GUARDING CONSUMER DATA ENHANCING PREFERENCES WITH DIFFERENCIAL CONFIDENTIALITY

CH.Anil, Assistant Professor CSE, Vaagdevi College of Engineering (Autonomous), India
M.Vandhana, UG student, CSE, Vaagdevi College of Engineering (Autonomous), India
T.Praveen, UG student, CSE, Vaagdevi College of Engineering (Autonomous), India
S.Pavan kumar, UG student, CSE, Vaagdevi College of Engineering (Autonomous), India
P.Sai kumar, UG student, CSE, Vaagdevi College of Engineering (Autonomous),India

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) for online 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
Keywords:

INTRODUCTION
IN the last decade, online banks were commonly used to provide financial services. However, online banks are vulnerable to outsider and insider attacks. Outsider attacks include brute-force attacks, distributed attacks and social phishing [1]. Insider attacks are data misused by people with authorized access. Outsider and insider attackers can collect the financial information of consumers to infer personal shopping preferences, 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 user loss 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 utilized encryption technology and authentication technology [2], which could prevent illegitimate and unauthorized access. However, it is generally difficult for cryptography schemes to handle insider attacks effectively. Insider attackers can still misuse their authorized access to obtain credit statistics and shopping records. On the other hand, differential privacy can provide strong privacy protection by ensuring the indistinguishability of one entity involvement in the dataset. However, directly applying differential privacy in online banks incurs some problems. The consumption amount with added noise may be beyond the boundaries after transactions as shown in Fig 1. The range of noise under differential privacy is from negative infinity to positive infinity, but in reality the consumption amount with added noise cannot exceed the balance in online bank account, otherwise in the online bank account there is no sufficient deposit to pay for bills. A straightforward method is to delete the noise beyond boundaries and regenerate the noise, but this method would not satisfy the standard definition of differential privacy, so the level of privacy

 Copyright @ 2024 Author

guarantee cannot be controlled. Existing differential privacy approaches have not considered setting boundaries on data with added noise [3].

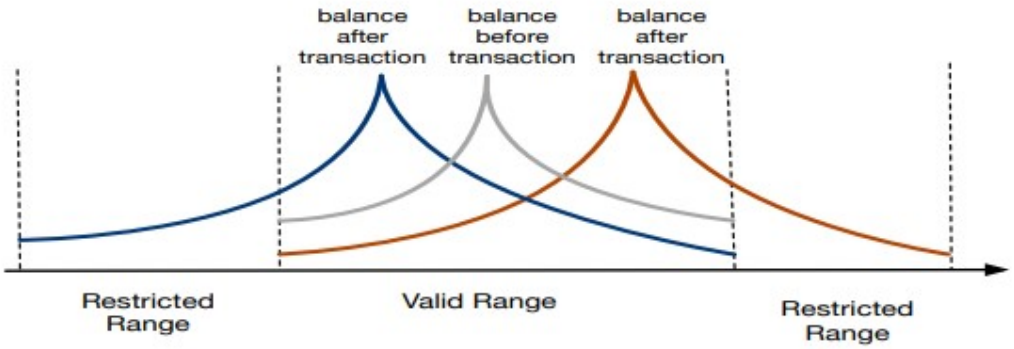


Fig. 1: Valid and restricted range for noise and balance

To address these challenges, we propose an optimized differential private online transaction scheme (O-DIOR), in which we define a new noise probability density function. The fundamental strategy is to basically eliminate the probability that noise is generated beyond the boundaries. The scheme can satisfy the differential privacy definition because the noise can be any value in a valid range to avoid the case that the consumption amount and noise can be inferred. Considering the consumption amount may be great and there is not enough money to generate the noise, we propose a revised O-DIOR scheme (RO-DIOR) [4] to select variable boundaries. We define a new parameter in the noise distribution to adjust boundaries at a time point. We adjust the noise distribution to increase the probability of saving money from a payment application when the consumption amount approaches to zero and increase the probability of withdrawing money from the payment application when the consumption amount approaches to maximum. To implement the scheme, we design a security module for an online payment application to generate and eliminate the noise to guarantee the utility of consumption amounts. Here we take Apple Pay for example. In our scheme, a consumer uses Apple Pay to pay for his bill, obtaining money from his online bank account and Apple Pay account. Apple Pay does not store consumers' card numbers and consumption records that can track consumers, so it cannot know consumers' shopping preferences. Traditionally, Apple Pay directly withdraws money from online banks, our additional step is to use money from consumers' own Apple Pay accounts, which may not incur more security and trust problems. The security module can compute the noise value and assign the consumption amount. For example, a consumer needs to pay $12 to a merchant. Without differential privacy, he needs to withdraw $12 from an online bank, so the actual consumption amount is exposed. With differential privacy, if the security module calculates the noise value as $5 and adds the noise to online bank account, so it needs to withdraw $17 from the online bank, which is not $12 as before. Hence, the personal consumption privacy can be protected. The security module then saves $5 in the Apple Pay to eliminate the added noise, so the actual consumption amount is $12 as before. The consumption record in the online bank is that Apple Pay has withdrawn the money $17 into the consumer's online bank account, so attackers cannot infer the consumer's payment amounts and shopping places in online banks. The main contributions of this paper are summarized as follows. • Our schemes can protect consumption privacy in online banks under differential privacy. The O-DIOR scheme is designed to limit the range of the consumption amount with added noise. O-DIOR [6] is proven to satisfy the differential privacy constraint. • The RO-DIOR scheme is further proposed to select variable upper and lower boundaries of consumption amount with added noise in online banks. The RO-DIOR scheme is also proven to satisfy differential privacy constraint. • The privacy loss is less than 0.5. The performances of schemes have been demonstrated through experiments about different people.

 Copyright @ 2024 Author

LITERATURE SURVEY

1. **Tittle :** A privacy management framework for the digital personal and trust bank.
   Authors : S. Nilakanta and K. Scheibe
   Abstract: In the United States, information privacy and protection is a hot topic in academics and industry. Technological improvements in fields such as data warehousing allow for the aggregation of data from seemingly unconnected sources to generate detailed profiles of individuals, causing privacy advocates to raise their voices in protest. This conflict poses the issue, "Who owns individuals' secondary or transactional information?" Currently, the organisation owns the property. In this study, we propose a paradigm for transferring ownership to individuals. We demonstrate how this transition benefits both the individual and the company. We highlight the benefits of allowing customers to control their Digital Persona, the electronically aggregated profile formed by transactional processes, and introduce a Trust Bank, an entity that acts as an agent for consumers.
2. **Tittle :** A framework for understanding and predicting insider attacks.
   Authors : E. E. Schultz
   Abstract An insider assault is defined in this paper as the intentional misuse of computers and networks by individuals who are allowed to use them. However, putting this criteria into practise to assess whether or not an assault was carried out by an insider is rarely straightforward. We know relatively little about insider assaults, and there are many myths about them. Many information security professionals, for example, believe that "most threats come from within," despite empirical statistics and firewall logs indicating otherwise. This study proposes a framework based on past insider behaviour studies and models, as well as personal experience with insider attacks.
3. **Tittle :** Protecting financial institutions from brute-force attacks.
   Authors : Herley and D. Florˆencio

ABSTRACT :

We look at how to safeguard online banking accounts against brute-force password attempts. We use a huge number of honeypot userID-password pairings as our technique. The attacker is logged into a honeypot account with fictional attributes when any of these honeypot credentials are presented. To identify the difference between a honeypot and a real account, the attacker must attempt to withdraw funds. For every true break-in, we show how easy it is to assure that a brute-force attacker will come across hundreds, if not thousands, of honeypot accounts. His activities in the honeypots offer the bank with information on the attackers' attempts to distinguish actual accounts from honeypot accounts, as well as his cash-out technique

PROBLEM STATEMENT

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 [7]. 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 rights in online banks.

To protect consumers' privacy, existing approaches mostly used cryptography. Cryptography schemes mainly utilized encryption technology [8] and authentication technology [9], which could prevent illegitimate and unauthorized access. However, it is generally difficult for cryptography schemes to handle insider attacks effectively.

 Copyright @ 2024 Author

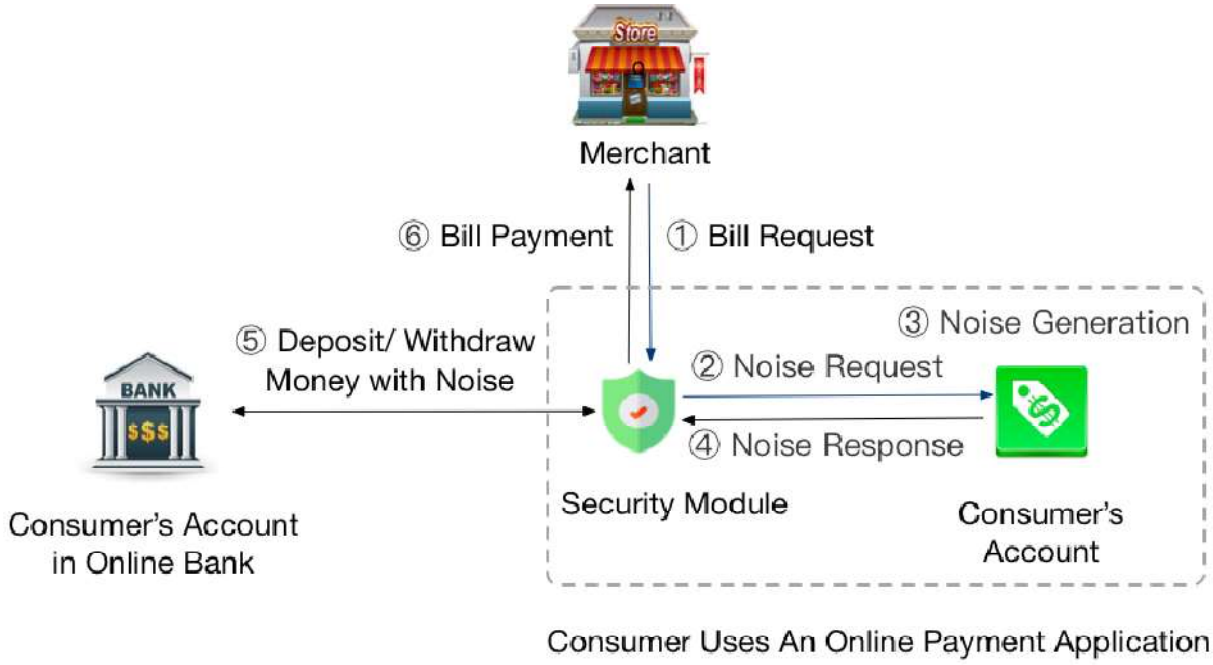
LIMITATION OF SYSTEM

Attackers can still misuse their authorized access to obtain credit statistics and shopping records

PROPOSED SYSTEM

we propose an optimized differential private online transaction scheme (O-DIOR), in which we define a new noise probability density function. The fundamental strategy is to basically eliminate the probability that noise is generated beyond the boundaries. The scheme can satisfy the differential privacy definition because the noise can be any value in a valid range to avoid the case that the consumption amount and noise can be inferred. Considering the consumption amount may be great and there is not enough money to generate the noise, we propose a revised O-DIOR scheme (RO-DIOR) to select variable boundaries. We define a new parameter in the noise distribution to adjust boundaries at a time point. We adjust the noise distribution to increase the probability of saving money from a payment application when the consumption amount approaches to zero and increase the probability of withdrawing money from the payment application when the consumption amount approaches to maximum [10].

4. SYSTEM ARCHITECTURE



Consumer Uses An Online Payment Application

IMPLEMENTATION

6.1 Bank Admin

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) ,View all users and authorize ,View All Transport company users and authorize,Add bank with its details such as bname, baddress,blocation,bpin,bmailid,bcno,add building image,View Credit card request and Process with Ac.No and CRN,credit limit,Card cvv(4 digit) 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.

 Copyright @ 2024 Author

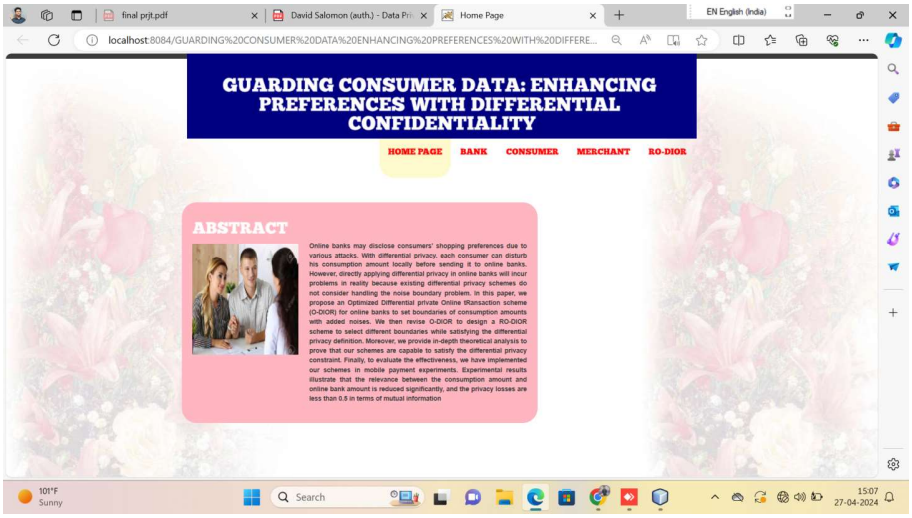
6.2 Consumers

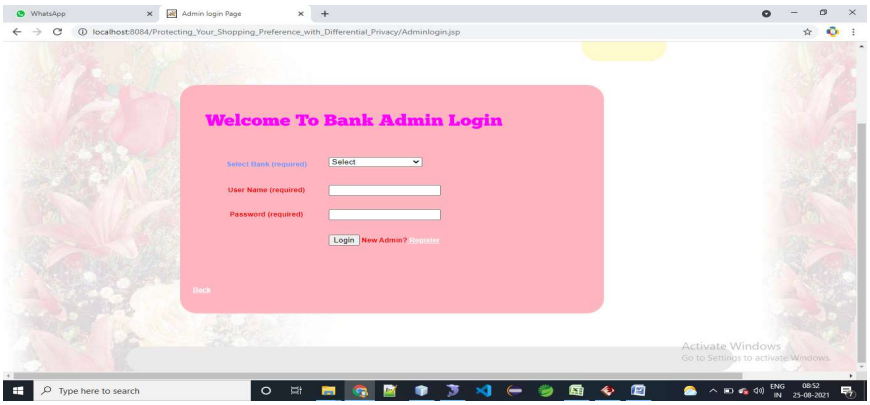
In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, View your profile, Manage Bank Account ,Request Credit card with * Details and view the same ,View Card Transactions based on transport booked details ,View your payments and transfer to your cc account (if user doesn't have enough amount to transfer then he is a fraud user or abnormal user) ,View all transport company and select corresponding company and book, give reviews, increment rank ,enter card cvv number(Find fraud if no balance in cc,if cvv number is wrong) ,View all Booked transport [10]

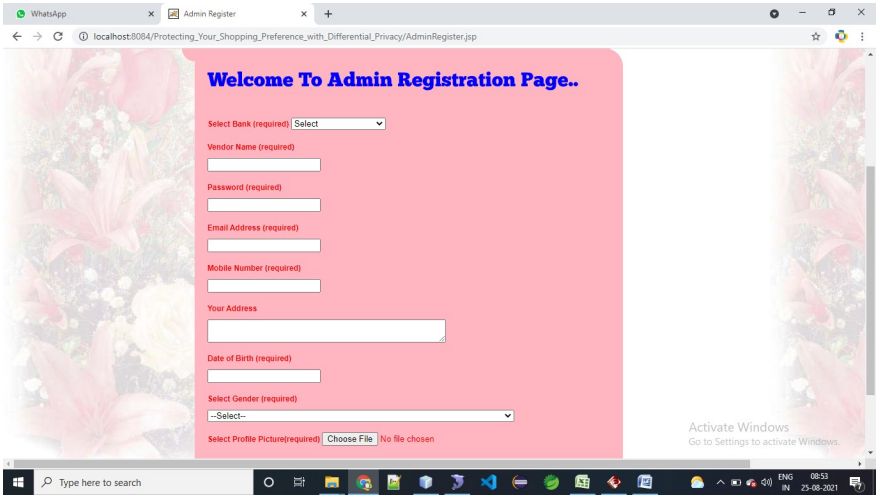
6.3 Merchant

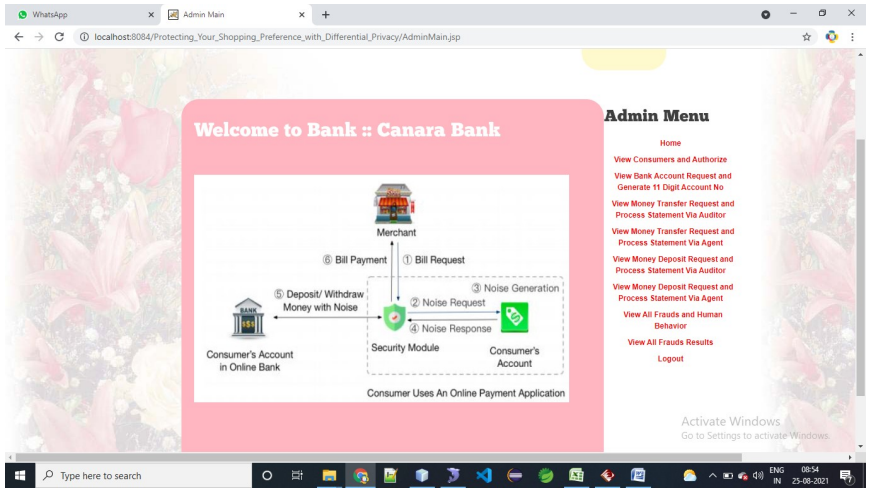
In this module, there are n numbers of users are present. Merchant user should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register with Company name and Login ,Add Transport Details(See below) ,View all Transport Details ,View all Booked Transport Details with total bill ,Find fraud -- View all normal and Fraud users ,View Type of frauds(Give link below to show numbers of same frauds in chart)

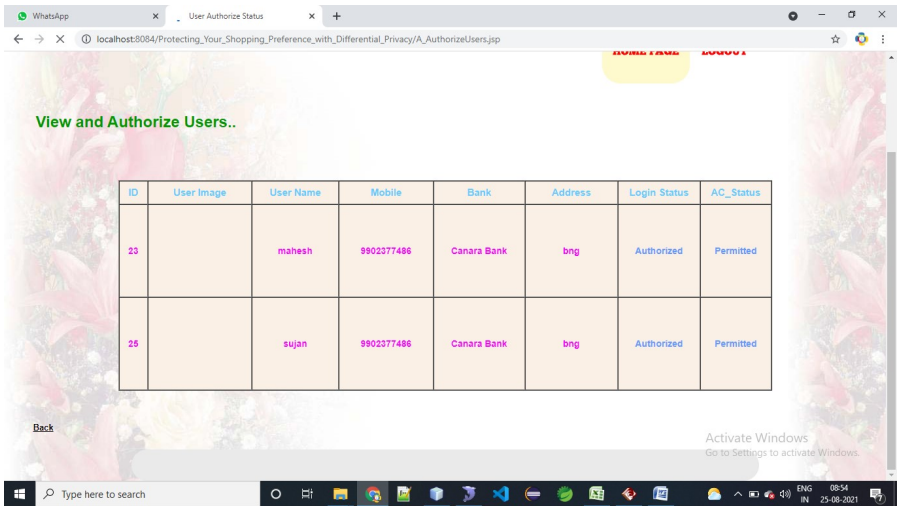
OUTPUT EXPERIMENTS



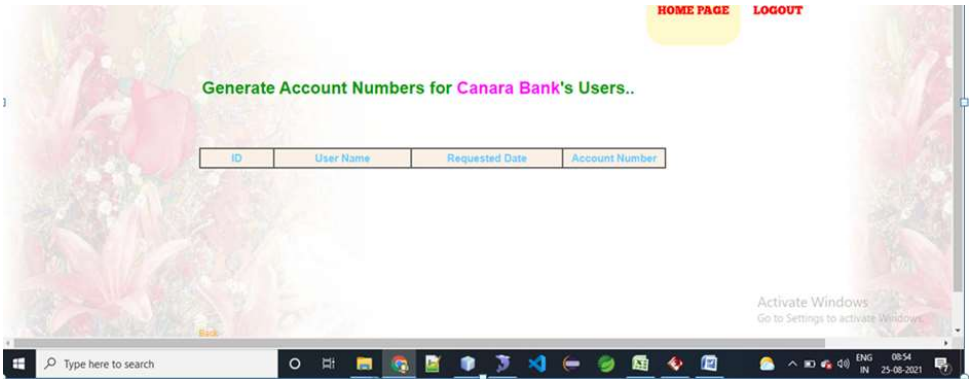


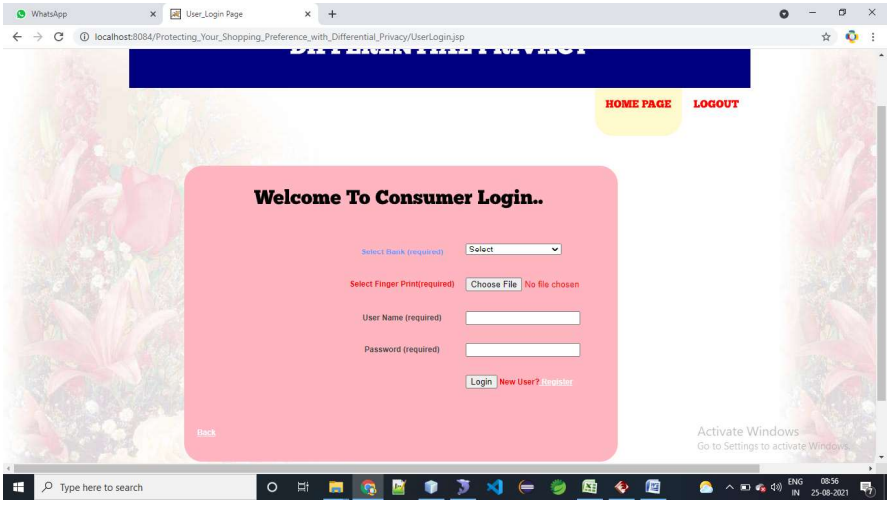






Copyright @ 2024 Author





CONCLUSION

Protecting user data with differential privacy is a challenging problem for online banks. 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 account balance in reality. With a payment application as a noise generator, activities and behaviors of consumers cannot be inferred from consumption records. Next, we further revise O-DIOR to 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. Experimental results illustrate that the relevance between the real consumption amount and online

bank transaction amount is reduced significantly, and the privacy losses are less than 0.5 in terms of mutual information To the best of our knowledge, this paper is the first effort about online consumption protection and boundary issue under differential privacy. Many challenging issues still remain, including protecting the location of shopping, handling the data transmission protection issue, and developing techniques for protecting the mobile applications, which we plan to address in our future work.

FUTURE SCOPE

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.

REFERENCES

[1] S. Nilakanta 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. Tjostheim, "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. Jagatic, 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 Montjoye, L. Radaelli, V. K. Singh et al., "Unique in the shopping mall: On the reidentifiability 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.

 Copyright @ 2024 Author