IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VIII (Feb. 2014), PP 72-75
www.iosrjournals.org

Flexible Dynamic Recommender System

Umakant Tupe, Prof.R.B.Joshi
M.E(II Year) Department Of Computer Engg. MMCOE Pune,Maharashtra,India
Asst. Prof. Department Of Computer Engg. MMCOE Pune,Maharashtra,India

***Abstract**: A Recommender System now becoming decision maker for the people who lack sufficient personal experience to evaluate the items that are on website. It provides recommendation for specific items such as books, news, tourism services etc. Personalization is common term for improving online services and attract more users. The previous recommender system like Amazon, Suggest, e-bay provide suggestion for specific items but drawback that service provider can see the ratings of users. It may happen that owner can give more ratings for particular item and can increase product popularity. This results in misguiding to user and privacy is violated. In our flexible recommender system users give ratings for some product in encrypted format, so service provider does not able to decrypt it. In this recommender system users decision time is saved, because time plays vital role in recommender system. During less amount of time user should get more rated products.*

***Keywords:** Homomorphic Encryption, probe technique ,Recommender System*

I. INTRODUCTION

RS are software agents that elicit the interests and preferences of individual consumers and make recommendations accordingly. They have the potential to support and improve the quality of the decision consumers make while searching for and selecting products online. Crores of people are using online services for their personal use. Most of people share data to service provider. Consider the following services.

Tourism services

In this people share their personal data to tourism services which then process and book the tickets and hotels.

Online Shopping

Many people use this for shopping cheap and quality products. Service provider collects user data like user preferences and click logs.

Facebook

In face book, people share their personal images, videos to their friends. Service provider has right to process collected data and sends to third parties. User's data is collected form user profiles and behavior

In all of the above services and many others recommender system based on collaborative techniques collect and process user information. From all of the above services people get benefit but direct access to private data of users have potentially risk that their important ratings get violated. Recent studies of recommender system show that privacy violation threatens the healthy growth of e-business. Therefore it is important to preserve the privacy of online customer for the benefit of both individual and e-business.

In this paper, we propose a cryptographic solution for preserving the privacy of customers in recommender system. In short private information of customers are kept secret and service provider generates recommendation by processing encrypted data.

II. LITERATURE SURVEY

In previous recommender system canny propose a model to protect the privacy of users based on a probalistic factor analysis model by using similar approach[3].Polat and Du suggest randomized technique[10,11].In this paper they use dummy set that cancels out result is good estimation of required output. In [5], Erkin put forward homomorphic encryption and multi party computation technique which gives secure data protection. But they suffer from computation and communication latency. In [6],An agent based system where trusted software is used but not provide accuracy to user. In [12] cryptography is used to increase reliability of forecast and correraltion.In some recommender system privacy is maintained but not the accuracy, when system tries to get accuracy we doesn't get accuracy so little bit tradeoff between privacy and accuracy. This happens due to distributed aggregation. In some scenario technique to hide data is put forward which uses statistical approach but this technique is not completely secure [10]. In some recommender system Perturbed rating is used which disguise the contents and users original contents is not preserved because pattern matching algorithm find the Perturbed rating in some fraction of seconds[9]. In some recommender system decision tree learning with ID3 algorithm is preferred but this protocol have few seconds of communication and less bandwidth[6].Recommendation generation is done using cryptography but drawback of this method is they are extremely slow and have extra overhead[14]. Erkin propose protocol based on cryptographic technique, which was better than previous one but drawback was users were participated which makes overall recommender system vulnerable, in that single user have to perform thousands of calculation of encryption and decryption which causes recommender system expensive for the users[16], but we want Recommender system which is flexible, user friendly and dynamic. In our proposed system, we will generate Recommender System which doesn't provide overhead on user, communication cost and bandwidth is minimized and user gets quick response of updated products.

OUR CONTRIBUTION

In our proposed work we aim to generate private recommender system which is dynamic, flexible and user get updated products. We use dynamic module which checks for updated stack entry and if new product found then database will be updated and Service provider get new product for similarity computation and user get more and more new products for online shopping.

III. PROPOSED SYSTEM ARCHITECTURE

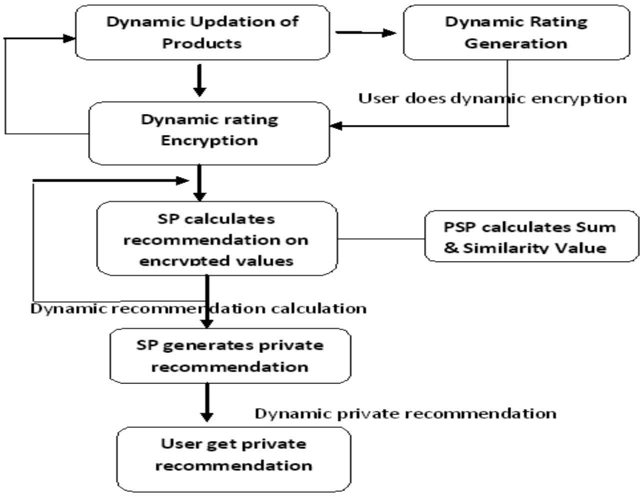
Dynamic Updation of Products
Dynamic Rating Generation
User does dynamic encryption
Dynamic rating Encryption
SP calculates recommendation on encrypted values
PSP calculates Sum & Similarity Value
Dynamic recommendation calculation
SP generates private recommendation
Dynamic private recommendation
User get private recommendation

Fig. Proposed System Architecture

Service Provider:

Service Provider who provides services to user. He has a business interest in generating recommendation for his customers. He has resources for storage and processing.

SP calculates recommendation on encrypted data.

Privacy Service Provider:

We include this third party to eliminate the need for active participation of users in computations.PSP has private keys for Paillier system. PSP calculates sum and similarity values. PSP completes his assigned task effectively without observing private data of customer.

.

Users:

Users are customers, based on their choices(rating),the service provider generated recommendations for them. Users upload their private data to service provider

Service provider and PSP runs a cryptographic protocol between them and generates recommendation. Cryptographic protocol between SP and PSP has to work on encrypted data which is difficult task, so we use secure multiplication and decryption protocol to reduce overhead to the system.

We have included dynamic module which cheeks for stack updates. If new product entry occurs then it will be send to SP, SP sends it to PSP which decrypt and send results to SP and last SP generates recommendation sends results to users.

Users get results of their choices, preferences.

A. ALGORITHM X

Step 1: Every user encrypts array by using public key of PSP and sends this encrypted data to PSP.
Step 2: Service provider & PSP calculate encrypted similarity value between user A and all other user.
Step 3: Most similar users are found by comparing each similarity value with publicly threshold value d.
Step 4: The service provider calculate total no. of users with similarity value above threshold. Service provider also calculate encrypted sum of ratings given by end user.
Step 5: Sp then sends these value to user.
Step 6: Sp then decrypts data using decryption algorithm.

B. ALGORITHM Y

Step 1: Enter the no. of products & user ratings.
Step 2: Create 2 threads one thread for similarity computation & other thread for ALGORITHM X
Step 3: Run ALGORITHM X parallel.
Step 4: ALGORITHM Y will dynamically poll and will find out latest no. of products and will calculate similarity..

In proposed algorithm, we simply use secure encryption and decryption of user ratings. User first request for service from server. In this user rating is collected from encrypted form then it sends to SP. User encrypt ratings using public key of PSP. Service provider doesn't disclose user profiles, important information because he is unable to decrypt it. SP uses third party PSP to reduce overhead on user. User is not actively participated in recommendation generation process. He has to give best choices (ratings) and get best product for their use.
PSP and SP works on interactive protocol to follow rules of recommender process.PSP decrypts user contents but doesn't disclose user information. In this way user privacy is maintained.PSP sends generated recommendation to SP,SP forward generated recommendation to user, so user get private recommendation and also newly updated product ratings.

C: WORKFLOW OF PROPOSED SYSTEM

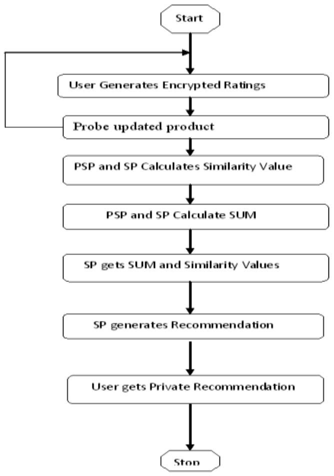
Start
User Generates Encrypted Ratings
Probe updated product
PSP and SP Calculates Similarity Value
PSP and SP Calculate SUM
SP gets SUM and Similarity Values
SP generates Recommendation
User gets Private Recommendation
Stop

Fig. Workflow of proposed system

In above figure user first creates encrypted ratings using public key of PSP.SP and PSP calculate similarity value and also calculate SUM. between this if new products are arrived or launched then it will be checked by probe stack.SP gets SUM and Similarity value. During idle time SP generates private recommendation. At last user get private recommendation.

IV. DATA SET

1.Input to recommender system is ratings, preferences, demographics in encrypted format .
2. Output is generated recommendation, Relevance score. Used for ranking
3.Processing include Database construction, Similarity Computation, calculation of SUM and generating recommendation

To generate recommendation system requires preference vector Va and Vb each for similarity computation and other for generating recommendation. Va is a set of rating given by user 1 for product1.Vb is a set of rating given by user 2 for product1,Vn is set of rating given by n user for product1.Likewise we calculate average rating given by user for particular item. After that product popularity and goodness is defined.

Specific user will give specific recommendation for specific product so rating given by user for particular product is true ratings.

V. Result Set

1. In the result set user get generated private recommendation.
2. We believe that it's a true ratings not perturbated ratings.

VI. Conclusion

Recent studies show that the privacy consideration in online e-commerce services is one of the most important scenarios that threaten the healthy growth of e-business. Therefore it is important to preserve the privacy of users of online e-commerce services for the benefit of both users and e-business.

In our dissertation work, we aim to build system that will generate recommendation privately using homomorphic Cryptography and we extend our work by designing new privacy preserving technique for recommendation generation by considering dynamic behavior. We believe that our dissertation will help in building safe and secure online E-commerce application.

In Future, attribute based encryption can be considered where many users attributes will be used for recommendation generation.

VII. ACKNOWLEDGEMENT

Every dissertation work has an imprint of many people and it becomes the duty of author to express deep gratitude for the same.

I thank Prof. Harmeet Khanuja M.E Coordinator for opening the doors of the department towards the realization of the IOSR-2014 paper, all the staff members, for their indispensable support, valuable suggestions and for most valuable time lent as and when required. With all respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly.

REFERENCES

[1] Generating Private recommendation using Homomorphic Encryption and Data Packing. IE EE TR ANS AC TIONS ON INF OR MAT ION F ORE NS IC S AND S EC UR ITY, VOL. 7, NO. 3 , J UNE 2 01 2 10 53

[2] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions,"IEEE Trans. Knowl. Data Eng., vol. 17, no. 6, pp. 734–749, Jun. 2005.

[3] N. Ramakrishnan, B. J. Keller, B. J. Mirza, A. Y. Grama, and G.Karypis, "Privacy risks in recommender systems," IEEE Internet Comput., vol. 5, no. 6, pp. 54–63, Nov./Dec. 2001.

[4] N. Kroes, Digital agenda, Brussels, May 19, 2011.

[5] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in Proc.SIGMOD Rec., May 2000, vol. 29, pp. 439–450.

[6] Y. Lindell and B. Pinkas, "Privacy preserving data mining," J. Cryptol., pp. 36–54, 2000, Springer-Verlag.

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

[8] H. Polat andW. Du, "SVD-based collaborative filtering with privacy," in Proc. 2005 ACM Symp. Applied Computing (SAC'05), New York, NY, 2005,

[9] S. Zhang, J. Ford, and F. Makedon, "Deriving private information from randomly perturbed ratings," in Proc. Sixth SIAM Int. Conf. Data

[10] 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.

[11] F.Mc Sherry 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.

[12] R. Cissée and S. Albayrak, "An agent-based approach for privacy preserving recommender systems," in Proc. 6th Int. Joint Conf. Autonomous Agents and Multiagent Systems (AAMAS'07), New York, NY, 2007, pp. 1–8, ACM.

[13] M.Atallah, M. Bykova, J. Li,K. Frikken, andM. Topkara, "Private collaborative forecasting and benchmarking," in Proc. 2004 ACM Workshop on Privacy in the Electronic Society (WPES'04), New York, NY, 2004, pp. 103–114, ACM.

[14] J. F. Canny, "Collaborative filtering with privacy.," in IEEE Symp. Security and Privacy, 2002, pp. 45–57.

[15] J. F. Canny, "Collaborative filtering with privacy via factor analysis," in SIGIR. New York, NY: ACM Press, 2002, pp. 238–245.

[16] Z. Erkin, M. Beye, T. Veugen, andR. L. Lagendijk, "Privacy enhance recommender system," in Proc. Thirty-First Symp. Information Theory in the Benelux, Rotterdam, 2010, pp. 35–42.

[17] 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.

[18] J. R. Troncoso-Pastoriza, S. Katzenbeisser, M. U. Celik, and A. N. Lemma, "A secure multidimensional point inclusion protocol," in Proc. ACM Workshop on Multimedia and Security, 2007, pp. 109–120.

[19] T. Bianchi, A. Piva, and M. Barni, "Composite signal representatio for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[20] O. Goldreich, Foundations of Cryptography. Basic Applications, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, May 2004, vol. 2,