International Journal of Innovative Research in Engineering
Volume 3, Issue 4 (July-August 2022), PP: 241-243.
www.theijire.com
ISSN No: 2582-8746

Optimized Differential Private Online Transaction Scheme for Online Shopping

Jayasree V[1], Dr. F. Ramesh Dhanaseelan[2]
[1]PG MCA Student, Department of MCA, ST.Xavier's Catholic College of Engineering, Nagercoil, India.
[2]Professor, Department of MCA, ST.Xavier's Catholic College of Engineering, Nagercoil, India.

How to cite this paper:
Jayasree V[1], Dr. F. Ramesh Dhanaseelan[2], "Optimized Differential Private Online Transaction Scheme for Online Shopping", IJIRE-V3I04-241-243.

Abstract: *Online banks may disclose consumer's shopping preferences due to various attacks. This project mainly focused on online consumption protection. Also this project describes how a customer can purchase products using their Fingerprint Authentication Algorithm. Only when the fingerprint is matched then the customers can able to purchase the products. An Optimized Differential private online transaction scheme (O-DIOR) is used for online banks to set boundaries of consumption amounts with added noises. Moreover, it provide in-depth theoretical analysis to prove that O-DIOR Scheme satisfy the differential privacy constraint. It helps to provide improved security for Online Shopping. Fingerprint Authentication Algorithm has been used for Finger print Verification.*

Keywords: *Fingerprint, Authentication, O-DIOR, Security.*

I. INTRODUCTION

Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser or a mobile app. Consumers find a product of interest by visiting the website of the retailer directly or by searching among alternative vendors using a shopping search engine, which displays the same product's availability and pricing at different e-retailers. As of 2020, customers can shop online using a range of different computers and devices, including desktop computers, laptops, tablet computers and smartphones. An online shop evokes the physical analogy of buying products or services at a regular "bricks-and-mortar" retailer or shopping center; the process is called business-to-consumer (B2C) online shopping. When an online store is set up to enable businesses to buy from another business, the process is called business-to-business (B2B) online shopping. A typical online store enables the customer to browse the firm's range of products and services, view photos or images of the products, along with information about the product specifications, features and prices. Online stores usually enable shoppers to use "search" features to find specific models, brands or items. Online customers must have access to the Internet and a valid method of payment in order to complete a transaction, such as a credit card, an Interact-enabled debit card, or a service such as PayPal. For physical products (e.g., paperback books or clothes), the e-tailer ships the products to the customer; for digital products, such as digital audio files of songs or software, the e-tailer usually sends the file to the customer over the Internet. The largest of these online retailing corporations are Alibaba, Amazon.com, and eBay.

II. RELATED WORK

1.Design and Implementation of an RFID-Based Customer Shopping Behavior Mining System

Zimu Zhou and LongfeiShangguan are the authors

Shopping behavior data is of great importance in understanding the effectiveness of marketing and merchandising campaigns. Online clothing stores are capable of capturing customer shopping behavior by analyzing the click streams and customer shopping carts. Retailers with physical clothing stores, however, still lack effective methods to comprehensively identify shopping behaviors. In this paper, we show that backscatter signals of passive RFID tags can be exploited to detect and record how customers browse stores, which garments they pay attention to, and which garments they usually pair up. The intuition is that the phase readings of tags attached to items will demonstrate distinct yet stable patterns in a time-series when customers look at, pick out, or turn over desired items.

2. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway

SaboutNagaraju and LathaParthiban are the authors

Banks provide the impetus for people and country to develop economically. They make financial dealing easy, safe and convenient. Banks take part in welfare activities and also help in social causes of the people. Most of the banks provide the financial dealings through passbooks, ATM, mobile banking, electronic banking and telephone banking. Among these financial dealings, e-banking and mobile banking will be more convenient and these two are essential for busy people. Specifically, it is critical to provide an efficient, reliable and secure e-banking service to the consumers because user needs and cyber attacks are increasing on the internet-based technologies.

3. Privacy-preserving Crowd-sourced Statistical Data Publishing with An Untrusted Server

Zhibo Wang and XiaoyiPang are the authors

The crowd-sourced data can be aggregated in real-time and mined by machine learning technologies to discover valuable information and further benefit our life (e.g., popular restaurants recommendation, real-time traffic analysis and navigation). Recently more and more agencies (e.g., governments and companies) are publishing the crowd-sourced data to the public for data mining purposes. However, the promising advantages of data publishing and mining are at the risk of disclosing sensitive information to data miners.

4. Ensuring Privacy with Constrained Additive Noise by Minimizing Fisher Information

FarhadFarokhi andHenrik Sandberg are the authors

Preserving the privacy of individual entries of a database when responding to linear or nonlinear queries with constrained additive noise is considered. For privacy protection, the response to the query is systematically corrupted with an additive random noise whose support is a subset or equal to a pre-defined constraint set. A measure of privacy using the inverse of the trace of the Fisher information matrix is developed.

III. EXISTING SYSTEM

In Existing System, 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. 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.

DISADVANTAGES

- Directly applying differential privacy in online banks incurs some problems.
- The consumption amount with added noise may be beyond the boundaries after transactions.

IV. PROPOSED SYSTEM

In our proposed System optimized differential private online transaction scheme (O-DIOR), in which 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, propose a revised O-DIOR scheme (RO-DIOR) to select variable boundaries. To implement the scheme, design a security module for an online payment application to generate and eliminate the noise to guarantee the utility of consumption amounts. This project mainly focused on online consumption protection. Also this project describes how an customer can purchase products using their Fingerprint Authentication Algorithm. Only when the fingerprint is matched then the customers can able to purchase the products. An Optimized Differential private online transaction scheme (O-DIOR) is used for online banks to set boundaries of consumption amounts with added noises. Moreover, it provide in-depth theoretical analysis to prove that O-DIOR Scheme satisfy the differential privacy constraint

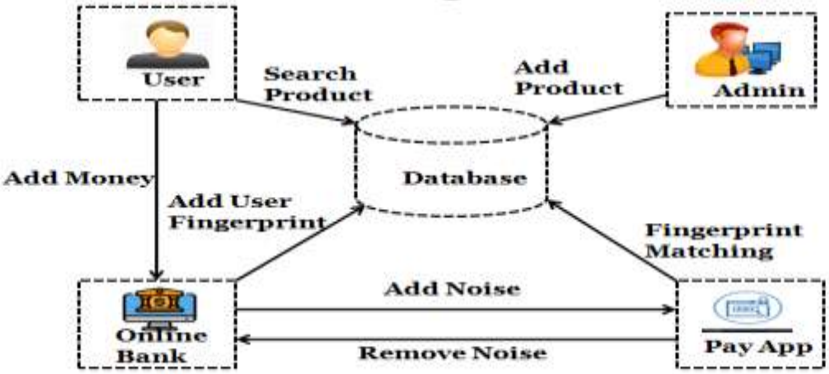

Figure 1: Architecture Diagram of Proposed System

ADVANTAGES

- The 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 is proven to satisfy the differential privacy constraint.
- Fingerprint pattern is unique for every users, so there is no chance for attacks.

V. METHODOLOGY

This paper will helps to overcome the problem of Online banks may disclose consumer's shopping preferences due to various attacks. This paper describes how a customer can purchase products using their Fingerprint Authentication Algorithm. Only when the fingerprint is matched then the customers can able to purchase the products. An Optimized Differential private online transaction scheme (O-DIOR) is used for online banks to set boundaries of consumption amounts with added noises. It helps to provide improved security for Online Shopping. Fingerprint Authentication Algorithm has been used for Finger print Verification.

VI. RESULT

In our research, the user can purchase their products by using his account number and Fingerprint, if the fingerprint matches with the database. User can purchase the products successfully.

VII. CONCLUSION

This project describes how a customer can purchasea products using their Fingerprint Authentication Algorithm. It shows the differential price amount for the purchased products and account number with added noise. The original details had not known to any intermediates. Fingerprint Authentication Algorithm used for Finger print Verification Successfully.

VIII. FUTURE WORK

This approach focuses on user can purchase their products by using their account number and Fingerprint. In Future will implement Three-way authentication Technology (Fingerprint , PIN and 3D-Password) to enhance security of transactions in online Shopping system.

Reference

[1] J. Claessens, V. Dem, D. De Cock, B. Preneel, and J. Vandewalle, "On the security of today's online electronic banking systems," Comput.Secur., vol. 21, no. 3, pp. 253–265, 2002.

[2] S. Kiljan, H. P. E. Vranken, and M. C. J. D. van Eekelen, "Evaluation of transaction authentication methods for online banking," Future Gener.Comput.Syst., vol. 80, pp. 430–447, 2018.

[3] R. Ganesan et al., "A secured hybrid architecture model for internet banking (e-banking)," The J. Internet Banking Commerce, vol. 14, no. 1, pp. 1–17, 1970.

[4] M. Tebaa, K. Zkik, and S. El Hajji, "Hybrid homomorphic encryption method for protecting the privacy of banking data in the cloud," Int. J. Secur.Appl., vol. 9, no. 6, pp. 61–70, 2015.

[5] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," IEEE Trans. Smart Grid, vol. 8, no. 2, pp. 619–626,Mar. 2017.

[6] M. Hardt and K. Talwar, "On the geometry of differential privacy," in Proc. 42ndACMSymp. Theory Comput., 2010, pp. 705–714.

[7] S. Meiser and E. Mohammadi, "Tight on budget?Tight bounds for r-fold approximate differential privacy," in Proc. ACM SIGSAC Conf. Comput.Commun.Secur., 2018, pp. 247–264.

[8] F. Farokhi and H. Sandberg, "Ensuring privacy with constrained additive noise by minimizing fisher information," Automatica, vol. 99, pp. 275–288, 2019.

[9] J. Soria-Comas, J. Domingo-Ferrer, D. S_anchez, and D. Meg_ıas, "Individual differential privacy: A utility-preserving formulation of differential privacy guarantees," IEEE Trans. Inf. Forensics Security, vol. 12, no. 6, pp. 1418–1429, Jun. 2017.

[10] T. Zhu, P. Xiong, G. Li, and W. Zhou, "Correlated differential privacy: Hiding information in non-IID data set," IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 229–242, Feb. 2015.

[11] M. Fanaeepour and B. I. P. Rubinstein, "Histogramming privately ever after: Differentially-private data-dependent error bound optimisation," in Proc. IEEE 34th Int. Conf.Data Eng., 2018, pp. 1204–1207.

[12] K. Chaudhuri, J. Imola, and A. Machanavajjhala, "Capacity bounded differential privacy," in Proc. Int. Conf. Neural Inf. Process. Syst., 2019, pp. 3469–3478.

[13] Z. Zhang, W. Cao, Z. Qin, L. Zhu, Z. Yu, and K. Ren, "When privacy meets economics: Enabling differentially-private batterysupported meter reporting in smart grid," in Proc. IEEE/ACM 25th Int. Symp. Quality Service, 2017, pp. 1–9.

[14] D. Cynthia and L. Jing, "Differential privacy and robust statistics," in Proc. 41st ACM Symp. Theory Comput., 2009, pp. 371–380.

[15] D. Cynthia, "Differential privacy," in Proc. Automata Lang. Program., 2006, pp. 1–10.

[16] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet Things J., vol. 3, no. 6, pp. 854–864, Dec. 2016.

[17] C. Dwork, "Differential privacy: A survey of results," in Proc. Int. Conf. Theory Appl. Models Comput., 2008, pp. 1–19.

[18] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Differentially private data publishing and analysis: A survey," IEEE Trans. Knowl. Data Eng.,vol. 29, no. 8, pp. 1619–1638, Aug. 2017.