International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4690 - 4694

Generating Private Recommendation System Using Multiple Homomorphic Encryption Scheme

Ms. Jagtap Renuka N.
Department of Computer Engineering
ACEM MARUNJI, Pune
Savitribai Phule Pune University
e-mail: jagtaprenuka31@gmail.com

Prof. Mrs. Sonali Patil
Department of Computer Engineering
ACEM MARUNJI, Pune
Savitribai Phule Pune University, India
e-mail: sonalin69@gmail.com

Abstract— The recommender system is important tool in online application to generate the recommendation services. Recommendations are generated by collecting the data from users need; online services access the user's profiles for generating useful recommendations. Privacy sensitive data is used for to collect the data. Collaborative filtering technique gives privacy for sensitive data if data is misused by other service providers or leaked. Existing system uses Paillier encryption algorithm & DGK algorithm to secure user data from malicious third party as well as to protect the private data against service provider but system is more complex and inefficient. Proposed system protects the privacy of user using encrypting the sensitive data. The system uses multiple homomorphic algorithms to secure user data from service providers. The system is used to protect the confidential data of user against the service provider while providing online services. Encrypting private data is recommended and process on data to generate recommendations. To construct efficient system that does not require the active participation of the user. The experiment shows that the result that provide the security by hiding the personal data of user from third party.

Keywords- *Recommender system, Multiple Homomorphic encryption, User privacy, Collaborative filtering Technique.*

*****

I. INTRODUCTION

Recommender is the important tool in E-commerce. Million peoples are uses the different services for the daily purpose. Recommender system is the system that is used to give the rating for user items. This system is used to apply on various applications in research area for developing new approaches .It requires for improving effective and applicable real life applications. Different online services are used in daily basis activities like watching movie, listening music's, play games, social networks, books, research articles, online shopping, etc. that required sharing of personal information with service provider .service provider uses smart applications to monitor people actions, to observes click logs, searches, likes & dislikes. Consider the different online services.

social network: social network is used to share the different information to many people like share the video, personal information, images that is accessed .service providers has right to process on users data and transfer it to third parties. Also it generate the recommendations for finding new friend, or groups by using collaborative filtering technique [3].

Online shopping: these services are used for to check the list of items and purchase the different items that are recommended suggestion according to user's logs and preferences.

IP-TV: according to click logs and watching habit of user, service provider recommends the different TV programs, movies and products that are according to user's interest. In all of the services, recommender systems based on collaborative filtering techniques that collect the data from particular user. From personal data people benefit the services but on other hand service provider directly access the private data that is risky for user because data [3] is stolen and that is used for other purposes. To provide the safely growth of e-commerce the most important part is providing the security of user information for the benefit of user as well as business. In recent survey to increase the healthy growth of e-business online services are most important factors so, it is important to protect the privacy of the users of online services for the benefit of both individuals and business.Recommender system is the system that is used as the subclass of information filtering system that seek to predict the 'rating' or 'preference' that given to the item. The most popular ones are probably music, news, books, research articles, search queries, social tags, and products in general.

The main goal & objective is to hide the personal data of user from service providers so it protect the data and provide security. The protocol should not have any significant impact on usability (user convenience).The protocol should be easy to deploy and scalable, requiring minimum computational resources in terms of memory, processing time, and disk space.

This protocol has the following steps.

1) The service provider and the PSP compute the encrypted similarity values between user A and all other users.
2) The most similar users are found by comparing each similarity value with a publicly known threshold in the encrypted domain.
3) The service provider computes encrypted L, which is the number of users with a similarity value above the threshold. The service provider also computes the encrypted sums of the ratings of these L users for each item.
4) The service provider sends the encrypted L and the sums to user A.
5) After obtaining the number L and the sum in plain text by running a decryption protocol with the PSP, given the user A divides the sum of ratings by L.

II. RELATED WORK

In [2],the Recommender system is classified in different categories like content based recommendation, collaborative filtering, and hybrid approach. Content based system prefers the past logs and generates recommendation. In collaborative

filtering techniques it is used for to find the similarity in two customers that is like minded customer's preferences that provide high quality data from customers. Collaborative Filtering is used for to suggest product to the customer. Hybrid is the combination of both systems. Nearest neighbour algorithm is used to find the similar preferences. Collaborative filtering has two classes first is model based algorithm is used for making the predictions. second is memory based model is used for finding the similar items.it again divide into two groups-user based heuristic algorithm is used for give the rating & second is item based for selecting the different items.

To protect the confidential data that is privacy sensitive data cryptography [5] & data perturbation [4] technique is used. Polat & Du [7] suggest randomized perturbation technique that is used to provide the accurate recommendation for protecting privacy of users.it is also used to calculate the accuracy that is affecting on privacy. Polat uses anonymous technique for hiding the data of user so, an identity of user is disclosing. But there is no guarantee of data.

In [11], Erkin proposed cryptographic approach for generating recommendations. Multiparty computation technique is used to remove significant overhead in computational complexity. In [12], canny propose the system in that users private data is encrypted & then recommendation is generated. Conjugate Gradient algorithm is used in characterization matrix. To calculate the reprojection in the encrypted domain characterization matrix is used. Also he propose the probabilistic analysis model for protecting the privacy of user. Probabilistic factor analysis model is used for to protect the privacy of user.

In [1] Cryptosystem is used to process the data in encryption form. Paillier cryptosystem is used for product the encrypted values from which it produce the decryption of message. DGK used sub protocol to increase the efficiency of encryption & decryption over Paillier system.

In [14] distributed method is used to protect the data from entrusted server for maintain the minimum loss of data & to provide the accuracy of system. An offline profile is used to protect the data from server & online profile used to generate the recommendation.

In [15] Data Sparity issue is addressed. From past information of user rating is provide or given to the user. Auto-adaptive imputation method impute the missing values that method used to improve the neighbourhood based CF method for improve the performance.

In [21] The Matrix-Factorization (MF) based models have become popular when building Collaborative Filtering (CF) recommender systems, due to the high accuracy and scalability. Most of nowadays matrix factorization models don't have acceptable execution time during to large datasets. In this article, we introduce a new collaborative filtering recommender system, based on matrix factorization by using genetic algorithm.

In [22] it compares the efficiency of the semantic approach with the traditional collaborative filtering in recommender systems applied to the field of audio-visual contents.IT use the actual data from Movie Lens database to train the recommenders' algorithms and to compare results. Ontology for the audio-visual content was developed importing data from IMDB. For the sake of reproducibility the novel Lens Kit platform has been utilized.

.

III. IMPLEMENTATION DETAILS

A. *System Architecture*

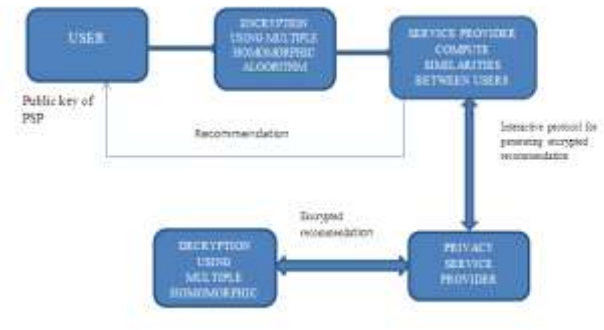

Fig 1: Proposed System Architecture

The main aim of system is to generate the recommendation as per user's requirement. Also the system is used for the security purpose. Firstly user registers the credentials for purchase the product or accessories. Either existing user or new user is login. After filling the information there are many different accessories or product shown. The active participation of user is requiring only for register the personal data. User can buy the product as well as user can see any recommendation related to product. After filling the information like Name, Phone number, password and Account-No, homomorphic algorithm is used for encryption data.

Service provider (SP) computes the similarities between two users. Then generate the recommendation & it sends to the user. Privacy service provider (PSP) is semi trusted third party which can interact with service provider for encrypt data.

Service provider & privacy service provider uses interactive protocol for generating encrypted recommendation. Also privacy service provider is decrypting the data using multiple Homomorphic algorithm.

B.Problem Statement

The Homomorphic encryption is encryption on the already encrypted data rather than original data.it works on plain text. Complex mathematical operation is done on cipher text. Multiple Homomorphic algorithm designing the protocol that is used for to provide the security of user's personal data.

In existing system heavy computational and communication overload is occur so to remove drawback multiple homomorphic algorithm is used.

In proposed system the user fills the personal information to purchase the items then algorithm is used to encrypt the data of user. Then service provider computes similarities between users with other user to generate the recommendation. Then privacy service provider and service provider interact with protocol for generating the encrypted recommendation. That means personal information of user is hide that doesn't access by any other service provider hence data is secured.

ISSN: 2321-8169
4690 - 4694

C .Algorithm Representation

Step 1: Register User
Step 2: Login using register credentials (username, password)
Step 3: Buy products or Accessories. Stored encrypted data in the database
Step 4: Encrypt data using Homomorphic Algorithm. Following algorithm is used

$$C1=E_{pk}(m1) \quad \text{AND } C2=E_{pk}(m2) \qquad (1)$$

With noise n1 & n2 respectively. We multiply these encryptions using homomorphic property SHE scheme then encryption is

$$C3=E_{pk}(m1*m2) \qquad (2)$$

Having m1*m2 under key p_k but C3 will now have noise n1*n2.Here first we have to C3 &S_k under p_k. This result generate two new cipher text

$$C4=E_{pk}(C3)=E_{pk}(Epk(m1*m2)) \text{ AND } C5=E_{pk}(sk) \qquad (3)$$

Step 5: Whenever new user buy a product recommendation is generated of the registered user & data is hided of register user from the new user.

D. Mathematical Representation

Input set: (U, P, I, R),
Where, U is No. of users, I is set of items, R is rated items ,P is Password.
Process:

a. Login (U,P)
b. Input item (Ri)
c. Encryption of data Ri
d. Ep, q, t : q^t modp → c1
e. Ep, q, t : yt* Ri mod p →c2
f. C1=(c1,c2),
g. C= { C1,C2,C3.. }
h. SP →C

Output set: User Recommendation.

E.Work Done

Input dataset

For implementation we use database as My SQL. And following tables are involved for showing the efficiency of proposed approach with its working. From given table it shows the recommender system for purchase items of customer.It only display the customer name and item which is buy.but other information like accno,userid, and password is encrypted.

Fig 2: Input dataset

F. Flow of Multiple Homomorphic Algorithm

- The First step is registering the user's credentials like personal information.
- Then If user wants to buy any product then he has to fill the personal information. User has three chances to provide correct password otherwise it generate the CAPTCHA for security purpose.
- After filling information personal data will be hide using multiple homomorphic algorithm.as well as user has right to see the generated recommendation but personal data like account_no, password is hide. Only user sees the name of particular user who buys the product & item.

G. Experimental Setup

Hardware Configuration

- Processor-Pentium IV
- Speed-1.1 GHz
- RAM-256 Mb(min)
- Hard Disk-20GB
- Key Board-Standard Windows Keyboard
- Monitor-SVGA

Software Configuration

- Operating System-Windows Xp/7/8
- Programming Language: Java
- Tool-Net Beans

IV. RESULTS AND DISCUSSION

This is the first step login either existing user or new user.

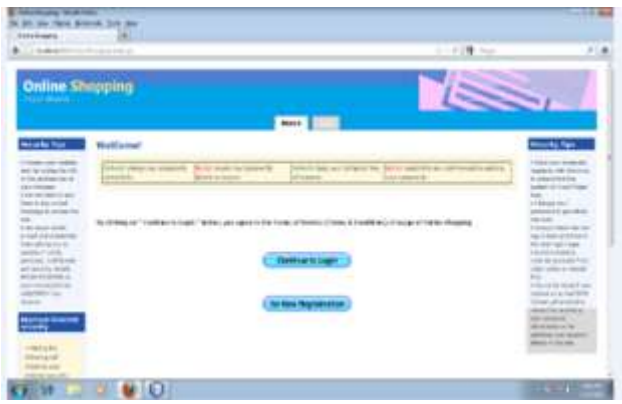

Fig 3: Login Form

ISSN: 2321-8169
4690 - 4694

If three times password is wrong then it generate the CAPTCHA for providing security from malicious user.

Fig 4: Security Provide Using CAPTCHA Technique.

Login to online shopping

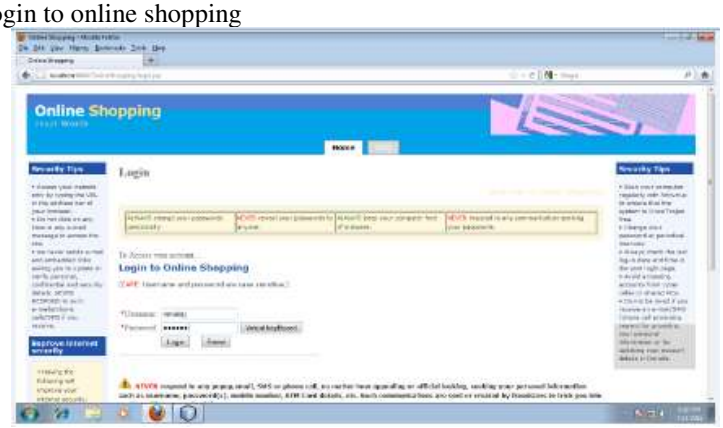

Fig 5: Security Provided using Virtual Keyboard.

Generating the recommendation that user wants to see that previous purchase items.

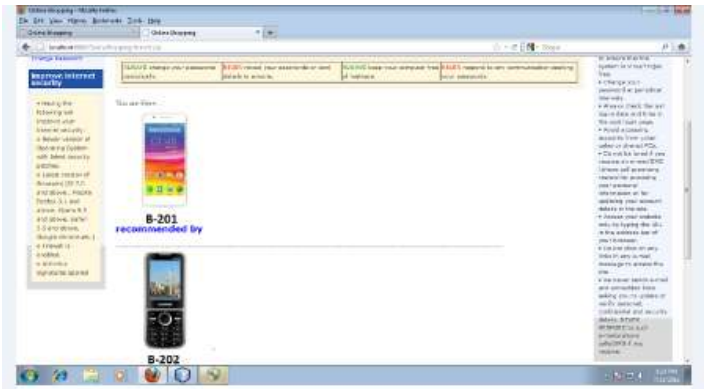

Fig 6: Recommendation Generation for user

Display the items that is encrypted by using homomorphic algorithm.which is the output that generate the recommendation as per users choice but the recommended data should be hide from other service provider or from customers.

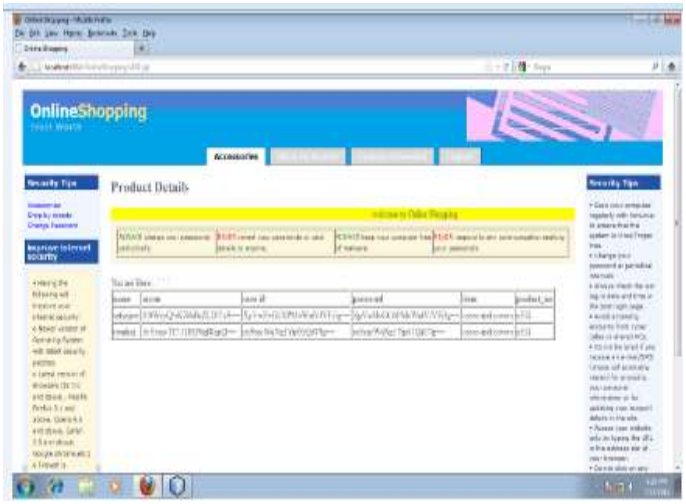

Fig 7: Encrypt the data of user

V.CONCLUSION AND FUTURE ENHANCEMENT

- Homomorphic algorithm is used for the encrypting user's sensitive data for security purpose.
- CAPTCHA and Virtual keyboard is also used for providing security purpose.
- Future work will system can expand into dynamic recommender system for many real life things.

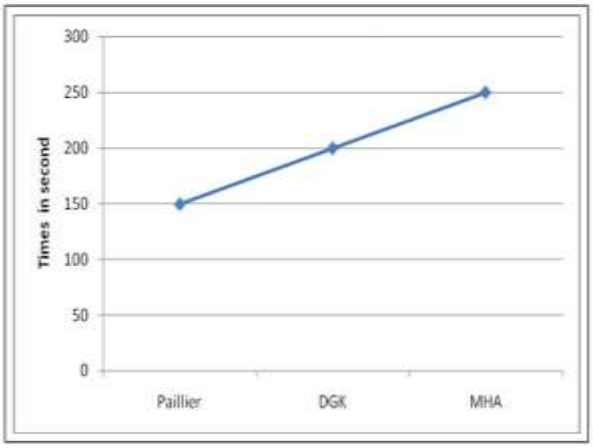

Fig 8: Comparison of different algorithm with time

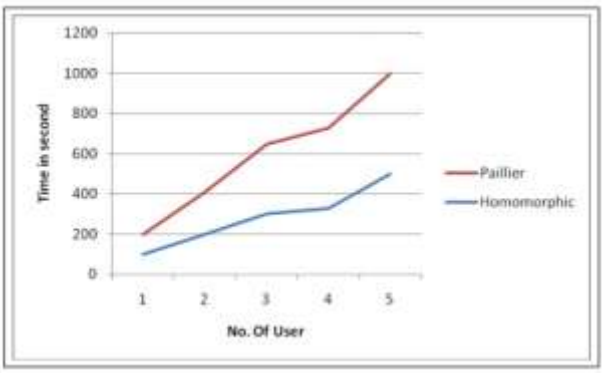

Fig 9: Average runtime of protocol to generate recommendation

ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Mrs.Sonali Patil for her exemplary guidance, monitoring and constant

Encouragement throughout the course of this project. I also take this opportunity to express a deep sense of gratitude to my Head of the department Mrs. P. Kalokhe, PG Coordinator Mrs. Sonali Patil for her cordial support, valuable information and

Guidance. Thanks to all those who helped me in completion of this work knowingly or unknowingly like all those researchers, my lecturers and friends.

REFERENCES

[1] Zekeriya Erkin,Thijsveugen,Tomas Toft,& Reginald L. Lagendijik, "Generating Private Recommendations Efficiently Using Homomorphic Encryption and Data Packing", IEEE Trans. On Information Forensics and Security, vol.7, No.3, June 2012

[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 Computer, vol. 5, no. 6, pp. 54–63, Nov./Dec. 2001.

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

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

[6] J. F. Canny. Collaborative filtering with privacy. In IEEE Symposium on Security and Privacy, pages 45–57, 2002.

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

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

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

[10] I. Damgård, M. Geisler and M.Krøigaard, ―Efficient and secure Comparison for online auctions,‖ in Proc. Australasian Conf.Information Security and Privacy (ACSIP 2007), ser. LNCS, J. Pieprzyk, H.Ghodosi and E. Dawson, Eds., Jul. 2–4, 2007, vol.4586, pp.416–430, Springer.

[11] Z. 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.

[12] F. Canny. Collaborative filtering with privacy. In IEEE Symposium on Security and Privacy, p ages 45–57, 2002.

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