GUARDING CONSUMER DATA ENHANCING PREFERENCES WITH DIFFERENTIAL CONFIDENTIALITY

1 Mr. R. VINOD KUMAR, 2 A. ESHWAR, 3 B. BALA KRISHNA

4 B. UPENDER, 5 S. DINAKAR

1Assistant Professor, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad

2345Under Graduate, Department of CSE, Sri Indu College of Engineering and Technology-Hyderabad

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 theprivacy losses are less than 0.5 in terms of mutual information.

Guarding consumer data and enhancing preferences with differential confidentiality involves protecting sensitive information while still providing valuable services based on the preferences of users. Differential privacy is a framework that can be used to achieve this goal. It focuses on adding noise or perturbation to data queries or responses in a way that does not disclose information about individuals, but still allows for meaningful aggregate analysis.

Here are steps and principles to enhance consumer data preferences with differential confidentiality:Familiarize yourself with the principles and concepts of differential privacy. This includes understanding epsilon-differential privacy, noise addition, and how to measure the privacy loss.Determine an appropriate privacy budget (epsilon value) that balances privacy with the utility of the data. Lower epsilon values provide stronger privacy but may reduce the accuracy of the analysis.

Keywords: **Cloud and Big Data, Data Security**

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. 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 recommendations, harassing messages 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 erosionof 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's involvement in the dataset . However, directly applying differential privacy in online banks incurs some problems. The consumption amount with addednoise 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 an online bank account, otherwise in theonline 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 guarantee cannot be controlled. Existing differential privacy approaches have not considered setting boundaries on data with added noise

To implement the scheme, we design a security module for an online payment application to generateand 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.

LITERATURE SURVEY

Key-exposure resistance has always been an important issue for in-depth cyber defense in many security applications. Recently, how to deal with the key exposure problem in the settings of cloud storage auditing has been proposed and studied. To address the challenge, existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local burdens to the client, especially those with limited computation resources, such as mobile phones. In this paper, we focus on how to make the key updates as transparent as possible for the client and propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates.

In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update burden on the client will be kept minimal. In particular, we leverage the third party auditor (TPA) in many existing public auditingdesigns, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for

key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from theTPA when uploading new files to cloud. Besides, our design also equips the client with capabilityto further verify the validity of the encrypted secret keys provided by the TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. We formalize the definition and the security model of this paradigm. The security proof and the performance simulation show that ourdetailed design instantiations are secure and efficient.

Secure search techniques over encrypted cloud data allow an authorized user to query data files of interest by submitting encrypted query keywords to the cloud server in a privacy- preserving manner. However, in practice, the returned query results may be incorrect or incomplete in the dishonest cloud environment. For example, the cloud server may intentionally omit some qualified results to save computational resources and communication overhead. Thus, a well-functioning secure query system should provide a query results verification mechanism that allows the data user to verify results. In this paper, we design a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the correctness of each data file in the set but also can further check how many or which qualified data files are not returned if the set is incomplete before decryption. The verification scheme is loose-coupling to concrete secure search techniques and can be very easily integrated into any secure query scheme. We achieve the goal by constructing secure verification object for encrypted cloud data. Furthermore, a short signature technique with extremely small storage cost is proposed to guarantee the authenticity ofverification object and a verification object request technique is presented to allow the query userto securely obtain the desired verification object. Performance evaluation shows that the proposed schemes are practical and efficient.

SYSTEM ANALYSIS

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 . 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 , 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 addednoise 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 guarantee cannot be controlled. Existing differential privacy approaches have not considered setting boundaries on data with added noise.

- Limited Insider Attack Protection: The mentioned cryptography schemes might struggle to effectively handle insider attacks, where individuals with authorized access misuse their privileges to access sensitive data. This limitation could undermine the overall security of theonline banking system, allowing insiders to misuse credit statistics and shopping records.

- Boundary Challenges in Differential Privacy: Applying differential privacy, while effectivein protecting privacy, faces challenges when dealing with boundaries. The addition of noise to transaction data can potentially lead to consumption amounts that exceed account balances. Dealing with this issue might require adjustments, but such modifications could compromise the level of privacy protection guaranteed by differential privacy standards.

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 begreat 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 ofsaving 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.

ADVANTAGES

Enhanced Privacy Guarantee: The proposed optimized differential private online transaction scheme (O-DIOR) introduces a new noise probability density function that eliminates the possibility of noise exceeding predefined boundaries. By maintaining the noise within valid ranges, this approach provides a higher level of privacy guarantee by avoiding scenarios where the consumption amount and noise can be deduced or manipulated.

IMPLEMENTATION

Modules:-

- Bank Admin
- Consumers
- Merchant

MODULE DESCRIPTION

BANK ADMIN

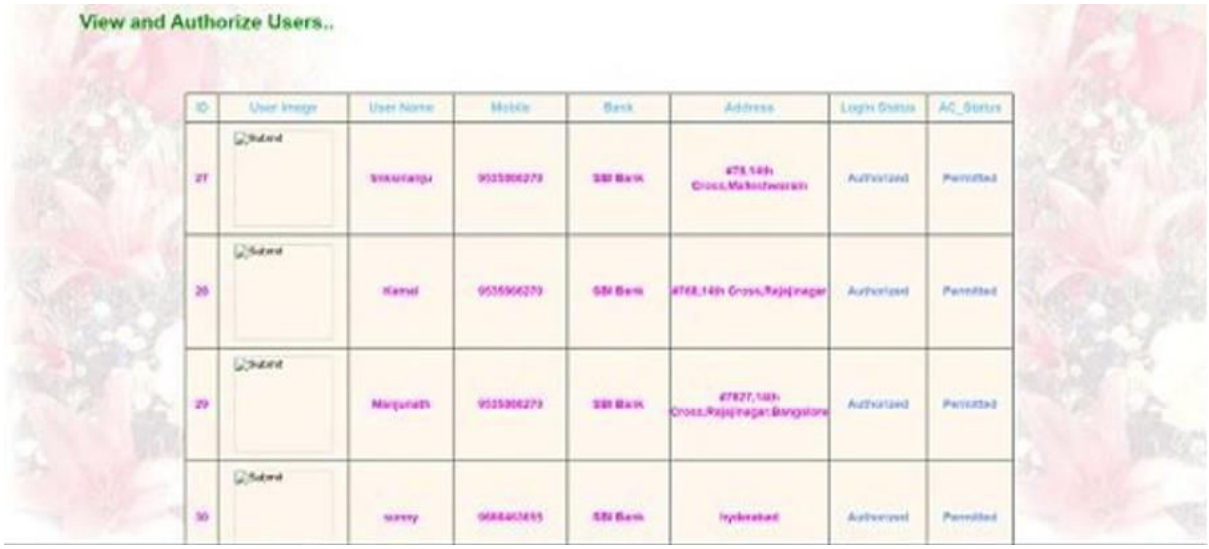
In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View all users and authorize, View all Transport Users and authorize, Register and Login(With Bank Name) ,View all users and authorize ,View All Transport company users 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,Cardcvv(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 basedon 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.

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 himand 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(Findfraud if no balance in cc,ifcvv number is wrong),View all Booked transport

RESULTS

HOME SCREEN



REGISTRY AUTORITY SCREEN

TRANSACTIONS SCREEN

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 furtherrevise 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.

To conclude a discussion on the topic of "GUARDING CONSUMER DATA ENHANCING PREFERENCES WITH DIFFERENTIAL CONFIDENTIALITY," you can provide a summary ofthe key points and implications of the concept. Here's a sample conclusion

In a rapidly evolving digital landscape, the need to protect consumer data and enhance preferences while maintaining differential confidentiality has become paramount. This approach not only addresses the crucial aspect of data privacy but also recognizes the significance of personalization and user empowerment. The state-of-the-art systems and methodologies designed for this purpose area testament to our commitment to both safeguarding individual data and delivering tailored user experiences.

REFERENCES

[1] S. Nilakanta and K. Scheibe, “The digital personal and trust bank: A privacy managementframework,” 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,” Journalof 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 internetsecurity,” Computer, vol. 35, no. 4, pp. 5–7, 2002.

[8] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” Communicationsof 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 thereidentifiability 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 visitationpatterns,” Scientific reports, vol. 3, p. 1645, 2013.