OPTIMIZED DIFFERENTIAL PRIVATE ONLINE TRANSACTION SCHEME FOR ONLINE BANKS

Mr. P.Muthyalu, Assistant Professor, Dept of CSE, Narayana Engineering College Gudur
M. Dhanalakshmi, **P. Pavani**, **N.Sai Hasa,** Student, Dept of CSE, Narayana Engineering College Gudur

Abstract – Online banks may unveil purchasers' shopping inclinations because of different assaults. With differential security, every customer can upset his utilization sum locally prior to sending it to online banks. Be that as it may, straightforwardly applying differential protection in online banks will bring about issues actually since existing differential protection plans don't consider taking care of the commotion limit issue. In this paper, proposing an Optimized Differential prIvate Online tRansaction conspire (O-DIOR) for online banks to define limits of utilization sums with added commotions. We at that point reconsider O-DIOR to plan a RO-DIOR plan to choose various limits while fulfilling the differential security definition. Also, giving inside and out hypothetical examination to demonstrate that our plans are competent to fulfill the differential security imperative.
Index terms – Differential Privacy, Bank, Shopping Preference Protection.

I. 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. Insider attacks are data misused by people with authorized access[1]. 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 bank[2]. 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, 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[3]. However, directly applyingDifferential privacy in online banks incurs some problems.

To address these challenges, then propose optimized differential private online transaction schemes (O-DIOR), in which that define a new noise probability density function. Thefundamental strategy is to basically eliminate the probabilitythat noise is generated beyond the boundaries. The schemecan satisfy the differential privacy definition because the noisecan be any value in a valid range to avoid the case that theconsumption amount and noise can be inferred. Consideringthe consumption amount may be great and there is not enoughmoney to generate the noise, we propose a revised O-DIORscheme (RO-DIOR) to select variable boundaries. We define anew parameter in the noise distribution to adjust boundaries ata time point. We adjust the noise distribution to increase theprobability of saving money from a payment application whenthe consumption amount approaches to zero and increase theprobability of withdrawing money from the payment application when the consumption amount approaches to maximum.

II. LITERATURE SURVEY

Online banks have been commonly used for paymentservices. A great deal of work aims to protect the onlineconsumption privacy for higher privacy-level performance.

The approaches can be classified into two categories.The first category is authentication. This work firstdescribed a systematic multi-factor biometric fingerprint authenticationapproach which provided an identity verificationprocess for validating the legitimacy of remote users[4]. Theydeveloped a privacy protection gateway for obscuring anddesensitizing the consumers account details using tokenizationand data anonymization techniques. The study in showed that the authentication of many Norwegian online banking consumerswas too weak, and discussed authentication methodsand possible attacks. The work studied authenticationissues of client and transaction for online banks. Paper focused on evaluating authentication methods which were usedin online banks. The work used a short-time passwordsolution and a certificate-based solution to resist the onlinechannel-breaking attacks.

The second category is encryption. Pathak et al. designed a protocol for privacy preserving bank computationsusing arithmetic cryptography. The work presenteda secure hybrid architecture model for internet banks usingHyperelliptic curve cryptosystem and Hash algorithm. Tebaaet al. proposed a hybrid homomorphic encryption methodfor protecting the privacy of banking data in the cloud. However, these schemes still have some limitations[5]. It isdifficult for authentication and encryption methods to handleinsider attacks in online banks, because consumption recordshave to be exposed to people with authorized access.

To handle insider attacks, differential privacy is widelyused. To the best of our knowledge, our scheme is the firstto meet the requirement of differential privacy for onlinebanks. We compare with existing schemes which address noiseboundary problems of differential privacy in other scenarios.Duchi and Jordan used lower and upper boundaries forestimation of population quantities and variational boundarieson mutual information under local privacy. Zhang et al. proposed differential privacy-preserving schemes for smartmeters, limiting the range of noise and capability of batteries.

Hardt and Talwar gave polynomial time computable upperand lower boundaries on noise complexity and error. The workpresented privacy buckets for computing upper andlower boundaries for approximate differential privacy after rfoldcomposition. The paper preserved privacy of individualentries with constrained additive noise and its optimalprobability density function could maximize the measure of privacy.

Besides, there are some differential privacy schemes which adjust noise for better utility[6]. The work under individualdifferential privacy allowed the data controller to adjust thedistortion to an actual dataset, which could reduce the noiseand preserve the utility better. Zhu et al. defined correlatedsensitivity to decrease the noise. E2EPRIV privately optimizeddata-dependent error boundaries and achieved true end-to-end privacy. The work presented capacity boundeddifferential privacy which could satisfy privacy axioms.However, existing differential privacy methods did not considerlimiting the range of data with added noise to correspondto reality. We cannot apply their schemes to protect onlineconsumption privacy directly. Besides, their schemes cannotselect different boundaries to satisfy the need of consumers.

To tackle the above problems, we define a new probabilitydensity function of noise while the consumption with addednoise has lower and upper boundaries. Our schemes can satisfydifferential privacy because the noise can be any value in validrange to avoid the consumption and noise being inferred.

III. PROPOSED SYSTEM

The system model in proposed system consists of three parts (1)a consumer’s account in the online bank, (2) a securitymodule in a payment application, (3) an account in a paymentapplication[7][8][9].

- Each online bank account has the balance and online transaction records of a consumer, so all operations of the consumer can be obtained.
- A security module is designed in a mobile payment application. It is popular for consumers to utilize mobile applications to pay for their bills. The security module is a key role to compute the value of noise to protect the consumption amount with noise under differential privacy. When

the security module receives the consumer's payment request, it can calculate the noise and schedule money from consumer's account in the online bank and in the payment application, then it will pay for the bill.

- The payment application could be Apple Pay, Alipay, Paypal or Wechat pay on the mobile. It is like a money pool which can store a certain amount for a consumer. It can facilitate us to generate and eliminate the noise for the consumption amount. In this paper, we employ Apple Pay as the payment application for example.

To solve the above challenge, a payment application couldbe used to add the noise before the data are reported to theonline bank. Unlike the online bank, the payment applicationcannot get the sensitive information, it only assigns the moneyto the security module to eliminate the noise. It cannot sendits actual consumption amount to the online bank, becausethey cannot trust each other. Therefore, the consumer could consider his account in the payment application as a noisegenerator.

At first we want to use the cloud server to calculate noiseand schedule money, but sending all the data to the cloud hasto require high network bandwidth. It is not necessary to usethe cloud server due to the data privacy concerns. The work shows that ninety percent of data generated from terminalserver are processed and stored locally instead of in the cloudserver. Therefore, we utilize a payment application in user's mobile to implement our schemes.

For that proposed a differential private online transaction (DIOR) scheme. The specification of DIOR is presented in Algorithm1. In DIOR, the noise follows the standard Laplacemechanism, its probability density function pdf(x) is shown inthe algorithm. The consumer's account in the security modulefirst calculates a noise which is randomly drawn from the Laplace distribution.If the noise is not enough to pay, thesecurity module will notify the consumer's account in theonline bank to withdraw the other part. Otherwise, if the noiseis more than the payment amount, the security module willsend extra part into the consumer's account in the online bank.

Algorithm 1 The specification of the DIOR scheme

Input: $c(i-1)$, $o(i-1)$, $\{m_j(i)\}$, $\{d_j(i)\}$.
Output: $n(i)$.

1. $d(i) = \sum_j (d_j(i))$
2. **For all** k, l, $\Delta f = \max |d_k(i) - d_l(i)|$
3. $\sigma = \Delta f / \epsilon$
4. $pdf(x) = \frac{e^{-\frac{|x|}{\sigma}}}{2b}$
5. $n(i) \leftarrow pdf(x)$
6. $o(i) = o(i-1) - d(i) - n(i)$
7. $c(i) = c(i-1) + n(i)$
8. **Return** $n(i)$

IV. CONCLUSION

Protecting user data with differential privacy is a challengingproblem for online banks. The method of directly applying differentialprivacy is illustrated in a DIOR scheme. In this paper,we propose O-DIOR, a differential private online transactionscheme to address privacy concerns during financial transactions.O-DIOR can set boundaries of consumption amountwith added noise, considering the range of account balancein reality. With a payment application as a noise generator, activities and behaviors of consumers cannot be inferred fromconsumption records.

REFERENCES

[1] S. Nilakanta and K. Scheibe, "The digital personal and trust bank: Aprivacy management framework," Journal of Information Privacy andSecurity, vol. 1, no. 4, pp. 3–21, 2005.

[2] K. J. Hole, V. Moen, and T. Tjostheim, “Case study: Online bankingsecurity,” IEEE Security & Privacy, vol. 4, no. 2, pp. 14–20, 2006.
[3] A. Rawat, S. Sharma, and R. Sushil, “Vanet: Security attacks and itspossible 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 attackdetection research,” Insider Attack and Cyber Security, pp. 69–90, 2008.
[5] E. E. Schultz, “A framework for understanding and predicting insiderattacks,” Computers & Security, vol. 21, no. 6, pp. 526–531, 2002.
[6] Ravinder Rao, P., Sucharita, V.A framework to automate cloud based service attacks detection and prevention International Journal of Advanced Computer Science and Applications, 2019, 10(2), pp. 241–250
[7]. Herley and D. Florˆencio, “Protecting financial institutions frombrute-force attacks,” in Proc. IFIP International Information SecurityConference, 2008.
[8] A. Householder, K. Houle, and C. Dougherty, “Computer attack trendschallenge internet security,” Computer, vol. 35, no. 4, pp. 5–7, 2002.
[9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Socialphishing,” Communications of the ACM, vol. 50, no. 10, pp. 94–100,2007.
[10] Y.-A. De Montjoye, L. Radaelli, V. K. Singh et al., “Unique in theshopping mall: On the reidentifiability of credit card metadata,” Science,vol. 347, no. 6221, pp. 536–539, 2015.