Optimized Differential Private Online Transaction Scheme For Online Shopping

S.Satheesh[1], R. Migeba Jasmine[2]
[1]Dept of Computer Science and Engineering
[2]Assistant Professor, Dept of Computer Science and Engineering
[1, 2] Ponjesly College Of Engineering

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 work 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, I have implemented our schemes in website payment experiments.*

Keywords- cryptography noise, hybrid algorithm, online transaction, privacy schemes .

I. INTRODUCTION

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The main concept involves mobile communication, mobile hardware, mobile software. The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from portable laptops, smartphones, tablet Pc's, Personal Digital Assistants. Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. This is the engine of the mobile device. In other terms, it is the operating system of the appliance. It's the essential component that operates the mobile device. Since portability is the main factor, this type of computing ensures that users are not tied or pinned to a single physical location, but are able to operate from anywhere. It incorporates all aspects of wireless communications.

II. MOBILE COMPUTING DEVICES

Usually, a mobile computing device would have a body- made of metal or plastic, a RAM, a CPU, a hard drive, a motherboard, a keyboard and a mouse- which could be separate components in the body or touch-based, a screen, a video card, an operating system, software applications, and finally, a network connection. This is around the same as the components of a personal computer, which isn't a mobile device. But mobile devices may have other components too, to make them portable, and certain characteristics that make them different size, power source, operating system, connectivity, applications. The portability of mobile devices demands a smaller size. Reduction in size without reducing capabilities has also always been a challenge when developing mobile devices. Mobile devices are usually powered by rechargeable batteries. Improving the battery life of mobile devices is another significant area of research. Laptops run on more or less the same OS as PCs, but for smartphones and other devices, the OS is significantly different. They are powerful but scaled-down and made specifically for particular devices. Mobile computing devices have capabilities that allow access to the internet. Also, mobile devices like smartphones have access to mobile broadband networks that allow you to make and receive phone calls. Applications meant for mobile devices are specifically designed for running on a particular OS. These applications are what extends the capabilities of devices beyond just connecting to the internet or making calls.

III. ONLINE TRANSACTIONS AND SECURITY

Online transaction is a payment method in which the transfer of fund or money happens online over electronic fund transfer. Online transaction process (OLTP) is secure and password protected. Three steps involved in the online transaction are Registration, Placing an order, and, Payment. Online transaction processing (OLTP) is information systems that facilitate and manage transaction-oriented

applications, typically for data entry and retrieval transaction processing. So online transaction is done with the help of the internet. It can't take place without a proper internet connection. Online transactions occur when a process of buying and selling takes place through the internet. When a consumer purchases a product or a service online, he/she pays for it through online transaction. There are three stages of Online Transactions. Pre-purchase/Sale, In this stage, the product or service is advertised online with some details for the customers. Purchase/Sale,When a customer likes a particular product or service, he/she buys it and makes the payment online. Delivery Stage, This is the final stage where the goods bought are delivered to the consumer. The consumer has to register online on the particular website to buy a particular good or service. The customer's email id, name, address, and other details are saved and are safe with the website. For security reasons, the buyer's 'Account' and his 'Shopping Cart' is password protected When a customer likes a product or a service, he/she puts the product in the 'shopping cart'. The shopping cart gives a record of all the items selected by the buyer to be purchased, the number of units or quantity desired to be bought per item selected and the price for each item. The buyer then has to select the payment option, he/she has various payment options. These payment pages are secured with very high-level encryptions so that the personal financial information that you enter (bank/card details) stay completely secure. Some ways in which you can make this payment are cash on delivery, cheque,net banking transfer, credit or debit card, digital cash.

IV. PROJECT OVERVIEW

In the last decade, online banks were commonly used to provide financial services. However, online banks are vulnerable to outsider and insider attacks. 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) 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.

V. SYSTEM MODULES

A. Consumers Account

Each online bank account has the balance and online transaction records of a consumer, so all operations of the consumer can be obtained.

B . Security Module

A security module is designed in a payment application. It is popular for consumers to utilize 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, and then it will pay for the bill.

C. Account in a Payment Application

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.

VI .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.

REFERENCES

[1] 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.

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

[3] A. P. Hiltgen, T. Kramp, and T. Weigold, "Secure internet banking authentication," IEEE Security & Privacy, vol. 4, no. 2, pp. 21–29, 2006.

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

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

[6] 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.