : yt*Ri → c2
C1= (c1, c2), C = C1,C2,C3,..
2) SP ← C
3) Similarities
Sim(C1;C2)

$$= \sum_{i=0}^{l-1} (v(c1,i),v(c2,i) \div \sqrt{} \sum_{i=0}^{l-1} v2(c1; i), v2(c2; i) \qquad (1)$$

$$= \sum_{i=1}^{l-1} v(c1, i), v(c2, i) \qquad (2)$$

4) SP: C → PSP
5) Dx : C1 C2 → Ri
6) Find Similar user Usi
7) Compute URs

Output:

If User → Request then SP → (URs) User

V. Expected Result and Output Design

A. DATASET

U= (U1, U2) set of users, I= (I1, I2..)Set of items,
R= (R1, R2..) Set of densely rated items
Output: URs As a data we are taking set of users which are going to purchase items that is I1,I2.... The items which have more ratings that is they are highly purchased by users. So the output is the densely rated items are recommended to the users.

B. Expected Result

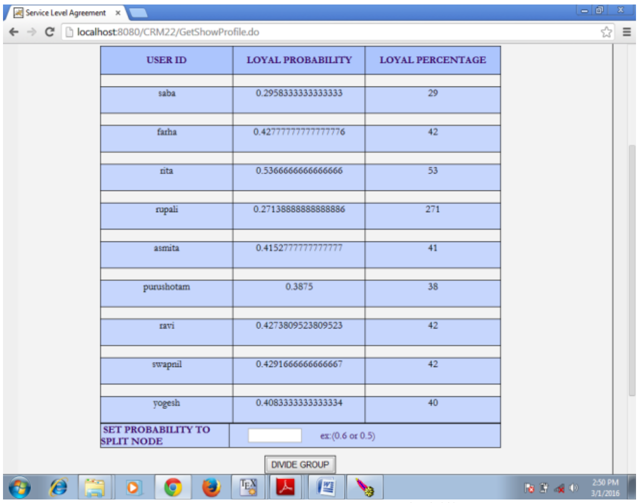
Expected result is to maintain and present the all information regarding loyal customers give number of purchase made by the customers, number of login made etc.

TABLE I. Expected result table

	Count
No. of software	7
No. of Logins made	115
No. of viewed software	104
No. of References	9
Feedback points	81
Cost of purchase	87670

C. Result

Here we design the percentage of loyal and unloyal customers depends on items purchase by the customers and logins made by the customers.



USER ID	LOYAL PROBABILITY	LOYAL PERCENTAGE
saba	0.2958333333333333	29
farha	0.4277777777777776	42
rita	0.5366666666666666	53
rupali	0.2713888888888886	271
asmita	0.4152777777777777	41
purushotam	0.3875	38
ravi	0.4273809523809523	42
swapnil	0.4291666666666667	42
yogesh	0.4083333333333334	40
SET PROBABILITY TO SPLIT NODE	ex:(0.6 or 0.5)	

Fig. 3. Loyal customer's probability

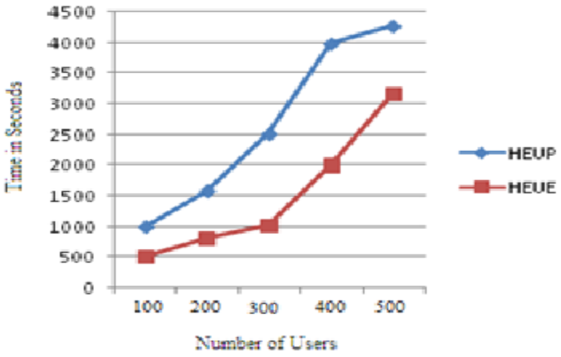


Fig. 4. Runtime of homomorphic encryption

Runtime of Homomorphic encryption shows evaluation between propose system and existing one. As the Homomorphic encryption using Paillier take more time to run than ElGamal encryption algorithm. From the graph above we see that Paillier algorithm take 4300 seconds to encrypt the data while ElGamal take 3100 seconds to encrypt the data so it is very efficient to use ElGamal algorithm for Encryption. That is existing system using Paillier algorithm which is not as efficient as the proposed system for which we are using ElGamal algorithm which is comparison measure used for system.

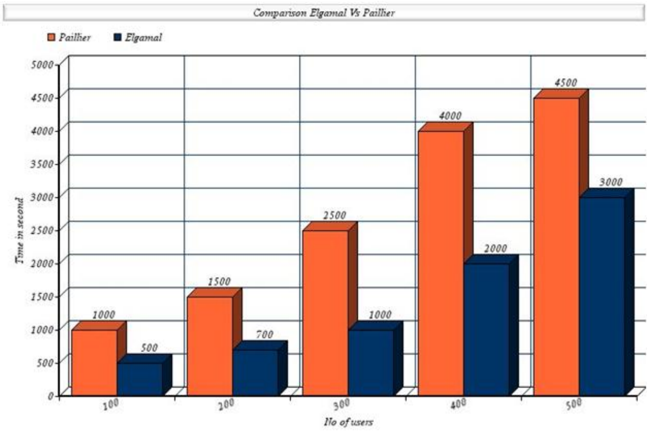


Fig. 5. Analysis of paillier and eigamal

VI. Conclusion

Proposed system is defensive to confidentiality of consumers in contradiction of service provider finished Homomorphism encryption founded on ElGamal schemes. Likened to existing private recommendation which uses Paillier systems, proposed system is protected, more effective and low-cost. The system marks it likely for servers to gather private info from consumers for Collaborative Filtering purpose without cooperating consumer's privacy necessities. In forthcoming, projected system can prolonged to lively recommender system for numerous groups in actual time environment.

VII. Acknowledgement

I am thankful to my guide Prof. Amrit Priyadarshi for him continuous support and guidance in my work. I want to thank to department staff for their great effort of supervising and leading me to accomplish this fine work. They were great
source of support and encouragement.

References

[1] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, Fellow, "Generating private recommendation efficiently using homomorphic encryption and data packing," *in IEEE Transaction on Information Forensics and Security*, vol. 7, no. 3, pp. 1053-1066, 2012.

[2] F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig, and A. Solanas, "Privacy preserving collaborative filtering with k-anonymity through micro aggregation," *IEEE 10th International Conference on e-Business Engineering (ICEBE)*, pp. 490-497, 2013.

[3] Z. Erkin, M. Beye, T. Veugen, and R. L. Lagendijk, "Privacy enhanced recommender system," *in Proceedings Thirty First Symposium Information Theory in the Benelux*, Rotterdam, pp. 35-42, 2010.

[4] H. Polat and W. Du, "Privacy-preserving collaborative filtering using randomized perturbation techniques," *Third IEEE International Conference on Data Mining*, pp. 625-628, 2003.

[5] J. L. Herlocker, J. A. Konstan, A. Borchers, and J. Riedl, "An algorithmic framework for performing collaborative filtering," *in Proceedings of the 22nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR99)*, New York, NY, pp. 230-237, 1999.

[6] P. Bogetoft, D. L. Christensen, I. Damgrd, M. Geisler, T. P. Jakobsen, M. Krigaard, J. D. Nielsen, J. B. Nielsen,K. Nielsen, J. Pagter, M. I. Schwartzbach, and T. Toft, "Secure multiparty computation goes live", *Financial Cryptography and Data Security*, pp. 325-343, 2009.

[7] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *in Proceedings of the 17th international conference on Theory and application of cryptographic techniques (EUROCRYPT99)*, vol. 1592, pp. 223-238, 1999.

[8] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and J. P. Hubaux, "Preserving privacy in collaborative filtering through distributed aggregation of offline profiles," *in Proceedings of the Third ACM Conference on Recommender systems (RecSys09)*, New York, NY, pp. 157-164, 2009.

[9] R. Cramer, I. Damgrd, and J. B. Nielsen, "Multiparty computation from threshold homomorphic encryption," *in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT01)*, London, U.K., pp. 280-299, 2001.