FINANCIAL FRAUD DETECTION SYSTEM

Session 2022 - 2026

Submitted by

Saba Shahdin 2022-CS-112
Ariba Shafaqat 2022-CS-113
Wajeeha Javed 2022-CS-136
Momina Rashad 2022-CS-137
Ghania Khan Niazi 2022-CS-156

Submitted to

Sir Nazeef Ul Haq

Department of Computer Science

University of Engineering and Technology Lahore, Pakistan

Contents

List of Figures

1 Introduction

The Financial Fraud Detection System stands as a comprehensive solution meticulously crafted to identify, analyze, and mitigate fraudulent activities inherent within financial transactions. By focusing on robust internal mechanisms, our system ensures the delivery of actionable insights to stakeholders, empowering them in fraud prevention and detection endeavors.

1.1 Project Objectives

The primary objectives of this project include:

1.1.1 Tailored Fraud Detection

Create a fraud detection system specifically designed for transactions between merchants and partners.

1.1.2 Real-time Monitoring

Ensure the system can monitor transaction data in real-time and perform continuous analysis to swiftly detect suspicious transactions.

1.1.3 Design User-friendly Interface

Develop an intuitive interface that allows businesses to access and interpret fraud detection alerts easily.

1.1.4 Evaluate System Effectiveness

Conduct comprehensive testing and validation to assess the accuracy and effectiveness of the fraud detection system.

1.1.5 Provide Actionable Insights

Offer businesses actionable insights to mitigate potential financial losses resulting from fraudulent activities.

1.1.6 Maintain System Relevance

Continuously update and refine the system to adapt to evolving fraud tactics and maintain high detection accuracy over time.

2 Project Features

2.1 Comprehensive Fraud Detection

The system offers comprehensive fraud detection capabilities, examining transactions between merchants and partners thoroughly.

2.2 Auditor Examination

An auditor component is integrated into the system, enabling complete examination of fraud detection processes and ensuring robustness.

2.3 Partner Addition

The system allows the addition of new partners, facilitating flexible adaptation to evolving business partnerships.

2.4 Merchant-Partner Transactions

Transactions between merchants and partners are scrutinized, providing a holistic view of financial activities within the ecosystem.

2.5 Multiple Payment Methods

Support for various payment methods, including online transactions, credit card payments, and cheque payments, ensures versatility in fraud detection.

2.6 Threshold-based Detection

The system implements threshold-based detection mechanisms, triggering fraud alerts when transactions exceed predefined thresholds for average credit card, cheque, and online transactions

2.7 Auditor Oversight

Auditors oversee the fraud detection process, ensuring adherence to standards and regulations, and enhancing the system's credibility.

2.8 Graphical Representation

Proper graphs are generated for each payment method, providing visual insights into transaction trends and anomalies.

3 Data Flow Diagram

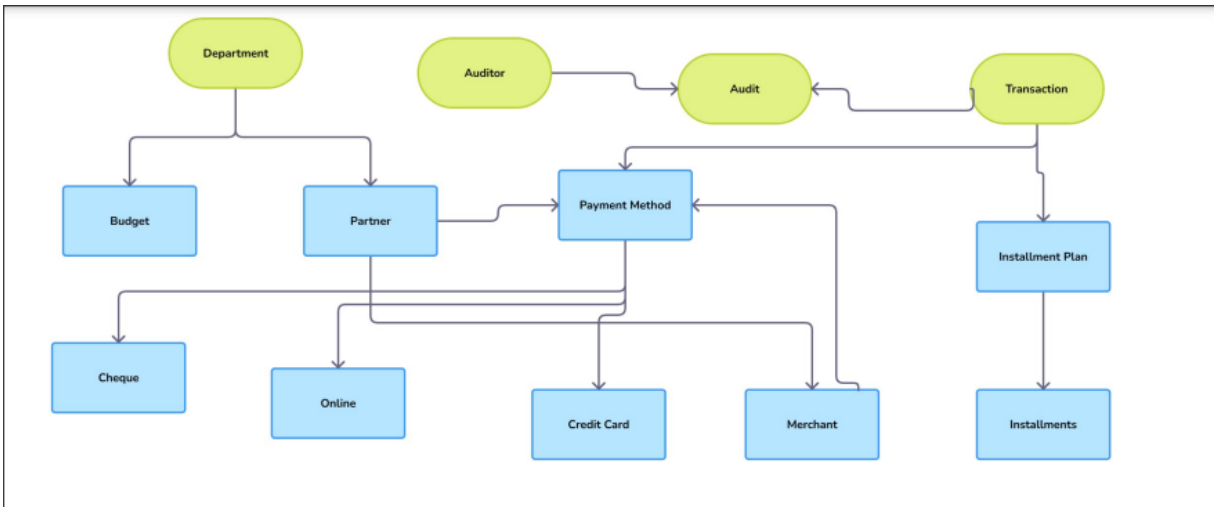

Figure 1: Dataflow diagram for Financial Fraud Detection

4 Entities and Relationships

Department

Attributes: DepartmentID (Primary Key), DepartmentName, TotalAmount, LastTransactionDate, UpdatedDate.
Represents a department within the organization's finance system.

Person

Attributes: PersonID (Primary Key), FirstName, LastName, Gender, Contact, Email.
Represents individuals involved in the system such as employees, partners, and auditors.

UserCredentials

Attributes: CredentialID (Primary Key), Username, Password, PersonID (Foreign Key), LastLoginDate.
Stores login credentials for system users.

Partner

Attributes: PartnerID (Primary Key), DepartmentID (Foreign Key), TotalInvestment, WithdrawalThreshold, Role.
Represents partners associated with specific departments.

Merchant

Attributes: MerchantID (Primary Key), MerchantStatus, MerchantType, LastTransactionDate, PartnerID (Foreign Key).
Represents merchants who engage in transactions with the organization, linked to partners.

Auditor

Attributes: AuditorID (Primary Key), Role, JoinedDate.
Represents auditors who perform audits on the organization's financial activities.

Budget

Attributes: BudgetID (Primary Key), BudgetStatus, Timeframe, BudgetType, BudgetName, DepartmentID (Foreign Key), AllocatedAmount, RemainingAmount.
Represents budgets allocated to departments.

Audit

Attributes: AuditID (Primary Key), Timestamp, AuditorID (Foreign Key), AuditType, AuditStatus.
Represents audits conducted by auditors, linked to auditors.

InstallmentPlan

Attributes: InstallmentPlanID (Primary Key), PartnerID (Foreign Key), MerchantID (Foreign Key), MaxInstallments.
Represents installment plans for transactions, associated with partners and merchants.

CreditCard

Attributes: CreditCardID (Primary Key), BankName, CardNumber, ExpiryDate, CVV, TransactionReference, CardHolderName, ReceiverName.
Represents credit card information used in transactions.

Cheque

Attributes: ChequeID (Primary Key), ChequeNumber, BankName, IssuerName, ReceiverName.
Represents cheque information used in transactions.

Onlines

Attributes: OnlineID (Primary Key), BankName, AccountNumber, TransactionReference, SenderName, ReceiverName.
Represents online transaction information.

PaymentMethod

Attributes: PaymentMethodID (Primary Key), PaymentType, CreditCardID (Foreign Key), ChequeID (Foreign Key), OnlineID (Foreign Key), PartnerID (Foreign Key), MerchantID (Foreign Key).
Associates payment methods with partners, merchants, and specific transactions.

Transactions

Attributes: TransactionID (Primary Key), TransactionType, Amount, Date, PaymentMethodID (Foreign Key), InstallmentPlanID (Foreign Key), BudgetID (Foreign Key).
Represents financial transactions, linked to payment methods, installment plans, and budgets.

Installments

Attributes: InstallmentID (Primary Key), InstallmentPlanID (Foreign Key), TransactionID (Foreign Key), InstallmentNumber, TotalAmount, PaidAmount, DueDate, PaymentStatus.
Represents installment details for installment plans and transactions.

Invoice

Attributes: InvoiceID (Primary Key), Amount, Date.
Represents invoices generated for transactions.

FraudAlerts

Attributes: AlertID (Primary Key), TransactionID (Foreign Key), AlertDate, AlertReason, AuditID (Foreign Key).
Represents alerts raised for potential fraud in transactions, linked to transactions and audits.

AuditorAction

Attributes: ActionID (Primary Key), AlertID (Foreign Key), ActionDate, TransactionID (Foreign Key), AuditID (Foreign Key), ActionReason, AuditAction, AuditResult. Represents actions taken by auditors in response to fraud alerts, linked to alerts, transactions, and audits.

5 Database Schema Diagram

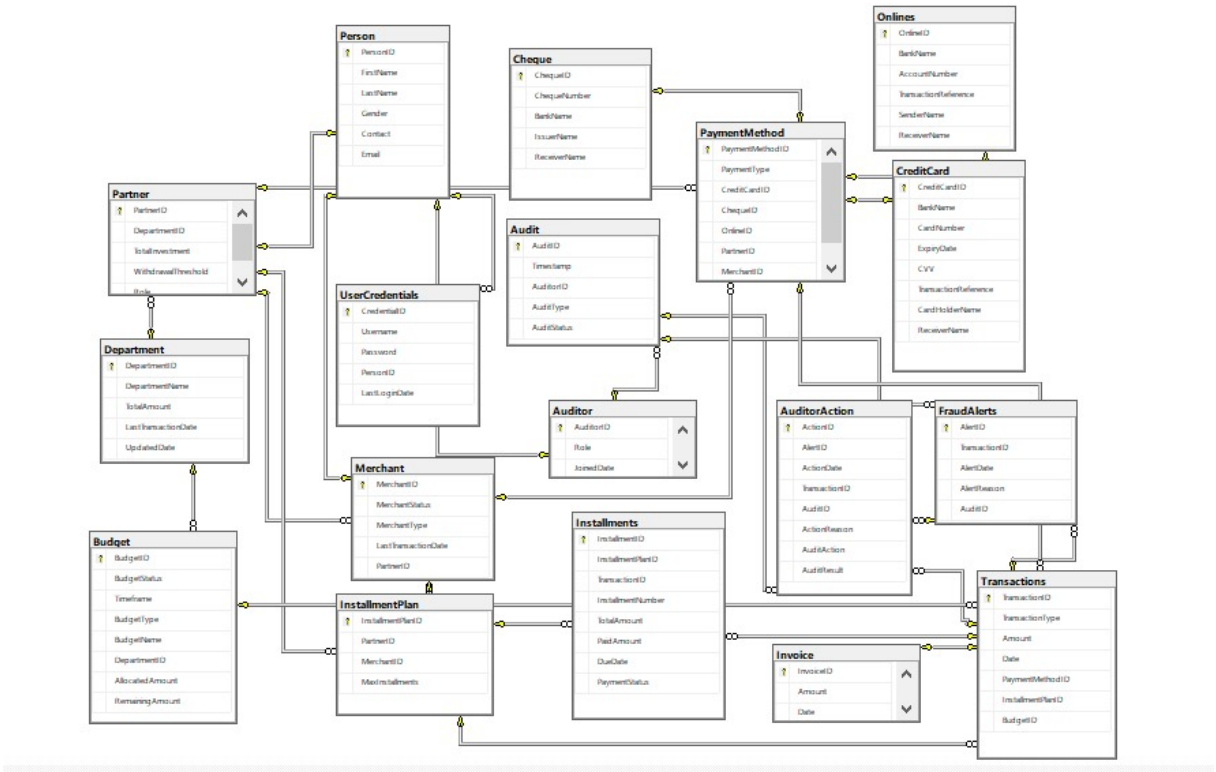

Figure 2: Database diagram for Financial Fraud Detection

6 Foreign Key Constraints

UserCredentials(PersonID)

This foreign key constraint links the `PersonID` column in the `UserCredentials` table to the `PersonID` column in the `Person` table. It ensures that every `PersonID` value in the `UserCredentials` table must correspond to an existing `PersonID` in the `Person` table. This relationship maintains integrity by associating user credentials with specific individuals.

Partner(PartnerID, DepartmentID)

PartnerID

The foreign key constraint on `PartnerID` references the `PersonID` column in the `Person` table, ensuring that each `PartnerID` in the `Partner` table corresponds to a valid `PersonID`. This maintains consistency by linking partners to individual persons.

DepartmentID

The foreign key constraint on `DepartmentID` links the `DepartmentID` column in the `Partner` table to the `DepartmentID` column in the `Department` table. It ensures that every `DepartmentID` value in the `Partner` table refers to an existing `DepartmentID` in the `Department` table, establishing the association between partners and departments.

Merchant(PartnerID)

This foreign key constraint associates the `PartnerID` column in the `Merchant` table with the `PartnerID` column in the `Partner` table. It guarantees that each `Merchant` is associated with a valid partner, maintaining the integrity of merchant-partner relationships.

Auditor(AuditorID)

The foreign key constraint on `AuditorID` links the `AuditorID` column in the `Auditor` table to the `PersonID` column in the `Person` table. It ensures that each auditor in the system corresponds to a valid person, maintaining consistency in the auditor records.

Budget(DepartmentID)

This foreign key constraint connects the `DepartmentID` column in the `Budget` table to the `DepartmentID` column in the `Department` table. It guarantees that each budget record is associated with an existing department, ensuring consistency and integrity in budget allocation.

Audit(AuditorID)

The foreign key constraint on `AuditorID` links the `AuditorID` column in the `Audit` table to the `AuditorID` column in the `Auditor` table. It ensures that each audit record is associated with a valid auditor, maintaining the integrity of audit data.

InstallmentPlan(PartnerID, MerchantID)

PartnerID

This foreign key constraint associates the `PartnerID` column in the `InstallmentPlan` table with the `PartnerID` column in the `Partner` table. It ensures that each installment plan is associated with a valid partner, maintaining consistency in installment plans.

MerchantID

This foreign key constraint associates the `MerchantID` column in the `InstallmentPlan` table with the `MerchantID` column in the `Merchant` table. It ensures that each installment plan is associated with a valid merchant, maintaining consistency in installment plans.

PaymentMethod(PartnerID, MerchantID)

PartnerID

This foreign key constraint associates the `PartnerID` column in the `PaymentMethod` table with the `PartnerID` column in the `Partner` table. It ensures that each payment method is associated with a valid partner, maintaining consistency in payment methods.

MerchantID

This foreign key constraint associates the `MerchantID` column in the `PaymentMethod` table with the `MerchantID` column in the `Merchant` table. It ensures that each payment method is associated with a valid merchant, maintaining consistency in payment methods.

7 Indexing

To enhance query performance, appropriate indexing strategies have been implemented. Indexes are applied to key attributes, facilitating faster retrieval of records in response to user queries. For instance, indexing may be applied to the primary key attributes of entities for efficient data retrieval.

8 Database Integrity

Data integrity constraints, such as primary key, foreign key, unique, and check constraints, play a vital role in ensuring data integrity within a database schema. These constraints enforce rules and conditions on the data to prevent invalid or inconsistent values from being stored. For example, a primary key constraint ensures that each record in a table has a unique identifier, while a foreign key constraint maintains referential integrity between related tables

9 Stored Procedure

- Credit Card Fraud Detection
- Cheque Fraud Detection
- Online Fraud Detection
- Adding Merchant
- Installment Fraud Detection
- Invoice Fraud Detection

10 Triggers

- Subtract Budget Amount Trigger
  To subtract or add Amount from respective budget of each transaction according to its type.
- Insert Invoice On Transaction Trigger
  For rapid generation of invoice whenever transaction is done.
- Update Department Amount Trigger
  To update the amount from respective department whenever budget is allocated.
- Update Budget And Department Trigger
  On updating budget the department record is also updated.

11 Transaction

Sign Up Process:

Handling the record of sign-up involves database transactions because the record has to move across 3 tables for successful results. From the person table to user credentials and finally to assigning the desired role for the account.

Merchant Records:

The insertion of merchant records involves database transactions. This process includes inserting merchant-related data into the appropriate tables in the database.

Transactions:

Transactions involve inserting data into the transactions table. Data for transactions likely comes from various entities, possibly including users, merchants, and items/services being transacted.

12 Wire frames

Figure 3: Audit

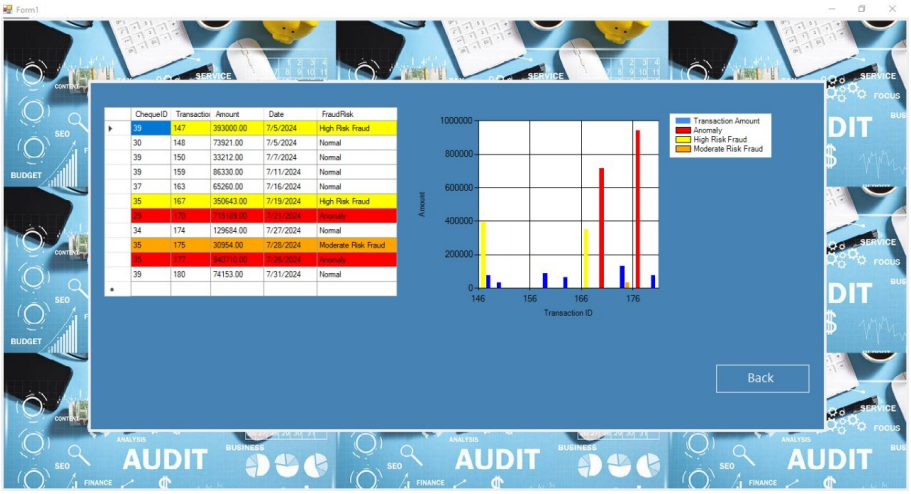

Figure 4: Resulting Graph

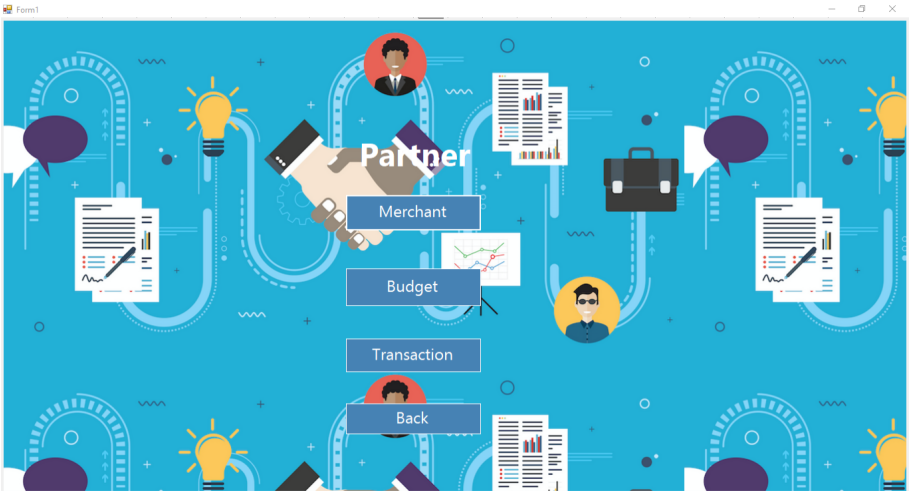

Figure 5: Partner

13 Reports

13.1 Audit Result:

The result of all the audit against transactions are view by the auditor in the single report format for the further decisions

Audit Result 5/10/2024

ActionDate	Amount	MerchantName	Reason	Action	Result
5/10/2024	16,317.00	Amber Nguyen	Moderate Risk Fraud	Not fair	Qualified
5/10/2024	38,850.00	Steven Lloyd	Normal	True and fair	Unqualified
5/10/2024	33,118.00	Mitchell Hoover	Normal	True and fair	Unqualified
5/10/2024	12,400.00	Tommy Cole	Moderate Risk Fraud	Not fair	Qualified
5/10/2024	28,186.00	Erica Schneider	Normal	True and fair	Unqualified
5/10/2024	79,820.00	Ebony Moses	Normal	True and fair	Unqualified
5/10/2024	24,291.00	Deborah Hall	Normal	True and fair	Unqualified
5/10/2024	185,100.00	Cory Cole	High Risk Fraud	Not fair	Qualified
5/10/2024	22,955.10	Dana Butler	Normal	True and fair	Unqualified
5/10/2024	83,502.30	Erica Schneider	Moderate Risk Fraud	Not fair	Qualified
5/10/2024	10,296.60	Cory Cole	Moderate Risk Fraud	Not fair	Qualified
5/10/2024	33,676.80	Rodney Moore	Normal	True and fair	Unqualified
5/10/2024	46,747.30	Ebony Moses	Normal	True and fair	Unqualified
5/10/2024	22,044.10	Dana Butler	Normal	True and fair	Unqualified
5/10/2024	95,505.10	Erica Schneider	High Risk Fraud	Not fair	Qualified
5/10/2024	45,539.20	Ryan Long	Normal	True and fair	Unqualified
5/10/2024	37,907.00	Cassandra Larse	Normal	True and fair	Unqualified
5/10/2024	25,732.30	Maria Moore	Normal	True and fair	Unqualified

Figure 6: Report of Audit Result

13.2 Fraud Alerts:

After passing the transactions through audit process the fraud risk alerts can also be monitored and viewed through single report

Fraud Alerts 5/10/2024

Merchant Name	Amount	Reason	DATE
Amber Nguyen	16,317.00	Moderate Risk Frau	5/10/202
Tommy Cole	12,400.00	Moderate Risk Frau	5/10/202
Cory Cole	185,100.00	High Risk Fraud	5/10/202
Erica Schneider	83,502.30	Moderate Risk Frau	5/10/202
Cory Cole	10,296.60	Moderate Risk Frau	5/10/202
Erica Schneider	95,505.10	High Risk Fraud	5/10/202
Ryan Long	257,320.30	Anomaly	5/10/202
Steven Lloyd	79,500.70	Moderate Risk Frau	5/10/202
Maria Moore	25,732.30	High Risk Fraud	5/10/202
Erica Schneider	40,213.50	Moderate Risk Frau	5/10/202
Dana Butler	22,044.10	Moderate Risk Frau	5/10/202
Erica Schneider	95,505.10	Moderate Risk Frau	5/10/202
Erica Schneider	40,213.50	Anomaly	5/10/202
Amber Nguyen	16,317.00	Moderate Risk Frau	5/10/202
Tommy Cole	12,400.00	Moderate Risk Frau	5/10/202
Cory Cole	185,100.00	High Risk Fraud	5/10/202
Erica Schneider	83,502.30	Moderate Risk Frau	5/10/202
Cory Cole	10,296.60	Moderate Risk Frau	5/10/202

Figure 7: Report of Fraud Alerts

13.3 Transaction:

The record of all transaction along with the merchant involved , amount , transaction type and date are view in a single report for easy analysis

Transaction Details 5/10/2024

PaymentType	TransactionType	Amount	Merchant Name	Date
Credit Card	Expense	284,714.00	Ryan Long	1/1/2024
Cheque	Expense	36,082.50	Rodney Moore	1/28/202
Credit Card	Expense	40,070.00	Rodney Moore	1/29/202
Cheque	Expense	34,003.60	Ebony Moses	1/30/202
Credit Card	Expense	40,400.00	Rodney Moore	1/31/202
Cheque	Income	1,594.40	Rodney Moore	1/31/202
Cheque	Expense	15,694.40	Ryan Long	1/31/202
Credit Card	Income	20,130.00	Ryan Long	2/1/2024
Online	Income	48,410.10	Ebony Moses	2/1/2024
Cheque	Expense	18,546.50	Tommy Cole	2/3/2024
Online	Income	12,490.60	Mitchell Hoover	2/3/2024
Cheque	Expense	32,061.50	Erica Schneider	2/4/2024
Credit Card	Income	24,630.00	Tyler Moore	2/5/2024
Cheque	Expense	27,996.70	Dana Butler	2/5/2024

Figure 8: Report of Transaction

13.4 Count of Merchant :

The merchants are closely analyzed for the proper handling of transactions that's why all record of merchant their transaction and amount are closely reviewed

Merchant Transactions 5/10/2024

MerchantID	Total Transactions	TotalAmount
12	13	534,000.60
13	3	152,753.60
14	5	172,660.50
16	2	45,608.60
17	6	206,554.30
19	3	60,359.70
21	2	37,081.30
24	2	69,017.00
25	14	1,153,036.50
29	9	466,346.70
30	3	50,970.50
31	3	49,427.10
32	9	820,580.20
33	2	195,396.60
34	10	237,201.00
36	1	46,800.00
38	5	293,478.60

Figure 9: Report of Merchant Records

13.5 Installment :

Some transaction involve installment so their record is necessary to compare the transaction with installment and without installment for easy fraud analysis

Transactions Involving installments 5/10/2024

TransactionID	installmentNumber	MaxInstallments	Amount	TotalAmount
3	1	2	36,082.50	39,277.50
9	1	3	20,130.00	101,769.00
10	1	3	48,410.10	146,223.00
15	1	2	27,996.70	248,437.00
16	1	3	17,590.00	110,560.00
19	2	3	32,333.40	146,223.00
20	1	2	46,800.00	54,172.00
24	2	3	42,440.00	101,769.00
26	1	2	33,069.90	49,137.00
27	1	2	20,024.00	109,436.00
29	1	2	30,378.20	121,108.00
32	2	2	90,730.20	121,108.00
35	1	3	39,850.00	57,174.00
36	1	2	29,220.00	99,213.00
37	1	3	48,374.80	96,207.00
38	1	3	37,903.00	135,008.00
40	1	3	97,303.10	233,021.00
41	1	3	87,008.90	132,520.00
46	2	2	31,957.60	39,277.50
47	2	2	16,068.20	49,137.00
48	1	2	29,215.60	52,166.00

Figure 10: Report of Merchant Records

14 Conclusion

In conclusion, the Financial Fraud Detection System embodies a sophisticated approach to safeguarding against financial malfeasance. Its utilization of indexing strategies, stringent data integrity constraints, and trigger mechanisms demonstrates a commitment to maintaining the integrity of financial data. As technology and threats evolve, continued vigilance and adaptation will be paramount to ensuring the system's efficacy in detecting and deterring fraudulent activities, thereby safeguarding the interests of stakeholders and maintaining trust in financial transactions.