PROTECTING YOUR SHOPPING PREFERENCE WITH DIFFERENTIAL PRIVACY

B. S Murthy [1], K. Vinod,

[1]**Assistant professor(HOD) , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - Suryanarayanamurthy.b@gmail.com
[2]**PG Student of MSC (cs), Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - vinodhankathula425@gmail.com

ABSTRACT

Online banks may disclose consumers' shopping preferences due to various attacks. With differential privacy, each consumer can disturb his consumption amount locally before sending it to online banks. However, directly applying differential privacy in online banks will incur problems in reality because existing differential privacy schemes do not consider handling the noise boundary problem. In this paper, we propose an Optimized Differential private Online transaction scheme (O-DIOR) foronline banks to set boundaries of consumption amounts with added noises. We then revise O-DIOR to design a RO-DIOR scheme to select different boundaries while satisfying the differential privacy definition. Moreover, we provide in-depth theoretical analysis to prove that our schemes are capable to satisfy the differential privacy constraint. Finally, to evaluate the effectiveness, we have implemented our schemes in mobile payment experiments. Experimental results illustrate that the relevance between the consumption amount and online bank amount is reduced significantly, and the privacy losses are less than 0.5 in terms of mutual information

1 INTRODUCTION

In the last decade, online banks were commonly used to provide financial services. However, online banks are vulnerable to outsider and insider attacks. Outsiderattacks include brute-force attacks, distributed attacks and social phishing. Insider attacks are data misused by people with authorized access. Outsider and insiderattackers can collect the financial information of consumers to infer personal shoppingpreferences, consumption patterns or credit statistics. If consumers' shopping records are disclosed, consumers may receive advertisement recommendation, harassing message and fraud emails. More seriously, it contributes to loan promotion, illegal investigation, property fraud, and even kidnapping. If consumers have no reasonable assurance of their accounts, they would be reluctant to use online banks, leading to userloss and higher cost for online banks. Therefore, appropriate methods are required to stem the erosion of privacy rights in online banks. To protect consumers' privacy, existing approaches mostly used cryptography. Cryptography schemes mainly utilizedencryption technology and authentication technology, which could prevent illegitimateand unauthorized access.

Literature Survey

Protecting shopping preferences with differential privacy involves ensuring thatindividual preferences or behaviours cannot be accurately determined from the data released. Here's a literature survey on this topic:

Differential Privacy: A Survey of Results (Dwork, 2008):

This foundational paper discusses the concept of differential privacy, which aims to provide strong guarantees about the privacy of individual data points in a dataset while still allowing for accurate analysis.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

If consumers' shopping records are disclosed, consumers may receive advertisement recommendation, harassing message and fraud emails. More seriously, it contributes to loan promotion, illegal investigation, property fraud, and even kidnapping [11]. If consumers have no reasonable assurance of their accounts, they would be reluctant to use online banks, leading to user loss and higher cost for online banks. Therefore, appropriate methods are required to stem the erosion of privacy rightsin online banks.

Proposed System & alogirtham

we propose an optimized differential private online transaction scheme (O- DIOR), in which we define a new noise probability density function. The fundamentalstrategy is to basically eliminate the probability that noise is generated beyond the boundaries. The scheme can satisfy the differential privacy definition because the noisecan be any value in a valid range to avoid the case that the consumption amount and noise can be inferred.

IMPLEMENTATION

In this module, the admin has to login by using valid user name and password. After login successful he can do some operations such as View all users and authorize,View all Transport Users and authorize, Register and Login (With Bank Name), Viewall users and authorize ,View All Transport company users and authorize, Add bank with its details such as name, address ,location, bpin, mailed ,bcno ,add building image,View Credit card request and Process with Ac. No and CRN, credit limit, Card cvv (4digit) number Cash Limit., View all transport booking fees details for each company based on cluster ,View all transport booked details for each company based on cluster,View all type of Fraud based on cluster, View all users with Fraud and give link to show number of same user is fraud in chart.

5 RESULTS AND DISCUSSION

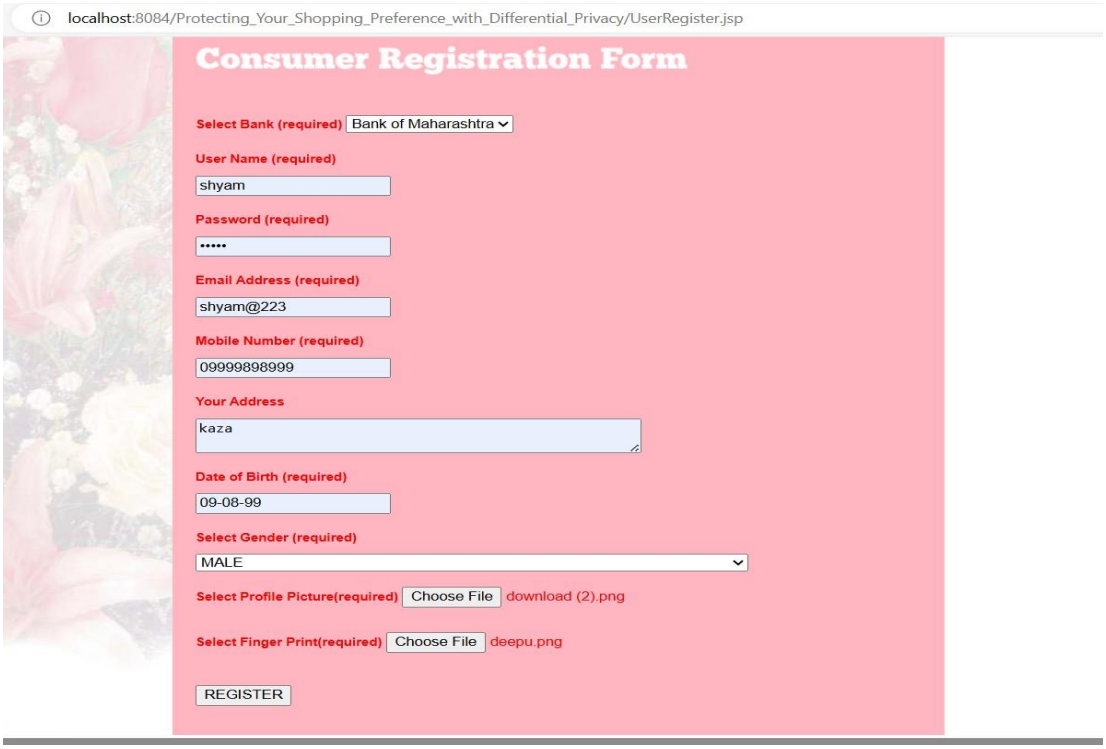
5.1 Home Page

Fig 5.1 Home Page

5.2 Admin Registration

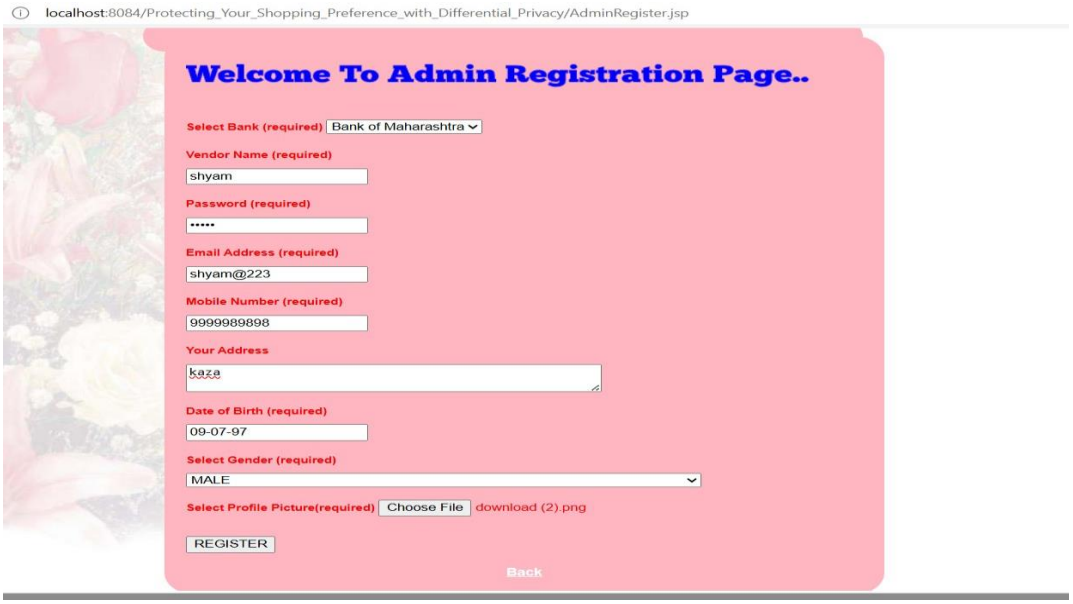
5.2 Admin Registration

5.3 Consumer registration



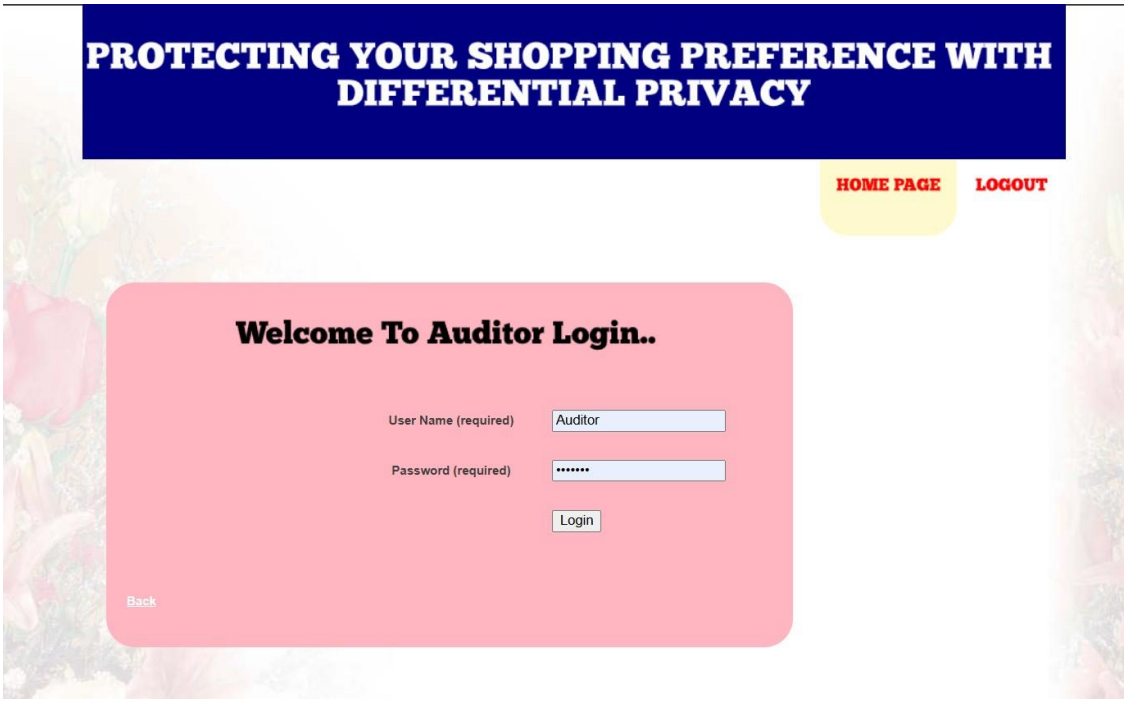
5.3Consumer Registration

5.4 Merchant Registration



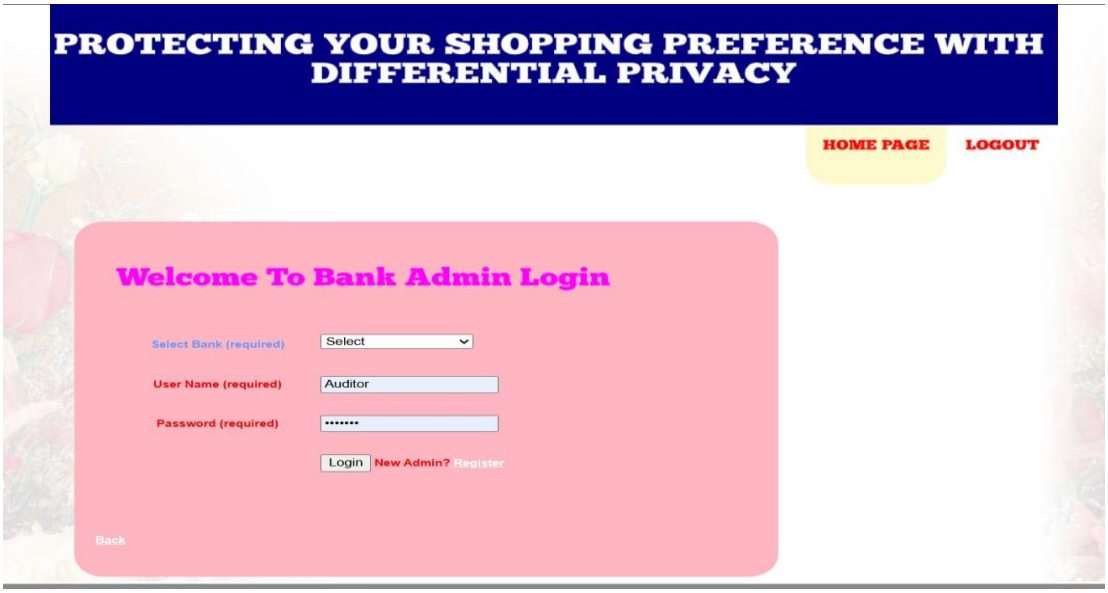
5.4 Merchant Registration

5.5 Auditor Login



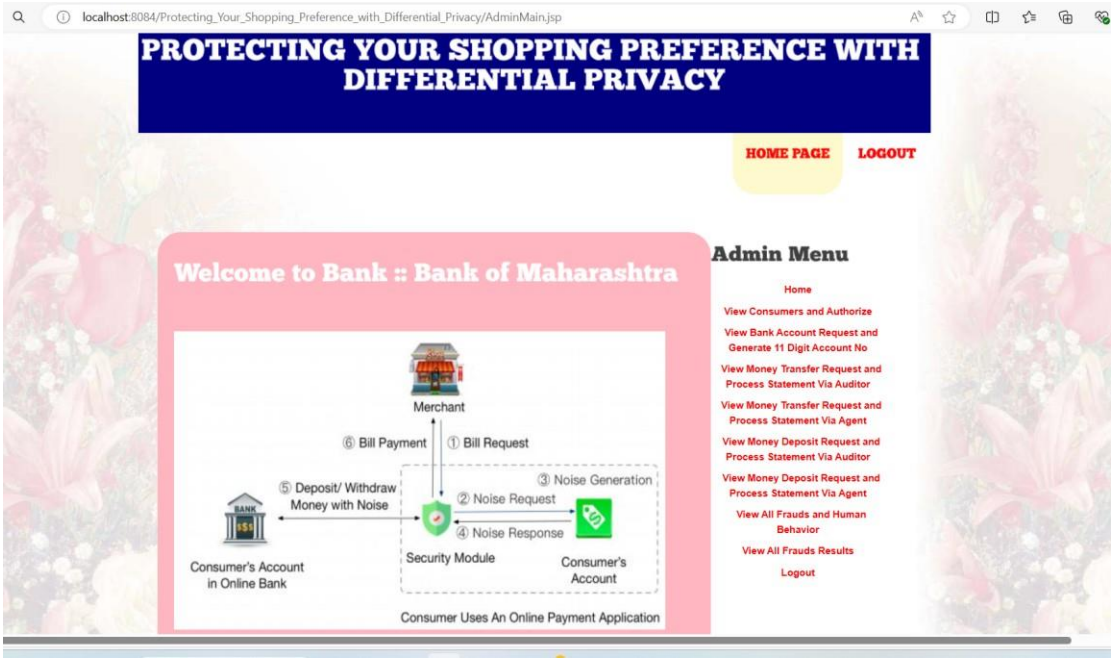
5.5 Auditor Login

5.6 Admin Login



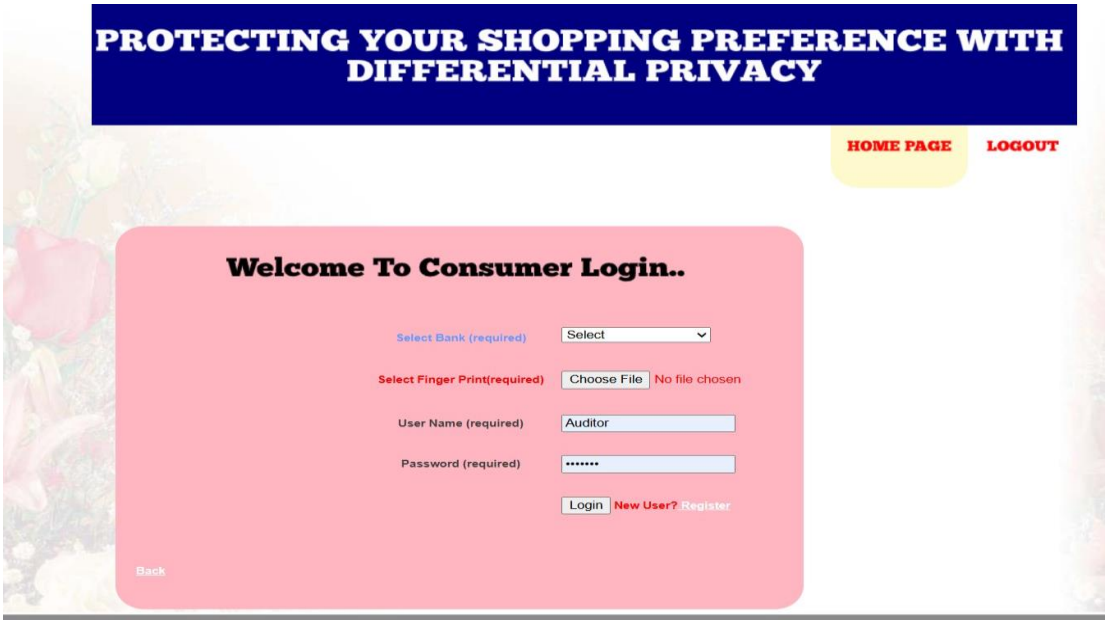
5.6 Admin Login

5.7 Admin Menu



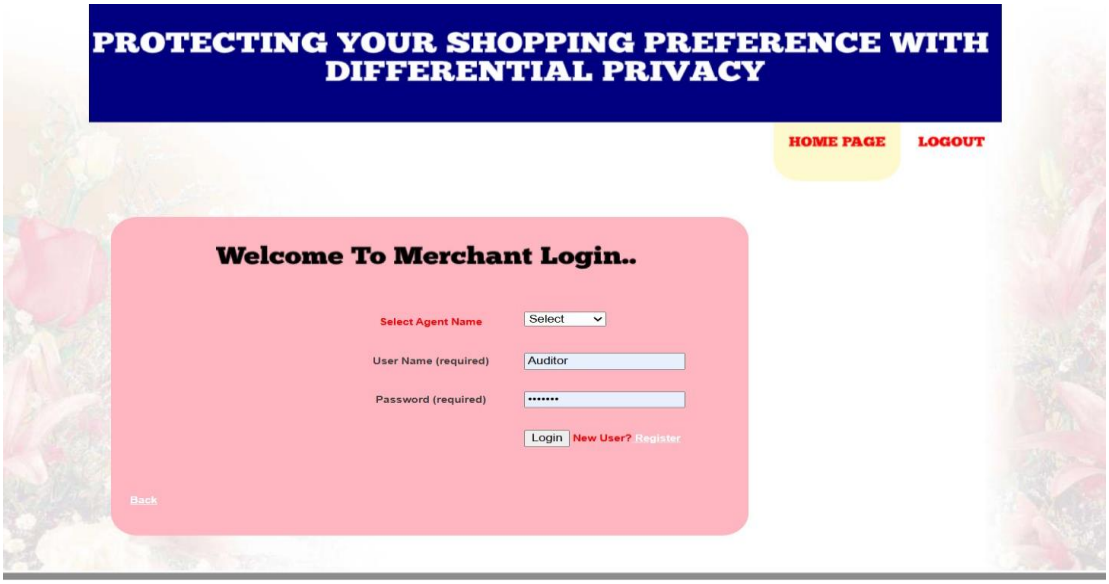
5.7 Admin Menu

5.3.8 Consumer Login



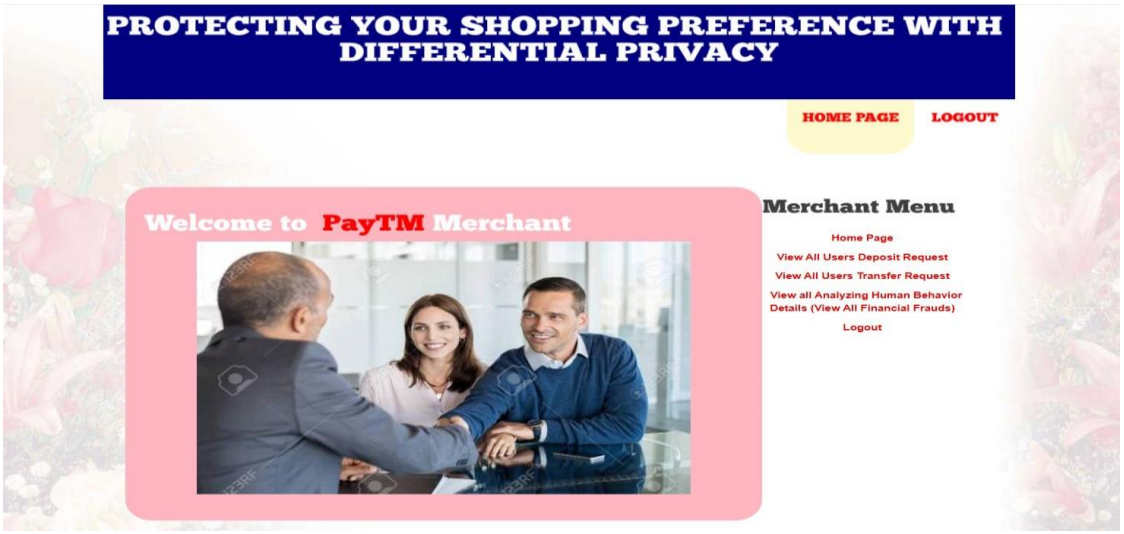
5.8 Consumer Login

5.9 Merchant Login



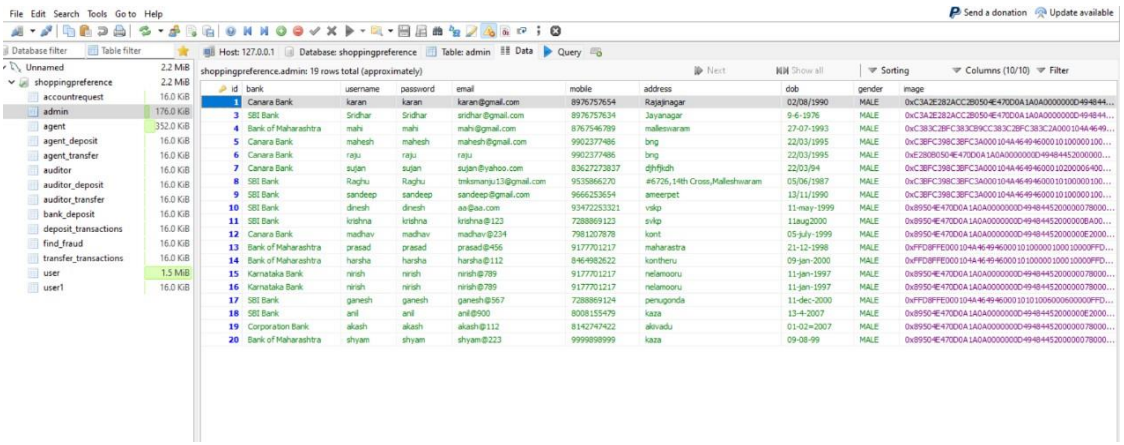
5.9 Merchant Login

5.10 Merchant Menu



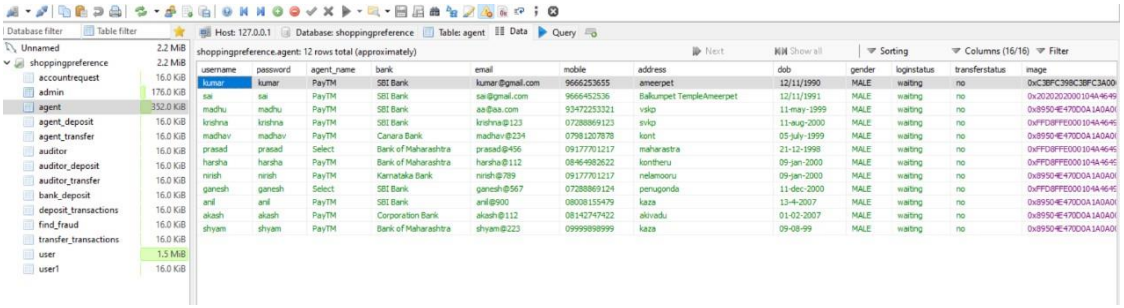
5.10 Merchant Menu

5.11 Admin Data



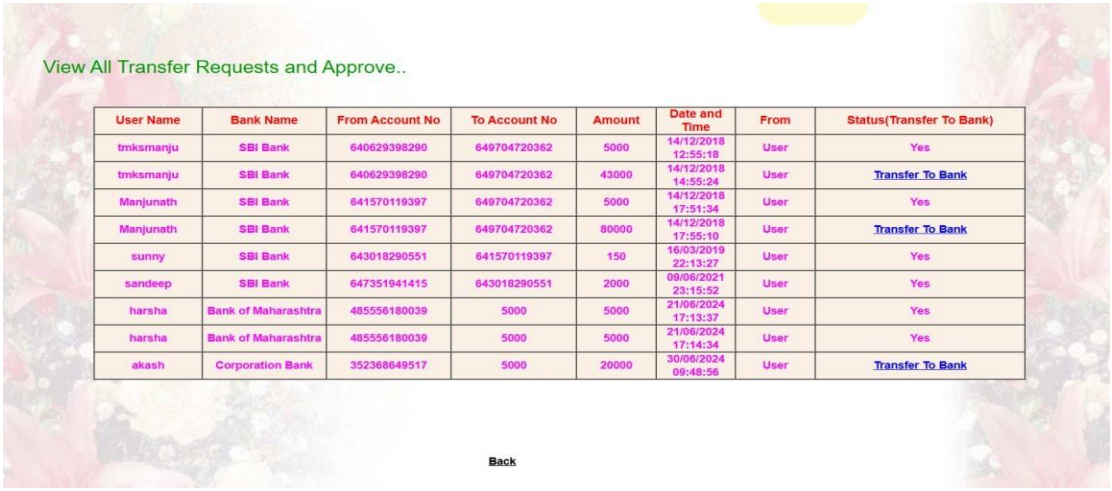
Admin Menu

5.11 agent data



5.12 Agent Data

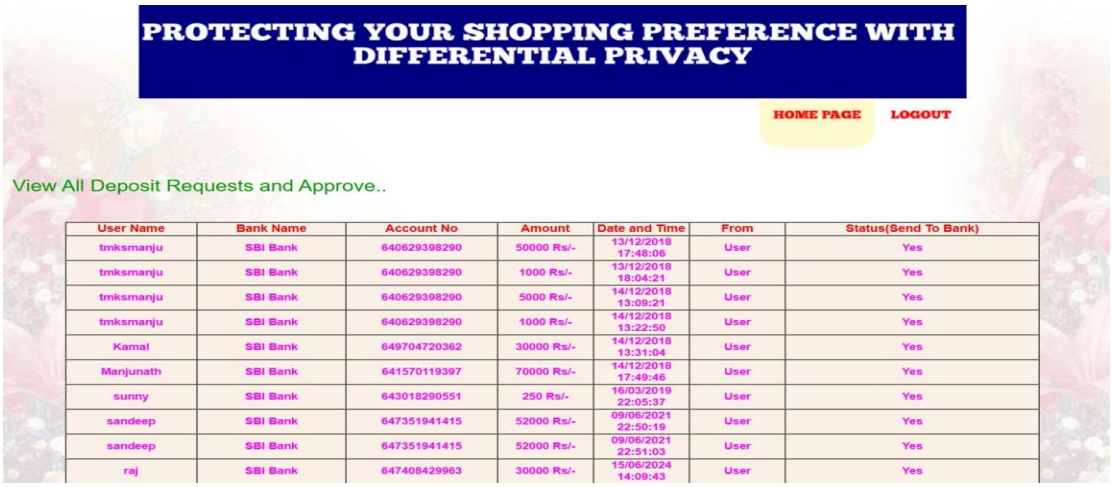
5.13 transfer data



User Name	Bank Name	From Account No	To Account No	Amount	Date and Time	From	Status(Transfer To Bank)
tmksmanju	SBI Bank	640629398290	649704720362	5000	14/12/2018 12:55:18	User	Yes
tmksmanju	SBI Bank	640629398290	649704720362	43000	14/12/2018 14:55:24	User	Transfer To Bank
Manjunath	SBI Bank	641570119397	649704720362	5000	14/12/2018 17:51:34	User	Yes
Manjunath	SBI Bank	641570119397	649704720362	80000	14/12/2018 17:55:10	User	Transfer To Bank
sunny	SBI Bank	643018290551	641570119397	150	16/03/2019 22:13:27	User	Yes
sandeep	SBI Bank	647351941415	643018290551	2000	09/06/2021 23:15:52	User	Yes
harsha	Bank of Maharashtra	485556180039	5000	5000	21/06/2024 17:13:37	User	Yes
harsha	Bank of Maharashtra	485556180039	5000	5000	21/06/2024 17:14:34	User	Yes
akash	Corporation Bank	352368649517	5000	20000	30/06/2024 09:48:56	User	Transfer To Bank

5.13 Transfer Data

5.14 Deposit Request



User Name	Bank Name	Account No	Amount	Date and Time	From	Status(Send To Bank)
tmksmanju	SBI Bank	640629398290	50000 Rs/-	13/12/2018 17:48:06	User	Yes
tmksmanju	SBI Bank	640629398290	1000 Rs/-	13/12/2018 18:04:21	User	Yes
tmksmanju	SBI Bank	640629398290	5000 Rs/-	14/12/2018 13:09:21	User	Yes
tmksmanju	SBI Bank	640629398290	1000 Rs/-	14/12/2018 13:22:50	User	Yes
Kamal	SBI Bank	649704720362	30000 Rs/-	14/12/2018 13:31:04	User	Yes
Manjunath	SBI Bank	641570119397	70000 Rs/-	14/12/2018 17:49:46	User	Yes
sunny	SBI Bank	643018290551	250 Rs/-	16/03/2019 22:05:37	User	Yes
sandeep	SBI Bank	647351941415	52000 Rs/-	09/06/2021 22:50:19	User	Yes
sandeep	SBI Bank	647351941415	52000 Rs/-	09/06/2021 22:51:03	User	Yes
raj	SBI Bank	647408429963	30000 Rs/-	15/06/2024 14:09:43	User	Yes

5.14 Deposit Request

6. CONCLUSION AND FUTURE WORK

protecting user data with differential privacy is a challenging problem for onlinebanks. the method of directly applying differential privacy is illustrated in a dior scheme. in this paper, we propose o-dior, a differential private online transaction scheme to address privacy concerns during financial transactions. o-dior can set boundaries of consumption amount with added noise, considering the range of accountbalance in reality.

with a payment application as a noise generator, activities and behaviours of consumers cannot be inferred from consumption records. next, we further revise o-diorto propose ro-dior, satisfying the need of selecting different boundaries. moreover, in- depth theoretical analysis has proved our schemes can satisfy the constraint of differential privacy.

7. REFRENCES

[1] S. Nila Kanta and K. Scheibe, "The digital personal and trust bank: A privacy management framework," Journal of Information Privacy and Security, vol. 1, no. 4, pp. 3–21, 2005.

[2] K. J. Hole, V. Moen, and T. Solstheim, "Case study: Online banking security," IEEE Security & Privacy, vol. 4, no. 2, pp. 14–20, 2006.

[3] A. Rawat, S. Sharma, and R. Sushil, "Vanet: Security attacks and its possible solutions," Journal of Information and Operations Management, vol. 3, no. 1, p. 301, 2012.

[4] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research," Insider Attack and Cyber Security, pp. 69–90, 2008.

[5] E. E. Schultz, "A framework for understanding and predicting insider attacks," Computers & Security, vol. 21, no. 6, pp. 526–531, 2002.

[6] C. Herley and D. Florencio, "Protecting financial institutions from ˆ brute-force attacks," in Proc. IFIP International Information Security Conference, 2008.

[7] A. Householder, K. Houle, and C. Dougherty, "Computer attack trends challenge internet security," Computer, vol. 35, no. 4, pp. 5–7, 2002.

[8] T. N. Jagatjit, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Communications of the ACM, vol. 50, no. 10, pp. 94–100, 2007.

[9] Y.-A. De Mountjoy, L. Radaelli, V. K. Singh et al., "Unique in the shopping mall:On the identifiability of credit card metadata," Science, vol. 347, no. 6221, pp. 536– 539, 2015.

[10] C. Krumme, A. Llorente, M. Cebrian, E. Moro et al., "The predictability of consumer visitation patterns," Scientific reports, vol. 3, p. 1645, 2013.

[11] H. Wang, M. K. O. Lee, and C. Wang, "Consumer privacy concerns about internetmarketing," Communications of the ACM, vol. 41, no. 3, pp. 63–70, 1998.

[12] R. Pathak, S. Joshi, and D. Mishra, "A novel protocol for privacy preserving banking computations using arithmetic cryptography," in Proc. Security and Identity Management, 2009.