Protecting Your Shopping Preference With Differential Privacy

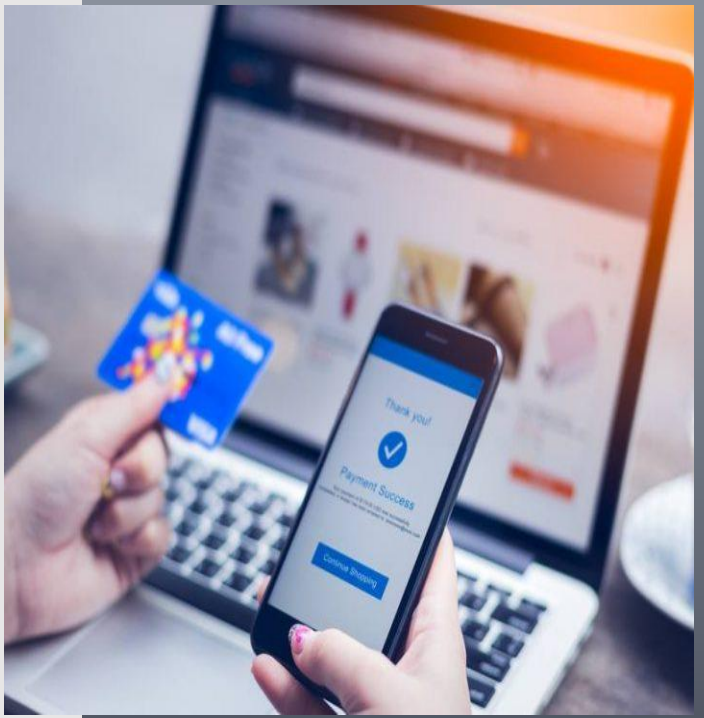
Group No:10
Amal Sankar C N - PKD19IT008
Athira S - PKD19IT017
Lyksina - PKD19IT034
Shahala K P - PKD19IT046

Guided By:
Sajitha M
Assistant Professor
Information Technology

Table Of Contents

Introduction

- In the last decade, online banks were commonly used to provide financial services. However, online banks are vulnerable to outsider and insider attacks.
- If consumers' shopping records are disclosed, consumers may receive advertisement recommendation, harassing message and fraud emails, loan promotion, illegal investigation, property fraud, and even kidnapping.
- An Optimized Differential private Online transaction scheme(O-DIOR) for online banks to set boundaries of consumption amounts with added noises is proposed to provide strong protection to privacy.



Objectives

- A new noise probability density function is used to propose an optimized differential private online transaction scheme (O-DIOR).
- To implement a security module for an online payment application to generate and eliminate the noise to guarantee the utility of consumption amounts.
- The RO-DIOR scheme is further modified to select variable upper and lower boundaries of consumption amount with added noise in online banks.
- To make considerable reduction in the relevance between consumption amount and online bank amount as well as reciprocal information privacy losses.

Problem Statement

Design and implement Optimized Differential Private Online Transaction Scheme to protect the shopping preference of each consumer and set boundaries of consumption amounts with added noises before sending to online banks.

Literature Review

1. Differential Privacy for Industrial Internet of Things: Opportunities, Applications, and Challenges

2. Trustworthy authorization method for security in Industrial Internet of Things

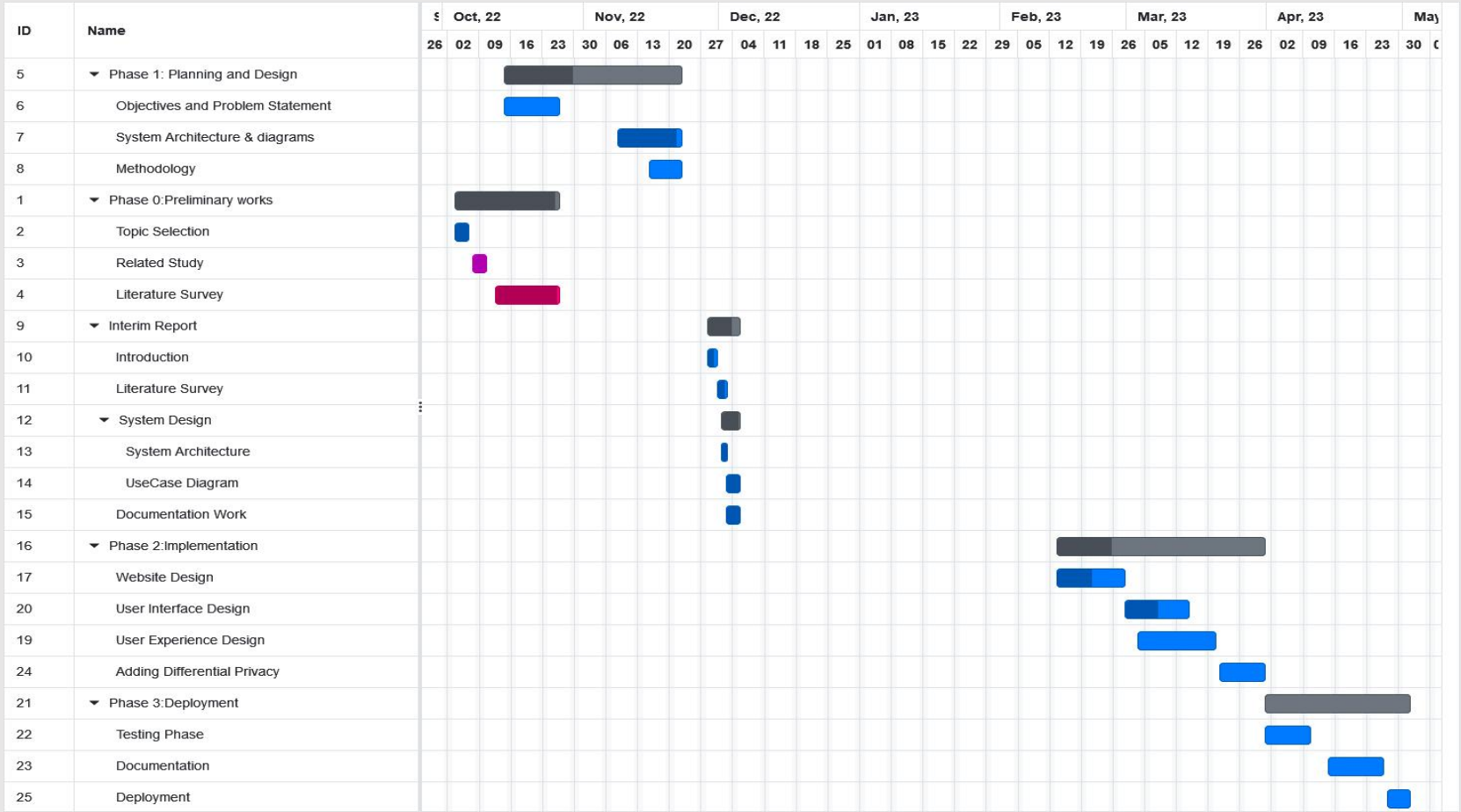
3. Break the Data Barriers While Keeping Privacy: A Graph Differential Privacy Method

4. A Blockchain-Based Approach for Saving and Tracking Differential-Privacy Cost.

Topic	Author	Objective	Methodology	Features	Limitation
Differential Privacy for Industrial Internet of Things: Opportunities, Applications, and Challenges[1]	Jiang, Bin, Jianqiang Li, Guanghui Yue, and Houbing Song	To conduct a comprehensive survey on the opportunities, applications, and challenges of differential privacy in Industrial Internet of things (IIoT).	• Summarizes the privacy issues in the IIoT, and to compare the existing methods. • The privacy measurement using laplace & index mechanism.	• Intelligent Self-decision • Real-time Monitoring • Smart Operation • Logistics Optimization • Smart Energy	• Wireless big data value • Authentication privacy • Privacy in block chain enabled data • Complex Integration of Business and Industry
Trustworthy authorization method for security in Industrial Internet of Things [2]	Zhao, Yang, Jiachen Yang, Yongjun Bao, and Houbing Song	To provide a reliable authentication method based on biological information in view of the human–computer interaction security in IIOT	• A finger vein recognition method combining local image blockcharacteristics and whole image characteristics.	• The complete local binary pattern (CLBP) is utilized to describe the texture details of the image block • The validation experiments are conducted on two public databases to verify the accuracy of our proposed recognition method.	• The quality of fingervein image seriously affects the accuracy of recognition • Multiple forms of identity recognition areconsidered to maintain the security of HCI in IIoT.
Break the Data Barriers While Keeping Privacy: A Graph Differential Privacy Method[3]	Li, Yijing, Xiaofeng Tao, Xuefei Zhang, Mingsi Wang, and Shuo Wang	To focus on how to prevent privacy disclosure of vehicles while sharing vehicle data to improve the service.	• Protect vehicle privacy while achieving cross-platform and cross-service data distribution and sharing utilization. • Accelerated nodes and edges Combined Graph Differential Privacy algorithm (ACGDP)is used.	• Improves storage efficiency • Reduces sharing pressure • Improves privacy protection • Abstract plain text into graph form.	• Disclosure for data privacy protection and the data availability • To minimize the distance between pick up customers each time in order receiving.
A Blockchain-Based Approach for Saving and Tracking Differential-Privacy Cost.[4]	Zhao, Yang, Jun Zhao, Jiawen Kang, Zehang Zhang, Dusit Niyato, Shuyu Shi, and Kwok-Yan Lam.	To design and implement a blockchain-based system for tracking,saving differential-privacy cost & optimal reuse fraction of the old noisy response.	• An algorithm to optimal reuse fraction of the old noisy response and add new noise to minimize the accumulated privacy cost • A data set may be used for answering multiple queries, accumulating the information leakage	• Reduces the number of times to request the server by using recorded noisy results. • Allows participants to track transactions without centralized control. • Complete transaction verification and synchronization.	• Attackers can obtainthe algorithm implemented in the smart contract • Privacy budget is quite limited. • Data set will not support too many different statistical queries.

System Planning

Gantt Chart


ID
Name
Oct, 22
Nov, 22
Dec, 22
Jan, 23
Feb, 23
Mar, 23
Apr, 23
26 02 09 16 23 30 06 13 20 27 04 11 18 25 01 08 15 22 29 05 12 19 26 05 12 19 26 02 09 16 23 30
5 Phase 1: Planning and Design
6 Objectives and Problem Statement
7 System Architecture & diagrams
8 Methodology
1 Phase 0:Preliminary works
2 Topic Selection
3 Related Study
4 Literature Survey
9 Interim Report
10 Introduction
11 Literature Survey
12 System Design
13 System Architecture
14 UseCase Diagram
15 Documentation Work
16 Phase 2:Implementation
17 Website Design
20 User Interface Design
19 User Experience Design
24 Adding Differential Privacy
21 Phase 3:Deployment
22 Testing Phase
23 Documentation
25 Deployment

TASK ALLOCATION

There are 3 major phases and documentation phase.
The three tasks are described below.

User Interface Design

- The user interface design for the project includes the website creation.
- Several pages has to be created including the login page, registration page, shopping page etc.
- Shahala K P & Lyksina are the candidates who are dealing with User interface design.
- Shahala K P will be dealing with the Login & Registration pages of user,merchant,online bank etc.
- Lyksina will be dealing with the other pages in the website.

Database Creation

- Database creation plays a major role in the project. Database consisting several tables has to be implemented.
- Database used by us is MySQL. Amal Sankar C N is assigned the task of creating the database and the tables for Registration for the user.

Noise Generation

- Noise generation is the important phase in the project. Calculating the noise values and boundaries, assigning to the customers account, creating the security module etc is carried out by Athira S.

Documentation phase

- All the documentation including the Report and Project presentation are divided among the 4 members of the team.

FEASIBILITY STUDY

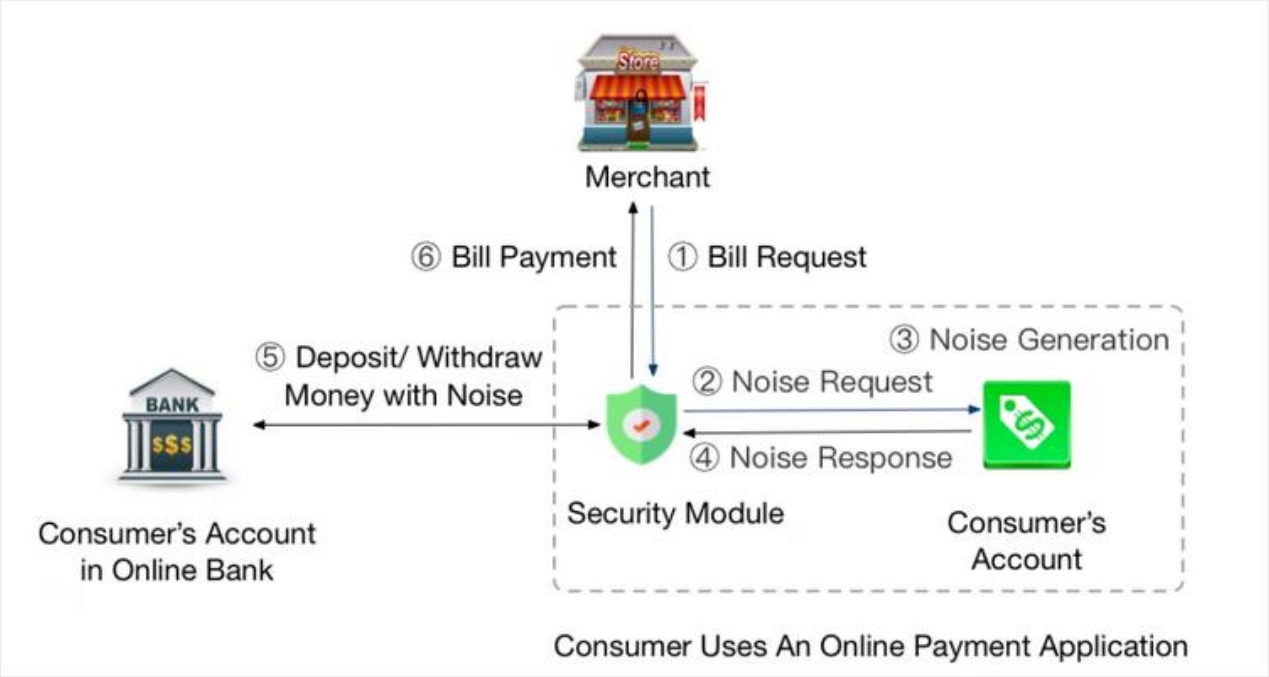
Technical Feasibility

- The prior works in this field have been based on implementing differential privacy.
- But it’s so important to calculate the noises and its boundaries.
- Several methods has to be employed to calculate noise boundaries and to implement the differential privacy.

Financial Feasibility

- Here, there is no need of development cost as well as installation cost as it is a website which uses the MySQL as the database.

System Architecture


Store
Merchant
⑥ Bill Payment
① Bill Request
③ Noise Generation
⑤ Deposit/ Withdraw
Money with Noise
② Noise Request
BANK
$$$
④ Noise Response
Security Module
Consumer's
Account
Consumer's Account
in Online Bank
Consumer Uses An Online Payment Application

The system model consists of three parts
(1) A consumer’s account in the online bank
(2) A security module in a payment application
(3) An account in a payment application.

- 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 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.We employ Apple Pay as the payment application for example.

- For example, a consumer needs to pay $12 to a merchant. Without differential privacy, he needs to withdraw $12 from an online bank, so the actual consumption amount is exposed.

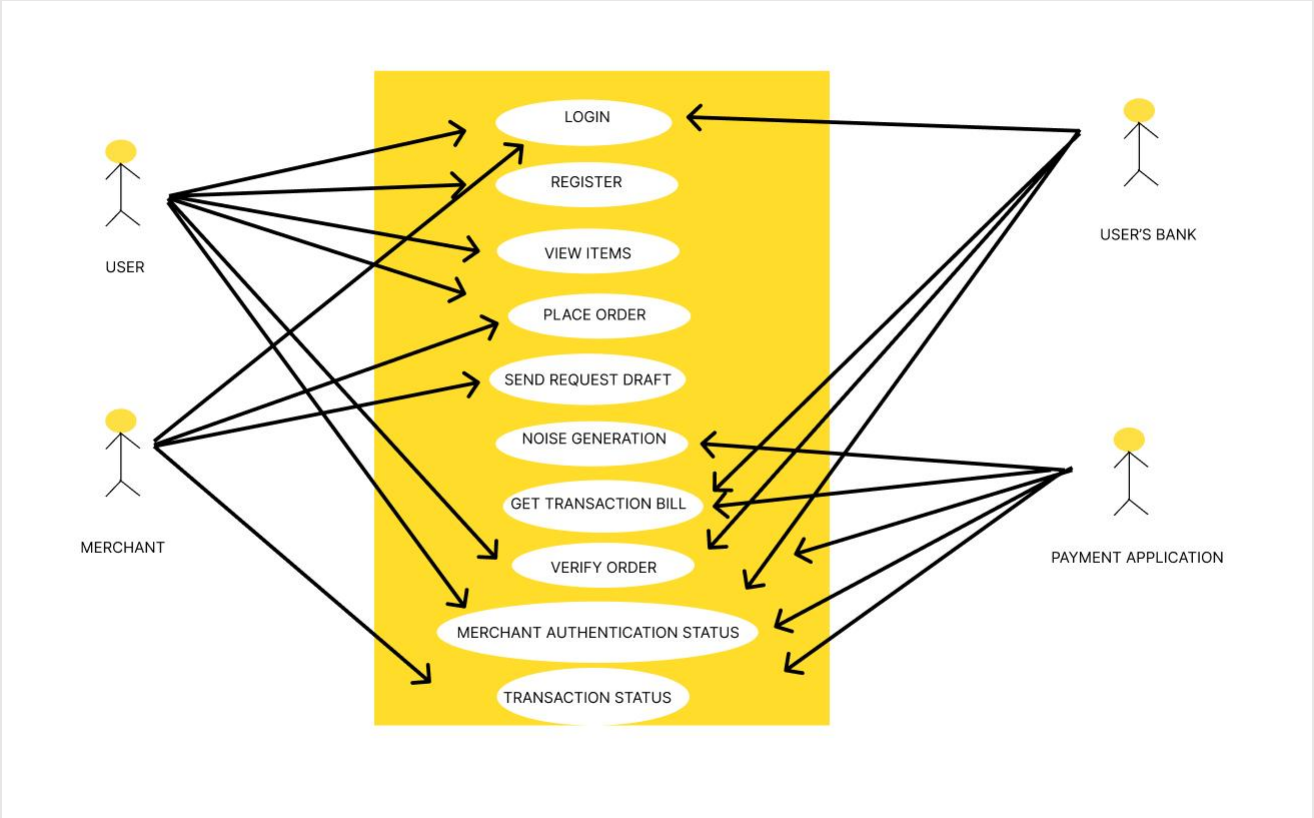
- With differential privacy, if the security module calculates the noise value as $5 and adds the noise to online bank account, so it needs to withdraw $17 from the online bank, which is not $12 as before. Hence, the personal consumption privacy can be protected.

- The security module then saves $5 in the Apple Pay to eliminate the added noise, so the actual consumption amount is $12 as before.

- The consumption record in the online bank is that Apple Pay has withdrawn the money $17 into the consumer's online bank account, so attackers cannot infer the consumer's payment amounts and shopping places in online banks.

System Design

Use-Case Diagram



System Implementation

System Requirements

Software Requirements

- Operating system : Windows 10.
- Coding Language : Java
- Tool : Netbeans 8.2
- Database : MYSQL

Hardware Requirements

- System : Pentium i3 Processor
- Hard Disk : 500 GB.
- Monitor : 15” LED
- Input Devices : Keyboard, Mouse
- Ram : 2 GB

Methodology

Software Requirements Specification

Users

User function

- To create a device data protection system for sending and receiving data.
- Device authority is utilised for delivering an encrypted file and then decrypting it using certain keys in this project. After that, perform a file search and send a key for that file.

Admin Functions

- The owner can register into the sites before logging in.
- Logging in is done using a username and password.

Functional Requirements

There are three groups of useful conditions for the framework

1.Clustering Server:

By selecting the suitable parts, it is possible to determine the level of uniqueness and the level of group uniformity.

2. Customer:

Used for specific customers, which improves executive client communication (CRM).

3. Marketing:

The categories that customers choose that are relevant to them allow the organisation to concentrate on its target consumers and design marketing strategies.

Non-Functional Requirements

Performance requirements

• The system will verify your login credentials in a matter of seconds. It'll be stored in the user, and administrator databases.

Safety Requirements

- The system should be able to revoke the devices when the devices are misplaced or stolen by a third party.
- The devices are subsequently disabled and a new password is assigned by our software.

Security Requirements

For device authentication, system should incorporate security criteria and a password.

Software Quality Attributes

- Availability

Programmes will not hang, will open quickly, and will quickly access data.

- Reliability

Erroneous inputs should be detected and rejected by the system.The system will display error messages if there is a problem.

- Usability

This technology talks with other users and distributes data with ease.

- Maintainability

The device password should be kept safe and the system should be well-maintained.

- Portability

The solution can work on any web browser on any platform with minimum or no adjustments.

STRATEGY

- The fundamental strategy is to basically eliminate the probability that noise is generated beyond the boundaries.

For a consumer's account in the online bank,
o(i) – The balance of the deposit at time i.
α – The minimal deposit
β – The maximal deposit

For his account in a payment application
n(i) represents the noise at time i, and c(i) represents the balance at time i, which is equal to the sum of all noise

$$c(i) = \sum_{j=0}^{i} n(j)$$

The range of noise is $\gamma \leq n(i) \leq \eta$ where n(i) is a negative number while withdrawing money from the payment application and n(i) is a positive number while saving money to the payment application.
For the security module, $d_j(i)$ represents the consumption amount of the j[th] item at time i. The total consumption amount at time i is $d(i) = \sum d_j(i)$
The range of the consumption amount d(i) is $\alpha \leq d(i) \leq \beta$

STRATEGY

- Unlike the online bank, the payment application cannot get the sensitive information, it only assigns the money to the security module to eliminate the noise.
- It cannot send its actual consumption amount to the online bank, because they cannot trust each other. Therefore, the consumer could consider his account in the payment application as a noise generator.
- For example, when the consumer needs to pay money $d(i)$ at time i, the security module calculates a noise. $n(i)$ that draw from Laplace distribution. $f(x) = \frac{1}{2\sigma} e^{\frac{-|x-\mu|}{\sigma}}$ μ is often equal to 0,and σ is determined by the sensitivity which represents the biggest impact of individual data on the result of function f.

- Then the consumer's account in the payment application will pay $n(i)$, and the consumer's account in the online bank will pay $d(i) - n(i)$.

- Let C be the money that consumer needs to pay when shopping.
- The consumer sends his request to the security module.
- The security module receives the request and begins to calculate the noise n under differential privacy.

- When the noise 0, the security module sends his request of withdrawing money C + n to the online bank. The online bank receives this request and sends the money C + n to the security module.
- The security module receives the money C + n, then it saves the money n in the payment application and sends the money C to pay for the bill.
- When the noise < 0, the security module sends the request of withdrawing money n to the payment application.
- The payment application needs to send money n to the security module.
- There are two situations. (1) When the noise n is less than the consumption C, the security module sends the request of withdrawing money C - n to the online bank.
- The online bank sends the money C-n to it. The security module sends the total money C to pay for the bill.
- (2) When the noise n is more than the consumption C, the security module saves money n-C in the online bank and sends money C to pay for the bill.

- Assume that the balance in the consumer's online bank is o(i - 1) = $1000, and the balance in the consumer's payment application is c(i - 1) = $100.
- The consumer goes to Burger King to buy a beef whopper d1(i) = $10:35 and a cake d2(i) = $2:50. The total consumption is d(i) = d1(i) + d2(i) = $12:85.
- If the security module calculates n(i) = -$20 as the noise, which is more than the spending $12:85.
- It will withdraw money $20 in the payment application and save money $7:15 in the online bank.
- After that, the deposit in the online bank is o(i) = o(i - 1) - d(i) - n(i) = $1007:15, and the balance in the payment application is c(i) = c(i-1)+n(i) = $80.
- If the security module calculates the value of noise n(i) = $-5,which is less than the spending $12:85, it can withdraw money $7:85 from the online bank and withdraw money $5 from the payment application.
- Likewise, if the security module calculates the value of noise n(i) = $5, it can withdraw money $17:85 from the online bank and save money $5 in the payment application.
- After that the deposit in the consumer's online bank account is o(i) = o(i-1)-d(i)-n(i) = $982:15, and the balance in the consumer's payment application is c(i) = c(i - 1) + n(i) = $105 .

- User, merchant, bank, payment application has to login using the Email & password. These are stored in the database.

- For registration user has to give the Name, email, phone, address, password. These are stored in the database. It will show whether registration is successful or not.

- Table purchase details will have 4 columns. Product image, product name, price, purchased time.
- There is a search bar provided to search the product.

- Add product feature of merchant has to store the product name, brand, description, price, tag, category, image.

- Add account feature of online bank stores the account details including the name, account number, bank name, branch, amount.

- Account details in transaction will show the username, product name, differential account number, differential price, purchased time.

- For buying the product we have to provide account number and password. Mode of payment is by default payment application.

Summary

- The challenging issue of preserving customer data with uneven privacy is one that online banks must deal with.
- The DIOR system demonstrates a direct implementation of differential privacy.
- We provide O-DIOR, a special private online transaction mechanism, to solve privacy problems in financial transactions.
- O-DIOR may set consumption amount restrictions by adding more noise and taking the account balance range into consideration. When a paid programme generates noise, user actions and behaviour cannot be separated from use data. In order to illustrate RO-DIOR, we modify O-DIOR in order to fulfil the need for alternate boundary selection.
- To our knowledge, this is the first attempt to address the issue of online consumption protection and border issues under unequal privacy.
- Many difficult concerns remain, such as safeguarding shopping locations, dealing with data transfer security, and developing strategies for protecting mobile applications, all of which are intend to address in future work.

References

- Jiang, Bin, Jianqiang Li, Guanghui Yue, and Houbing Song. "Differential privacy for industrial internet of things: Opportunities, applications, and challenges." IEEE Internet of Things Journal 8, no. 13 (2021): 10430-10451 [1].

- Zhao, Yang, Jiachen Yang, Yongjun Bao, and Houbing Song. "Trustworthy authorization method for security in Industrial Internet of Things." Ad Hoc Networks 121 (2021): 102607 [2].

- Ul Hassan, Muneeb, Mubashir Husain Rehmani, Maaz Rehan, and Jinjun Chen. "Differential privacy in cognitive radio networks: A comprehensive survey." Cognitive Computation (2022): 1-36.

- Yang, Wencheng, Song Wang, Jiankun HuHu, and Nickson M. Karie. "Multimedia security and privacy protection in the internet of things: research developments and challenges." International Journal of Multimedia Intelligence and Security 4, no. 1 (2022): 20-46.

Thank You