SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Winter Semester- 2024-25

CSI1007- Software Engineering Principles

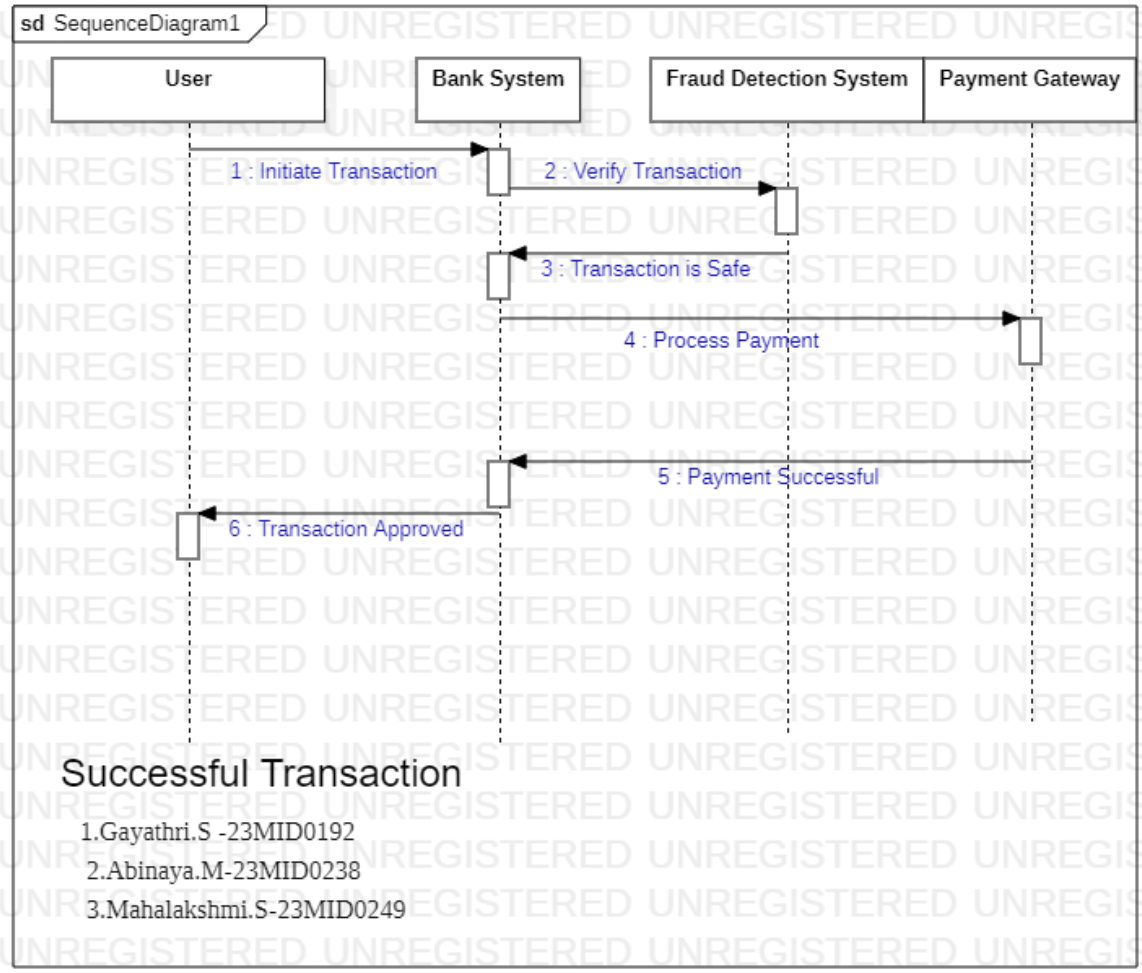
Lab Assesment-4

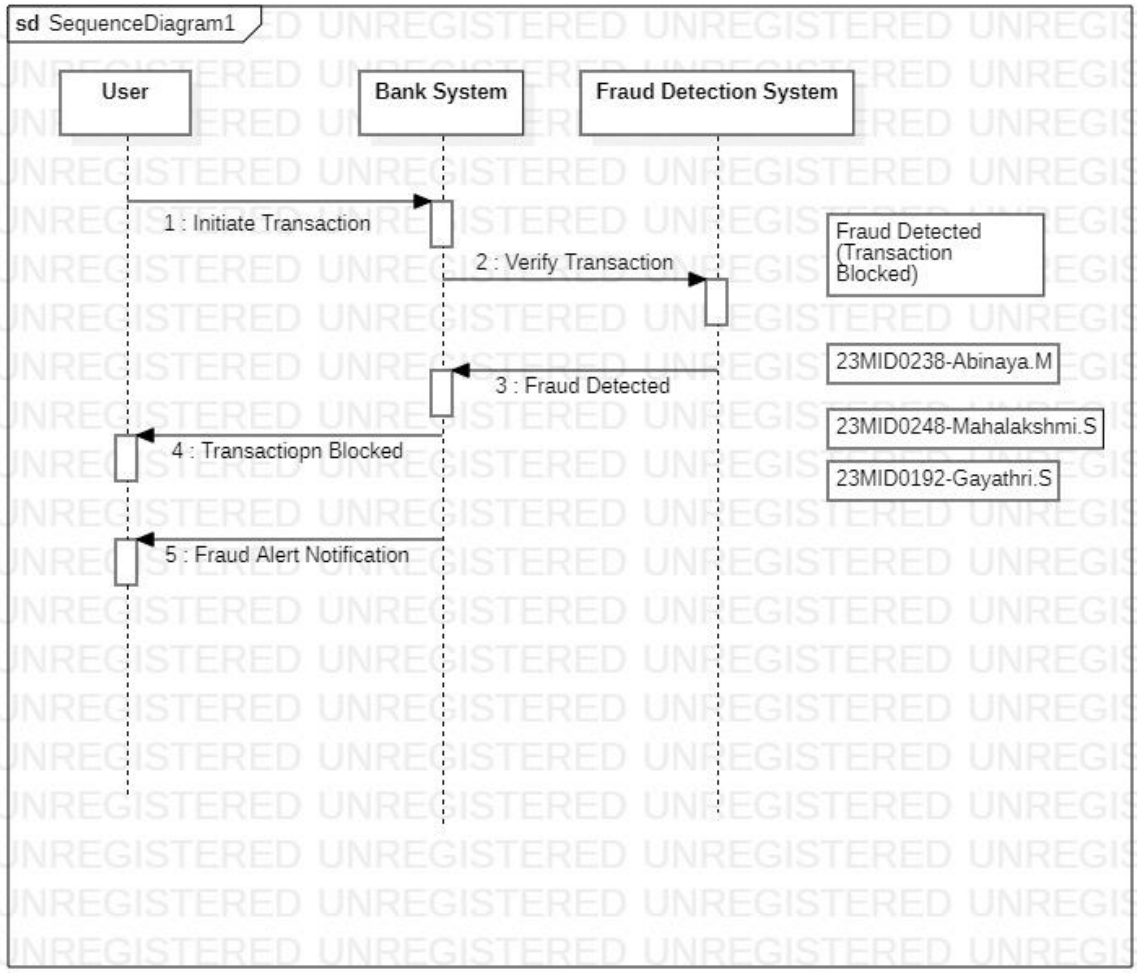
Name: Gayathri.S

Reg no: 23MID0192

Slot: L13+L14

1.Draw sequence diagrams to visualize the interactions within your project for 2 scenarios.





2. Create comprehensive test cases for 2 key scenarios in your project.

Test Scenario 1: Successful Transaction

Test Case Description:
Ensure that a legitimate transaction with valid details is processed successfully without any fraud alerts.

Test Steps:

1. Open the online transaction page.

2. Enter valid payment details (card number, expiration date, CVV).

3. Enter valid personal details (name, billing address).

4. Click the "Pay Now" button.

5. The system sends the transaction details to the Bank System.

6. The Bank System calls the Fraud Detection System (FDS) for verification.

7. FDS analyzes the transaction and confirms it is safe.

8. The Bank System processes the payment through the Payment Gateway.

9. Receive a confirmation that the payment was successful.

Test Data:

Valid Case:

Payment Amount: $50

Card Number: 4111 1111 1111 1111

Expiration: 12/25

CVV: 123

Device/Location: Registered device and usual location

Test Expected Result:

The transaction should be processed without interruption.

The user should see a confirmation message such as "Transaction Approved" or be redirected to a success page.

Actual Result:

Valid transaction was processed successfully, and a confirmation message was displayed.

Pass/Fail: Pass

Test Scenario 2: Fraud Detected (Transaction Blocked)

Test Case Description:

Ensure that the system correctly identifies and blocks a fraudulent transaction, preventing unauthorized payment processing.

Test Steps:

1. Open the online transaction page.

2. Enter payment details that appear suspicious (e.g., a stolen or fake card).

3. Enter mismatched personal details or use a new/unregistered device.

4. Click the "Pay Now" button.

5. The system sends the transaction details to the Bank System.

6. The Bank System calls the Fraud Detection System (FDS) for verification.

7. FDS detects high-risk factors (e.g., unusual amount, location, or device) and flags the transaction as fraudulent.

8. The Bank System blocks the transaction.

9. The system displays an error message and sends a fraud alert notification to the user.

Test Data:

Fraudulent Case:

Payment Amount: $5000

Card Number: 4000 0000 0000 0002 (or similar test data for a flagged card)

Expiration: 11/23

CVV: 321

Device/Location: New, unregistered device from an unusual location

IP Address: Suspicious or blacklisted IP

Test Expected Result:

The transaction should be blocked.

The user should receive a message stating "Transaction Blocked – Fraud Detected" along with a fraud alert notification.

Actual Result:

The system blocked the transaction and displayed the fraud alert message as expected.

Pass/Fail: Pass