CRIME DETECTION IN CREDIT CARD FRAUD

A PROJECT REPORT

Submitted by

SAKTHI SWATHI .M (2303811710422135)

in partial fulfillment of requirements for the award of the course

CGB1201 - JAVA PROGRAMMING

In

COMPUTER SCIENCE AND ENGINEERING

K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY

(An Autonomous Institution, affiliated to Anna University Chennai and Approved by AICTE, New Delhi)

SAMAYAPURAM – 621 112

NOVEMBER- 2024

K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY (AUTONOMOUS)

SAMAYAPURAM – 621 112

BONAFIDE CERTIFICATE

Certified that this project report on **“CRIME DETECTION IN CREDIT CARD FRAUD”** is the bonafide work of **SAKTHI SWATHI.M(2303811710422135)** who carried out the project work during the academic year 2024 - 2025 under my supervision.

CGB1201-JAVA PROGRAMMING Dr.A.DELPHIN CAROLINA RANI, M.E.,Ph.D., HEAD OF THE DEPARTMENT PROFESSOR	CGB1201-JAVA PROGRAMMING Mr.MALARMANNAN A, M.E., SUPERVISOR ASSISTANTP ROFESSOR
SIGNATURE	**SIGNATURE**
Dr.A.Delphin Carolina Rani, M.E.,Ph.D.,	Mr. A. Malarmannan, M.E.,
HEAD OF THE DEPARTMENT	**SUPERVISOR**
PROFESSOR	ASSISTANT PROFESSOR
Department of CSE	Department of CSE
K.Ramakrishnan College of Technology (Autonomous)	K.Ramakrishnan College of Technology (Autonomous)
Samayapuram–621112.	Samayapuram–621112.

Submitted for the viva-voce examination held on …………….

CGB1201-JAVA PROGRAMMING Mr. M. SARAVANAN, M.E., INTERNAL EXAMINER ASSISTANT PROFESSOR	CGB1201-JAVA PROGRAMMING Mr.R. KARTHIK, M.E., EXTERNAL EXAMINER ASSISTANT PROFESSOR 8138-SCE, TRICHY. 06/12/2024
INTERNAL EXAMINER	EXTERNAL EXAMINER

DECLARATION

I declare that the project report on **“CRIME DETECTION IN CREDIT CARD FRAUD”** is the result of original work done by us and best of our knowledge, similar work has not been submitted to **“ANNA UNIVERSITY CHENNAI”** for the requirement of Degree of **BACHELOR OF ENGINEERING**. This project report is submitted on the partial fulfilment of the requirement of the completion of the course **CGB1201 - JAVA PROGRAMMING.**

.

Signature

M. Sakthi Swathi

SAKTHI SWATHI.M

Place: Samayapuram

Date: 6/12/2024

ACKNOWLEDGEMENT

It is with great pride that I express our gratitude and in-debt to our institution “**K.Ramakrishnan College of Technology (Autonomous)**”, for providing us with the opportunity to do this project.

I glad to credit honourable chairman **Dr. K. RAMAKRISHNAN**, **B.E.,** for having provided for the facilities during the course of our study in college.

I would like to express our sincere thanks to our beloved Executive Director **Dr. S. KUPPUSAMY, MBA, Ph.D.,** for forwarding to our project and offering adequate duration in completing our project.

I would like to thank **Dr. N. VASUDEVAN, M.Tech., Ph.D.,** Principal, who gave opportunity to frame the project the full satisfaction.

I whole heartily thanks to **Dr. A. DELPHIN CAROLINA RANI, M.E.,Ph.D.,** Head of the department, **COMPUTER SCIENCE AND ENGINEERING** for providing her encourage pursuing this project.

I express our deep expression and sincere gratitude to our project supervisor **MR. A. MALARMANNAN, M.E.,** Department of **COMPUTER SCIENCE AND ENGINEERING,** for his incalculable suggestions, creativity, assistance and patience which motivated us to carry out this project.

I render our sincere thanks to Course Coordinator and other staff members for providing valuable information during the course.

I wish to express our special thanks to the officials and Lab Technicians of our departments who rendered their help during the period of the work progress.

VISION OF THE INSTITUTION

To serve the society by offering top-notch technical education on par with global standards

MISSION OF THE INSTITUTION

- Be a center of excellence for technical education in emerging technologies by exceeding the needs of the industry and society.
- Be an institute with world class research facilities
- Be an institute nurturing talent and enhancing the competency of students to transform them as all-round personality respecting moral and ethical values

VISION OF DEPARTMENT

To be a center of eminence in creating competent software professionals with research and innovative skills.

MISSION OF DEPARTMENT

M1: Industry Specific: To nurture students in working with various hardware and software platforms inclined with the best practices of industry.

M2: Research: To prepare students for research-oriented activities.

M3: Society: To empower students with the required skills to solve complex technological problems of society.

PROGRAM EDUCATIONAL OBJECTIVES

1. PEO1: Domain Knowledge

To produce graduates who have strong foundation of knowledge and skills in the field of Computer Science and Engineering.

2. PEO2: Employability Skills and Research

To produce graduates who are employable in industries/public sector/research organizations or work as an entrepreneur.

3. PEO3: Ethics and Values

To develop leadership skills and ethically collaborate with society to tackle real-world challenges.

PROGRAM SPECIFIC OUTCOMES (PSOs)

PSO 1: Domain Knowledge

To analyze, design and develop computing solutions by applying foundational concepts of Computer Science and Engineering.

PSO 2: Quality Software

To apply software engineering principles and practices for developing quality software for scientific and business applications.

PSO 3: Innovation Ideas

To adapt to emerging Information and Communication Technologies (ICT) to innovate ideas and solutions to existing/novel problems

PROGRAM OUTCOMES (POs)

Engineering students will be able to:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions

5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations

6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice

7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development

8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

ABSTRACT

The **Credit Card Fraud Detection** program, built using Java's AWT library, is a graphical application designed to validate credit card numbers and PINs. It simulates fraud detection by allowing users to input a card number and PIN, comparing them with predefined valid credentials for ten users. The program enforces input validation for card numbers (8 digits) and PINs (4 digits). Upon successful validation, it grants access and resets the incorrect attempt counter. If the input is invalid, it increments the attempt count and displays an error message. After three incorrect attempts, it triggers a fraud alert, including a beep sound and an alert dialog.The application provides a user-friendly interface with input fields, validation buttons, and result labels. It uses dialogs for success or fraud alerts, enhancing user interaction. The program incorporates essential security measures like masked PIN input and a limited number of login attempts to simulate a basic fraud detection mechanism. Its modular design ensures ease of modification and serves as an educational example of AWT-based GUI development.

ABSTRACT WITH POs AND PSOs MAPPING

CO 5 : BUILD JAVA APPLICATIONS FOR SOLVING REAL-TIME PROBLEMS.

ABSTRACT	POs MAPPED	PSOs MAPPED
The **Credit Card Fraud Detection** program, built using Java's AWT library, is a graphical application designed to validate credit card numbers and PINs. It simulates fraud detection by allowing users to input a card number and PIN, comparing them with predefined valid credentials for ten users. The program enforces input validation for card numbers (8 digits) and PINs (4 digits). Upon successful validation, it grants access and resets the incorrect attempt counter.	**PO1 -3** **PO2 -3** **PO3 -3** **PO4 -3** **PO5 -3** **PO6 -3** **PO7 -3** **PO8 -3** **PO9 -3** **PO10 -3** **PO11-3** **PO12 -3**	**PSO1 -3** **PSO2 -3** **PSO3 -3**

Note: 1- Low, 2-Medium, 3- High

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Objective

The objective of the Credit Card Fraud Detection program is to detect fraudulent credit card activities by validating the card number and PIN entered by a user against predefined valid card numbers and PINs. The program aims to:Ensure correct card number (8 digits) and PIN (4 digits) are entered.Allow a maximum number of incorrect attempts before flagging the account as a potential fraud case.Alert the user when fraudulent behavior is suspected, either due to repeated invalid inputs or correct inputs triggering a success.

1.2 Overview

The program provides a graphical user interface (GUI) using AWT (Abstract Window Toolkit) to interact with the user. The user enters their card number and PIN, and the program checks whether the combination exists in the list of predefined card numbers and PINs. If the details are valid, access is granted. Otherwise, the system tracks incorrect attempts and gives an alert after a predefined number of failed attempts. After a successful attempt, an alert is shown confirming the successful validation**.**

1.3 Java Programming Concepts

1.3.1 AWT (Abstract Window Toolkit):

- Used to build the user interface (UI) of the application, such as windows, buttons, text fields, and labels.
- Frame, TextField, Button, Label, Dialog are all AWT components used in this program.

1.3.2 Event Handling:

- The program uses ActionListener to capture user interactions (clicking the"Validate" button).
- Different actions like entering card numbers and PINs are handled by the actionPerformed() method.

1.3.3 Array Handling:

- The program uses arrays to store valid card numbers and PINs for 10 users.
- It iterates over these arrays to check if the input card number and PIN match any valid combination**.**

1.3.4 Control Flow:

- Conditional statements like if and else are used to check whether the entered details match the valid data.
- Loops (like for loop) are used to iterate through the list of predefined valid card numbers and PINs.
- The program uses a counter (incorrectAttempts) to track the number of failed attempts.

1.3.5 Dialog Boxes:

- The Dialog class is used to show success or fraud alerts as pop-up windows

1.3.6 Error Handling:

- The program checks the lengths of the card number and PIN to ensure they meet the required format

CHAPTER 2

PROJECT METHODOLOGY

2.1 Proposed Work

2.1.1 Enhancements for User Experience:

- Implement better error handling to capture various possible user input mistakes, such as entering letters or special characters in place of digits.
- Add additional security features like checking for locked accounts after multiple failed attempts.
- Optionally, integrate this program with a real database for storing valid card numbers and PINs.

2.1.2 Scalability:

- Expand the program to handle a larger number of users, card numbers, and PINs.
- Implement better fraud detection algorithms based on more complex criteria, such as geographical location, transaction patterns, etc.

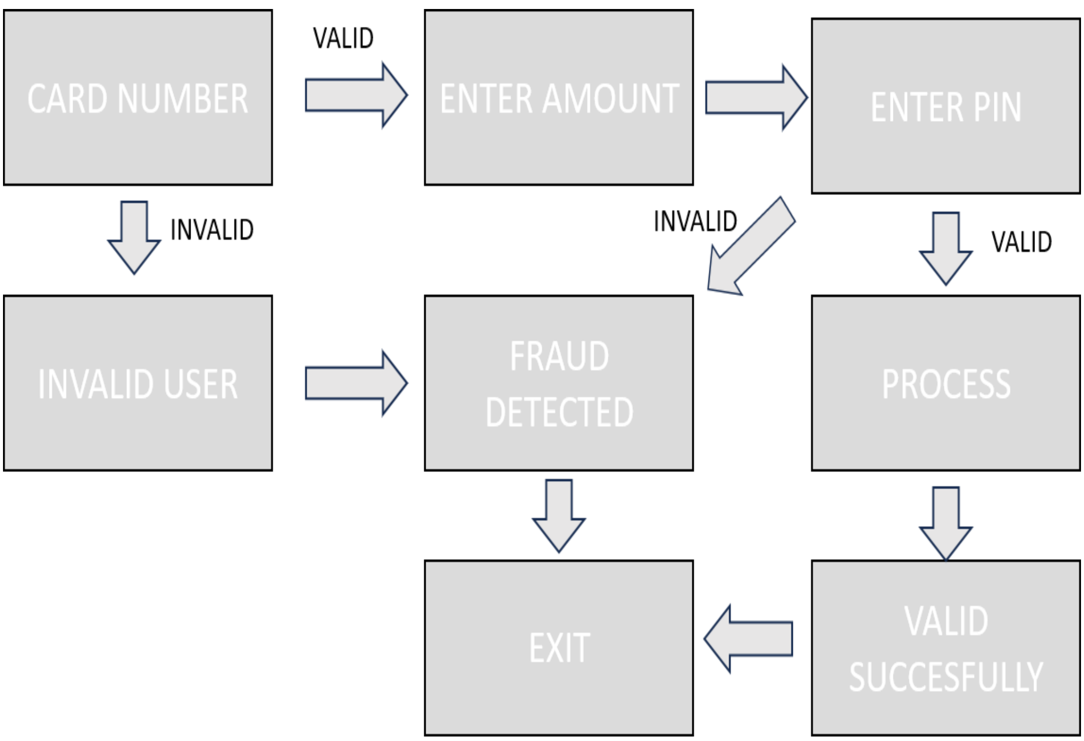
2.1.3More Detailed Alerts:

- Integrate a logging system to store the time and nature of failed attempts.
- Optionally, add more comprehensive alerts, such as sending email notifications upon multiple incorrect attempts or successful fraud detection.

2.1.4 Testing:

- Thorough testing should be conducted to ensure that the program correctly handles all user input cases and edge cases like invalid inputs, maximum attempts, etc.

2.2 Block Diagram



CHAPTER 3
MODULE DESCRIPTION

3.1 Module 1 - Card Number and PIN Validation Module

This module checks if the entered card number and PIN exist in the predefined lists. If they match, access is granted; otherwise, incorrect attempts are logged.

3.2 Module 2 - Fraud Detection Module

This module tracks the number of incorrect login attempts and triggers a fraud alert once the user exceeds the maximum allowed attempts.

3.3 Module 3 - User Interface Module

This module provides a graphical interface for users to input their card number and PIN. It also displays success messages and fraud alerts through dialog boxes.

3.4Module 4 - Alert System Module

The alert system uses dialog boxes to notify users of successful login or fraud suspicion, accompanied by appropriate messages and sounds.

CHAPTER 4

CONCLUSION & FUTURE SCOPE

4.1 CONCLUSION

The **Credit Card Fraud Detection** program effectively addresses the need for security and fraud prevention in credit card transactions. Using basic **AWT components**, the program validates user inputs, checks against a predefined list of valid card numbers and PINs, and triggers alerts for successful or fraudulent activities. The system ensures a user-friendly interface, and the implementation of fraud detection through incorrect attempt tracking enhances security. Future enhancements could include integrating machine learning or more complex fraud detection algorithms to improve accuracy and minimize false positives.

4.2 FUTURE SCOPE

The future scope of this Credit Card Fraud Detection system can be significantly expanded by incorporating advanced machine learning techniques for real-time fraud detection. By analyzing transaction patterns, geolocation data, and user behavior, the system could identify anomalies and flag potential fraudulent activities. Integrating artificial intelligence would enable predictive analysis, allowing the system to detect fraud even before a transaction is completed. Additionally, multi-factor authentication methods like biometric verification (fingerprint or facial recognition) and OTP-based confirmations could enhance security and make the system more robust.Furthermore, the system can be scaled for enterprise use by enabling integration with secure APIs for encrypted communication with banking systems. Cloud-based deployment would ensure high availability and scalability, allowing it to handle millions of users concurrently.

The inclusion of blockchain technology could provide a transparent and tamper-proof mechanism for transaction validation. With continuous updates and compliance with evolving regulations, the system could become an essential tool for mitigating financial fraud in an increasingly digital world.

APPENDIX A

```
    import java.awt.*;
    import java.awt.event.*;

    public class CreditCardFraudDetection extends Frame implements
ActionListener {
        private TextField cardNumberField, pinField;
        private Label resultLabel;
        private Button validateButton;

        // Predefined valid card numbers and PINs for 10 users
        private final String[] validCardNumbers = {
            "12345678", "23456789", "34567890", "45678901", "56789012",
            "67890123", "78901234", "89012345", "90123456", "01234567"
        };

        private final String[] validPins = {
            "1234", "2345", "3456", "4567", "5678",
            "6789", "7890", "8901", "9012", "0123"
        };

        private int incorrectAttempts = 0; // Count of incorrect attempts
        private final int maxAttempts = 3; // Maximum number of allowed attempts

        public CreditCardFraudDetection() {
```

```
        // Set up the Frame
        setTitle("Credit Card Fraud Detection");
        setSize(400, 300);
        setLayout(new FlowLayout());
        setResizable(false);

        // Card Number and PIN Input Fields
        Label cardNumberLabel = new Label("Card Number (8 digits):");
        cardNumberField = new TextField(20);
        add(cardNumberLabel);
        add(cardNumberField);

        Label pinLabel = new Label("PIN (4 digits):");
        pinField = new TextField(20);
        pinField.setEchoChar('*'); // Mask the PIN input
        add(pinLabel);
        add(pinField);

        // Validate Button
        validateButton = new Button("Validate");
        validateButton.addActionListener(this);
        add(validateButton);

        // Result Label
        resultLabel = new Label("Enter card number and PIN, then click
'Validate'");
        add(resultLabel);

        // Close Window
```

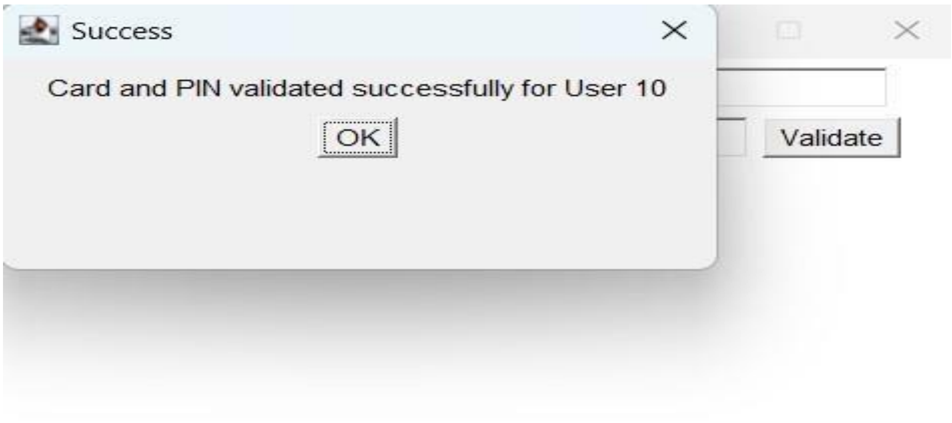
```
    addWindowListener(new WindowAdapter() {
        public void windowClosing(WindowEvent e) {
            System.exit(0);
        }
    });

    setVisible(true);
}

@Override
public void actionPerformed(ActionEvent e) {
    if (e.getSource() == validateButton) {
        String cardNumber = cardNumberField.getText();
        String pin = pinField.getText();

        // Validate card number and PIN length
        if (cardNumber.length() != 8) {
            resultLabel.setText("Card number must be 8 digits!");
            return;
        }
        if (pin.length() != 4) {
            resultLabel.setText("PIN must be 4 digits!");
            return;
        }

        boolean valid = false;

        // Iterate through all the valid card numbers and PINs
        for (int i = 0; i < 10; i++) {
```

```
                        if (cardNumber.equals(validCardNumbers[i]) &&
pin.equals(validPins[i])) {
                            valid = true;
                            resultLabel.setText("Access Granted for User " + (i + 1) + "!");
                            incorrectAttempts = 0; // Reset the incorrect attempts counter on
success
                            showAlert("Success", "Card and PIN validated successfully for
User " + (i + 1), false);
                            break;
                        }
                    }

                    if (!valid) {
                        incorrectAttempts++;
                        resultLabel.setText("Invalid details. Attempt " + incorrectAttempts +
"/" + maxAttempts);

                        // If incorrect attempts reach the limit, show fraud alert
                        if (incorrectAttempts >= maxAttempts) {
                            showAlert("Fraud Alert", "Multiple incorrect attempts detected!
Fraud suspected.", true);
                        }
                    }
                }
            }

            // Method to show alerts (success or fraud)
            private void showAlert(String title, String message, boolean isFraudAlert) {
                Dialog alertDialog = new Dialog(this, title, true);
```

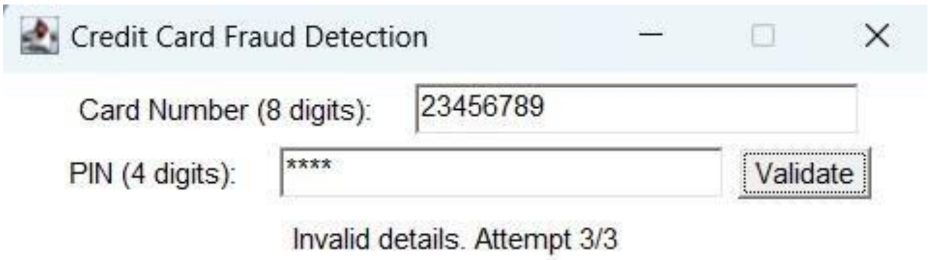
```
        alertDialog.setLayout(new FlowLayout());
        alertDialog.setSize(300, 150);

        Label alertLabel = new Label(message, Label.CENTER);
        alertDialog.add(alertLabel);

        Button okButton = new Button("OK");
        okButton.addActionListener(e -> alertDialog.setVisible(false));
        alertDialog.add(okButton);

        if (isFraudAlert) {
            Toolkit.getDefaultToolkit().beep(); // Beep sound for fraud alert
        }

        alertDialog.setVisible(true);
    }

    public static void main(String[] args) {
        new CreditCardFraudDetection(); // Run the program
    }
}
```

APPENDIX B

(SCREENSHOTS)



Card and PIN validated successfully for User 10



Card Number (8 digits): 23456789

PIN (4 digits): ****

Invalid details. Attempt 3/3

REFERENCES

- "Real-Time Credit Card Fraud Detection System Using Machine Learning" by D. M. Shobha and M. S. P. Manoharan (2019).

- "Credit Card Fraud Detection using Deep Learning Techniques" by R. T. V. S. Goud and K. N. D. B. V. Prasad (2020).

- "A Hybrid Model for Credit Card Fraud Detection Using Machine Learning Techniques" by H. A. Yaseen et al. (2019).