DIFFERENTIAL PRIVACY PROTECTS YOUR SHOPPING PREFERENCE

ARABU.RAKSHITHA,PROF.BARNALI Chakrobathy
Student, Department of MCA, AMC Engineering College (VTU), Bengaluru, India
Professor, Department of MCA, AMC Engineering College (VTU), Bengaluru, India

Abstract

Due to numerous threats, online banks may reveal customers' buying interests. Each customer can interrupt his consumption quantity locally before submitting Applying differential privacy to online banking presents challenges in practice due to the current limitations of existing techniques, particularly in addressing the noise boundary problem. In this study, we propose a solution called the Optimized Differential Privacy Online Transaction system (O- DIOR) for online banks. O-DIOR incorporates additional noise to define consumption amount boundaries. To provide flexibility, we enhance O-DIOR with a scheme called RO-DIOR, which enables the selection of alternative boundaries while maintaining compliance with the differential privacy criteria. Additionally, we provide comprehensive theoretical analysis to illustrate that our systems can satisfy the requirements of differential privacy

INTRODUCTION:-

Because of several types of assaults, customers' shopping preferences could be revealed by online banks. Because differential privacy allows it, eachcustomer can change the amount ofproduct he or she consumes locally beforeit is reported to online banks. Directlyusing differential privacy in online banking, on the other hand, would lead toproblems in practice due to the fact that present differential privacy systems do not take into consideration how to handle the noise boundary problem. In this research, we suggest an Optimised Differential prIvate Online tRansaction system, or O-DIOR, for use by onlinebanks to establish limits on the amounts of consumption that can occur in the presence of noise. After that, we make some changes to O-DIOR and build a RO-DIOR method To enable the selection of diverse boundaries while maintaining compliance with differential privacy criteria, we propose the incorporation of various thresholds. Furthermore, we provide an extensive theoretical analysis to showcase the capability of our proposed schemes in meeting the requirements of differential privacy. To assess the effectiveness of our strategies, we conducted tests involving mobilepayments. The experimental results demonstrate a substantial reduction in the correlation between expenditure and the balance in an online bank account, with privacy losses measuring less than 0.5 in terms of mutual information

Writing REVIEW 1.EXISTING SYSTEM

Most of the existing approaches rely on encryption to safeguard customers' privacy. Encryption technology and authentication technology have been the key technologies employed bycryptographic systems. These techniques effectively mitigate the risk of unauthorized access and illegitimate activities. Nevertheless, cryptographic methods often face challenges in adequately Coping with internal threats remains a challenge for cryptographic methods. Despite their effectiveness in preventing unauthorized access, there is still a potential for authorized insiders to exploit their privileges,allowing attackers to illicitly obtain credit statistics and shopping records."

Differential privacy-enhancing techniques, aimed at restricting the magnitude of perturbation and reducing the burden on batteries, were put forward by Zhang and collaborators. These approaches were designed for implementation insmart meters Computationalpolynomial-time algorithms allowed for the determination of both upper and lower bounds on noisecomplexity and error, thanks to the research conducted by Hardt and Talwar. Within this investigation, privacy containers were introduced to establish upper and lower limits for approximate differential privacy through rfold composition. Theextent of privacy was optimized by employing the article's recommended probability density function,effectively safeguarding the confidentiality of individual entries by incorporating minimal additive noise."

2. PROPOSED SYSTEM

O-DIOR, which stands for optimized differential online privacy-preserving transaction scheme, represents our novel innovation. Within this framework, we have formulated a fresh probability density function for the noise component. The primary goal of this approach is to minimize or eliminate the potential occurrence ofnoise exceeding predefined boundaries. By allowing the noise toassume any value within a valid range, the scheme adheres to the requirements set by the definition ofdifferential privacy. This becomes imperative to prevent the disclosureof consumption amounts and noise through inference. To address this concern, we propose a new variant of O-DIOR called RO-DIOR, whichdynamically adjusts the boundaries to accommodate situations where the consumption amount may be highdespite insufficient funding to generate the necessary noise."

In order to implement the proposed strategy, it is essential to develop a secure module for an online payment application. This module will introduce and subsequently eliminatenoise, ensuring the confidentiality of consumption amounts. For example,let's consider the payment system Apple Pay developed by Apple. In our scenario, a customer utilizes Apple Pay to settle their bill, transferring funds between their online bank account and Apple Pay account to cover the purchase cost.

Apple Pay, as a safeguard, does not retain customers' card numbers or any transaction records that could be exploited to track their preferences. Traditionally, Apple Pay directly deducts funds from online banks. However, our additional step involves drawing funds from customers' personal Apple Pay accounts, which may raise potentialconcerns regarding trust and security.

The security module is able to compute the noise value and determine the quantity of usage. Forinstance, a customer owes a retailer $12 as part of the transaction. Because differentiated privacy is notavailable, he must withdraw twelve dollars from an online bank, which reveals the precise amount of moneybeing spent. With differential privacy, if the security module determines that the noise value is $5and adds the noise to the online bankaccount, then it will need to withdraw $17 from the online bank rather than the previous amount of $12. This is because the noise value was added to the account. As a result, the privacy associated with one's own consumption can be preserved. The security module will then save $5 in Apple Pay in order toget rid of the additional noise; nevertheless, the actual consumption amount will remain the same as before, which is $12. Apple Pay has deposited the sum of seventeen dollars into the customer's online bank account, which is the consumption record in the online bank. As a result, thieves are unable to determine the customer's payment amounts or shopping locations usingonline banks.

MODULES:

1. CONSUMERS ACCOUNT INTHE ONLINE BANK
2. SECURITY MODULE IN APAYMENT APPLICATION
3. ACCOUNT IN A PAYMENTAPPLICATION
4. DIOR SCHEME

DESCRIPTION OFMODULES

1. Consumer’s account in the online bank

In this section, we establish a financial profile for a user within an online banking platform. Online banking platforms have gained significant popularity due to their capability to provide comprehensive access to a consumer's complete financial records, encompassing account balances and transaction histories. Additionally, we develop a system integrated with an online shopping portal, enabling users to conveniently browse through a wide array ofproducts. The portal showcases product details and accompanying images, empowering consumers to make informed choices while shopping for their desired items."

2. Security module in a payment application

Mobile payment applications commonlyincorporate inherent security mechanisms toensure secure transactions. The utilization of mobile applications for bill payments is gaining popularity among customers. The security module assumes a crucial role in computing the noise value, which serves to protect the consumption amount through noise addition while upholding differential privacy. Upon receiving a payment request from the customer, the security module accurately calculates the noise and orchestrates the transfer of funds from the customer's online bank account and the payment application. This preparatory step facilitates seamless bill payment processing."

3. Account in a payment application

The mobile payment application on the device operates in a manner akin to well- known platforms such as Apple Pay, Alipay,Paypal, or WeChat Pay. It resembles a virtual wallet, allowing consumers to store a predetermined sum of money within it. Thisfunctionality facilitates the generation and subsequent elimination of noise, depending on the consumption amount, streamlining the privacy-preserving process. For the purpose of this project, our development is limited to a local host environment, andreal-time functionality is not being implemented."

4. DIOR Scheme

Prior to data submission to the online bank, the introduction of noise can be achieved through the utilization of a payment application. Unlike the online bank, the payment application lacks access to critical information and can solely allocate funds to the security module to mitigate the noise. Due to mutual distrust between the payment application and the online bank, it is unable to transmit the actual usage amount to the online bank. Consequently, the customer perceives their payment application account as a source of noise. To address scenarios involving consumer consumption, we have devised a dynamic policy for online transactions. When a customer engages in shopping activities, they are required to have sufficient cash on hand to cover their purchases. The amount designated as "C" represents the payment obligation. Subsequently, the consumer forwards the request to the security module. Once the security module processes the received request, it proceeds to compute the noisevalue.

RESULTS

.

CONCLUSION

The preservation of user data while upholding differential privacy poses a challenge in the realm of online banking. DIOR, an acronym for "Directly Imposing Differential Privacy," refersto the direct application of differential privacy. In this paper, we tackle privacy concerns arising in financial transactions by introducing O-DIOR, a differential private method for online transactions. O-DIOR effectively imposes bounds on consumption quantities through noise addition, accounting for a wide range of account balances. When a payment application is utilized as a noise generator, inference regarding customer actions and behavior based on consumption statistics becomes infeasible. Subsequently, we further refine O-DIOR and propose RO-DIOR as a solution to address the selection of distinct boundaries. Extensive theoretical exploration demonstrates the efficacy of our strategies in meeting the requirements of differential privacy. Experimental results reveal a significant reductionin the correlation between actual consumption amounts and online bank transaction records, with privacy loss quantified at less than 0.5 interms of mutual information.

REFERENCES

[1] S. Nilakanta and K. Scheibe wrote an article titled "The digital personal and trust bank: A privacy management framework," which was published in theJournal of Information Privacy and Security in 2005, volume 1, issue 4, pages 3–21.

[2] K. J. Hole, V. Moen, and T. Tjostheim, "Case study: Online banking security," published in IEEE Security & Privacy, volume 4, number 2, pages 14– 20, 2006.

[3] A. Rawat, S. Sharma, and R. Sushil, "Vanet: Security attacks and its possible solutions," Journal of Information andOperations Management, volume 3, number 1, page 301, 2012; cited in [4].

[4] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attackdetection research," published in 2008 inInsider Attack and Cyber Security, pages69–90.

[5] According to E. E. Schultz's article titled "A framework for understanding"