Privacy Preserving Dynamic Recommender System

Umakant L Tupe
M.E Student at MMCOE

R.B. Joshi
Department of Computer Engg

ABSTRACT

A Recommender System is now becoming main decision maker in today's word. It provides information for specific items such as books, news, cloths and many more. Personalization is now becoming common term for improving e-commerce services and attract more users. Todays recommender system provides suggestion for specific items but drawback that service provider can increases the ratings of specific product and unnecessarily popularity increases. This leads to misguiding the users while purchasing some products, so privacy is violated. Our main aim is to preserve privacy, so we have used homomorphic encryption scheme which uses no. of public private keys to preserve privacy. We have used PSP to remove active participation of user in encryption and decryption. In this paper we propose a cryptographic solution for preserving privacy of customers in recommender system. In short private information of customer is kept secret and service provider generates recommendation by processing encrypted data.

Keywords

Homomorphic Encryption, Dynamic Recommender System.

1. INTRODUCTION

1.1 Online Shopping

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

1.2 Facebook

In Facebook, People share their personal images, videos and send to third parties, user's data is collected from click logs and profiles. From all of the above services people get benefit but direct access to private data of user have potentially risk that their important ratings get violated, Recent study 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.

2. OUR CONTRIBUTION

In our proposed work we aim to generate private recommender system which is dynamic, flexible and user get updated products. We used PSP which generates public and private keys, modulus, phi and generate encrypted ratings. when user give rating to some product, no one will decrypt the ratings because ratings are in encrypted format. SP also unable decrypt it .Homomorphic algorithm uses n-bit public private keys for preserving privacy. So user privacy is maintained and not violated from SP.

3. LITERATURE SURVEY

In previous recommender system privacy is maintained but not the accuracy, when system tries to get accuracy we don't get accuracy so little bit tradeoff between privacy and accuracy. This happens due to distributed aggregation. In some scenario, techniques 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]. An agent system is used for privacy preservation in online services. The drawback of this method is that it requires trusted software and secure environment however our method does not have this drawback[11].Collaborative forecasting and benchmarking is used to increase forecast and data creation using cryptographic technique. The drawback of this method is cryptographic method in this paper is not privacy preserving but in our paper cryptographic method are privacy preserving [12]. 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] In Canney's recommender system cryptographic technique used which causes heavy computation and communication burden on Recommender system[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.

4. IPMLEMENTATION DETAIL

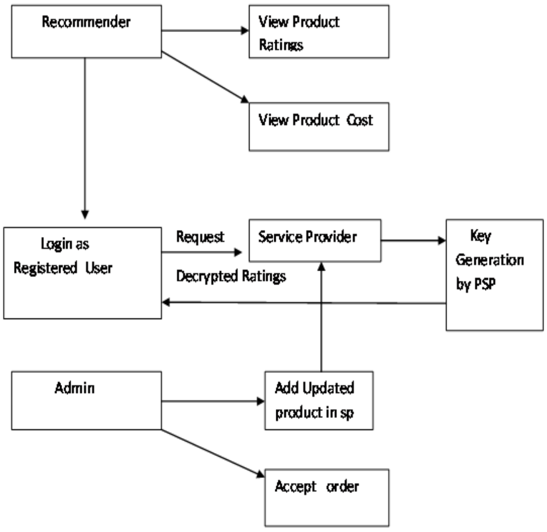


Fig.1 System Architecture

Proposed System contains Service Provider, Privacy Service Provider and Users. It contains Dynamic Module which will add new products and show to users.

4.1 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.

4.2 Privacy Service Provider

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

4.3 Recommender

Recommender is a just a user who visit recommendation system for purchasing some products or to see some offers are there or to give ratings for ordered products.

In this, new user can see, new products, their rate, description of products. When Recommender want to buy products he must login into Recommender system and then only he can buy products, so only registered user will give ratings and no other user will give rating. So rating given to product will be true ratings and no pretreated rating.

At a time only 1 user will give 1 rating then rate button will be disable that means user1 will not give more ratings to single product and product popularity will not be increased. Like this SP will not give more ratings to products.

4.4 Admin

Admin will allow products or accept orders ordered by user. Then ordered will be delivered to specified users location. Admin can add manufacturer, add products, add category, confirm order given by user and then new added products will be seen by recommender. That is our system is dynamic recommender system .new products will be added and updated to database and will be seen by user. User can rate products which will be saved in database in encrypted format so, ratings given by user are in encrypted format and seen by anyone, so user privacy is maintained.

4.5 Homomorphic Algorithm

4.5.1 Key Generation

(a) Homomorphic(int N)

(b) Pass to this N number i.e. 100 as a input

(c) Calculate P=N/2 (Biginteger Number i.e. 1000,2000, etc)

(d) Calculate Q=N/2 (Biginteger Number i.e. 1000,2000, etc)

(e) Calculate Phi as //variable name to calculate public key.

(f) Biginteger phi=(p.subtract(one)).multiply(q.subtract(one));

(g) Calculate modulus as modulus=p.multiply(q);

(h) Calculate Public Key i.e. 2^16+1 = 65537

(Because of it's a common value of public key when we run a project n times we get a common public value as above.)

(i) Calculate Private Key

PrivateKey=PublicKey.modInverse(phi);

4.5.2 Encrypt

(a) Take the rating from user i.e. 3,4,2

(b) Convert this rating into Biginteger no.

(c) Call encrypt function and pass ratings as a message & modulus as a Biginteger no.

(d) Pass public key & modulus to message.modpow function

(e) We get Biginteger message (encrypted message as a rating)

4.5.3 Decrypt

(a) Pass encrypted ratings, private key & modulus to decrypt function.

(b) Encrypt message.modpow(pk,md)

(c) Get decrypted ratings.

We have used homomorphic algorithm for security reason. In most RecSys they have used different algorithm but this algo is magic.We can generate n-bit private key generation using this algo.We can work on large data set say 5 lakh products so we will generate 2^20+ 1 product key. Where user give ratings at 1 time then private key will be generated, this private key and public key will be used and then encryption will be done of user ratings. This encrypted ratings will be stored in database by SP in encrypted format, so privacy is preserved from SP. During single login only user can rate product at once then rate button will be disable, so no one will give more ratings to single product. Using this algorithm scalability achieved which was drawback of earlier system. Using this algo we can work on large data set. Response time of our system is 0.002 seconds for clicking 1 product and also encryption and decryption time is 1 ms.

4.6 Dynamic Updation of Products

This algorithm works for dynamic updation of products that means when new product added then it is placed into database, like this every new entry of products will be increased and we get large data set. When user request for new products then dynamic update system fetch the products and will show to user.

Step 1. User request for product information

Step 2: Admin update new products in the web application

Step 3: Dynamic update system creates a stack k & pushes set Pnew on dynamic system product stack.

Step 4: When user request for product information system checks dynamic system products stack & uses it for generating recommendation privately.

Step 5: SP sends updated stack to PSP for private recommendation generation and continuously polls for updated stack. SP also estimates time required for completion of private recommendation generation for sent product stack using no. of concurrent user, historical data & computational power Tp.

Step 6: SP waits for Tp time to get private recommendation over & meanwhile if dynamic system product stack gets updated then aborts previous private recommendation generation with updated product state P+Pnew.

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.

4.7 Workflow of Proposed System

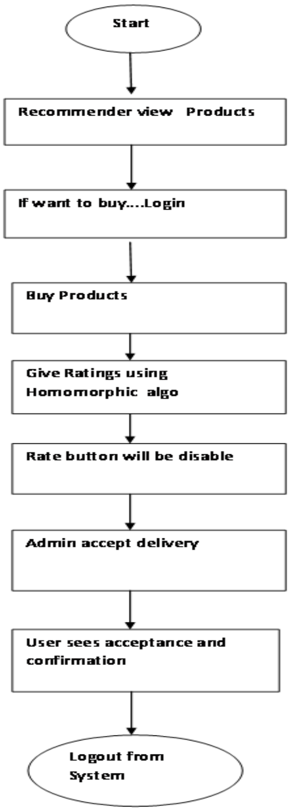

Start
Recommender view Products
If want to buy....Login
Buy Products
Give Ratings using Homomorphic algo
Rate button will be disable
Admin accept delivery
User sees acceptance and confirmation
Logout from System

Fig.2 Workflow of Proposed System

4.8 Data Set

4.8.1 Static System:

Fixed data set of amazon store. Which is sample data set used by amazon for testing purposes.

Items: Books,Musics,Video,DVDS

4.8.2 Dynamic System:

Data of various manufacturers like LG, Lenova, Samsung cost of these products from flipcart, amazon.

4.8.3 Input:

15000 people and their ratings in encrypted format for 1001 items.

4.8.4 Output:

Encrypted Recommendation

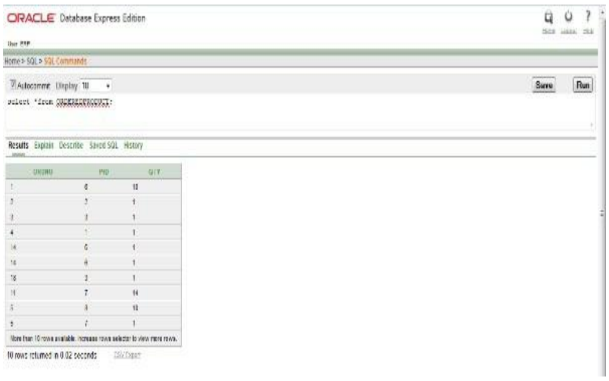
4.9 Result Set

4.9.1 Security Analysis by Statistical Approach

A good encryption scheme should resist all kinds of known attacks, such as known plain text attack, cipher-text attack, statistical attack, differential attack, and various brute-force attacks. Some security analysis techniques perform on the Homomorphic encryption scheme, including the statistical analysis and key space analysis.

4.9.1.1 Statistical Analysis:

Statistical analysis has been performed on the Homomorphic, Dynamic updation of products and response time to execute query and also time required for encryption and decryption of ratings. Demonstrating its superior performance compare to other recommender.



```
select *from ORDEREDPRODUCT;
```

ORDNO	PID	QTY
1	6	10
2	3	1
3	3	1
4	1	1
14	6	1
16	8	1
18	3	1
11	7	14
5	8	10
9	7	1

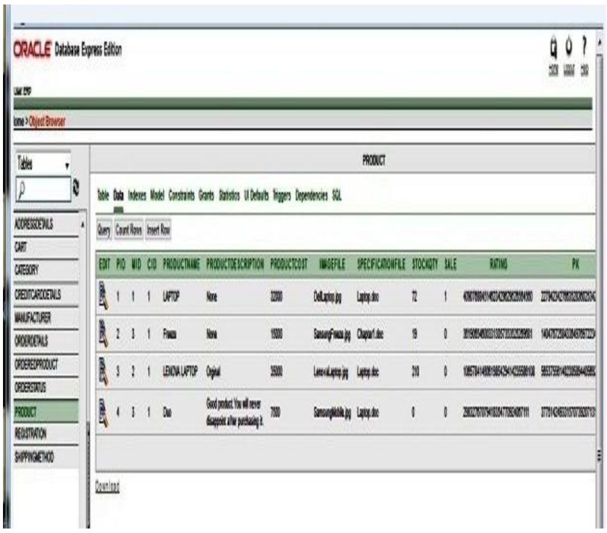
More than 10 rows available. Increase rows selector to view more rows.

10 rows returned in 0.02 seconds

Fig.3 Response time to execute query in Recommender System is 0.002 seconds

4.9.2 Performance of Homomorphic Algorithm w/r/b Encryption

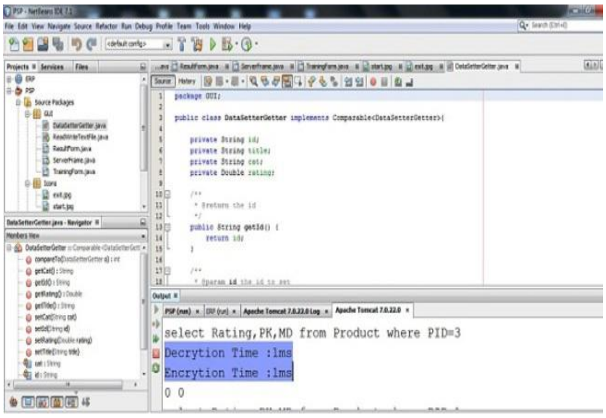
Apart from security considerations, some other issues for homomorphic algorithm are also important. This includes the running speed, particularly for real time encryption and decryption of ratings.



PRODUCT

EDIT	PID	MID	CID	PRODUCTNAME	PRODUCTDESCRIPTION	PRODUCTCOST	IMAGEFILE	SPECIFICATIONFILE	STOCKQTY	SALE	RATING	PK
	1	1	1	LAPTOP	None	32000	DellLaptop.jpg	Laptop.doc	72	1	[illegible]	[illegible]
	2	3	1	Freeza	None	15000	SamsungFreeza.jpg	Chapter1.doc	19	0	[illegible]	[illegible]
	3	2	1	LENOVA LAPTOP	Orginal	35000	LenovaLaptop.jpg	Laptop.doc	210	0	[illegible]	[illegible]
	4	3	1	Duo	Good product. You will never disappoint after purchasing it.	7000	SamsungMobile.jpg	Laptop.doc	0	0	[illegible]	[illegible]

Fig.4. GUI of encrypted ratings at service provider site



```
package GUI;

public class DataSetterGetter implements Comparable<DataSetterGetter>{

    private String id;
    private String title;
    private String cat;
    private Double rating;

    /**
     * @return the id
     */
    public String getId() {
        return id;
    }

    /**
     * @param id the id to set
```

```
select Rating,PK,MD from Product where PID=3
Decrytion Time :1ms
Encrytion Time :1ms
0 0
```

Fig.5 Encryption and Decryption Time in RecSys

5. CONCLUSION

Recommendation System has become important tool for personalization of online services. However Traditional data protection techniques do not preserve the privacy of users while generating Recommendations.

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 could be done where many users' attributes will be considered for recommendation generation.

6. 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 take this opportunity to express my deep sense of gratitude towards my esteemed guide **Prof. Ram Joshi** for giving me this splendid opportunity to select and present this topic and also providing facilities for successful completion.

With all respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly.

7. REFERENCES

[1] "Generating Private recommendation using Homomorphic Encryption and Data Packing". IEEE 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. Ramakrishna, 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 2001.

[4] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in Proc.SIGMOD Rec., May 2000, vol. 29

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

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

[7] H. Polat andW. Du, "SVD-based collaborative filtering with privacy," in Proc. 2005 ACM Symp. Applied Computing (SAC'05), New York, NY, 2005, pp. 791–795, ACM Press.

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

[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] 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 , New York, NY, 2009, pp. 627–636, ACM.

[11] 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.

[12] 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.

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

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

[16] 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.

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

[18] 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. no. 1, pp. 180–187, Mar. 2010.