

# **CRIME DETECTION IN CREDIT CARD FRAUD**

**A PROJECT REPORT**

*Submitted by*

**PADMAPRIYA S 230381172432280**

*in partial fulfillment of requirements for the award of the course*

**CGB1201 – JAVA PROGRAMMING**

*in*

**ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**

**K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY**

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

**SAMAYAPURAM – 621 112**

**DECEMBER, 2024i**

**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 **PADMAPRIYA S 2303811724322080** who carried out the project work during the academic year 2024 - 2025 under my supervision.



**Signature**

Dr. T. AVUDAIAPPAN M.E., Ph.D.,

**HEAD OF THE DEPARTMENT,**

Department of Artificial Intelligence,  
K. Ramakrishnan College of Engineering,  
Samayapuram, Trichy -621 112.



**Signature**

Mrs. S. GEETHA M.E.,

**SUPERVISOR,**

Department of Artificial Intelligence,  
K. Ramakrishnan College of Engineering,  
Samayapuram, Trichy -621 112.

S

Submitted for the viva-voce examination held on 3.12.24



**INTERNAL EXAMINER**

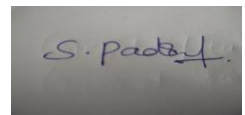


**EXTERNAL EXAMINER**

## **DECLARATION**

I declare that the project report on “**CRIME DETECTION IN CREDIT CARD FRAUD**” is the result of original work done by me and best of my knowledge, similar work has not been submitted to “**ANNA UNIVERSITY CHENNAI**” for the requirement of Degree of **BACHELOR OF TECHNOLOGY**. This project report is submitted on the partial fulfillment of the requirement of the award of the **CGB1201 – JAVA PROGRAMMING**.

**Signature**

A rectangular box containing a handwritten signature in blue ink. The signature appears to be 'S. Padma Priya'.

**PADMA PRIYA S**

**Place:** Samayapuram

**Date:** 3/12/2024

## ACKNOWLEDGEMENT

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

I extend our sincere acknowledgement and appreciation to the esteemed and honourable Chairman, **Dr. K. RAMAKRISHNAN, B.E.**, for having provided 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 our project and offering an adequate duration to complete it.

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

I thank **Dr.T.AVUDAIAPPAN, M.E.,Ph.D.**, Head of the Department of **ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**, for providing her encouragement in pursuing this project.

I wish to convey our profound and heartfelt gratitude to our esteemed project guide **Mrs.S.GEETHA M.E.**, Department of **ARTIFICIAL INTELLIGENCE AND DATA SCIENCE**, for her incalculable suggestions, creativity, assistance and patience, which motivated us to carry out this project.

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

## **VISION AND MISSION OF THE DEPARTMENT**

To excel in education, innovation and research in Artificial Intelligence and Data Science to fulfill industrial demands and societal expectations.

Mission 1: To educate future engineers with solid fundamentals, continually improving teaching methods using modern tools.

Mission 2: To collaborate with industry and offer top-notch facilities in a conducive learning environment.

Mission 3: To foster skilled engineers and ethical innovation in AI and Data Science for global recognition and impactful research.

Mission 4: To tackle the societal challenge of producing capable professionals by instilling employability skills and human values.

## **PROGRAM EDUCATIONAL OBJECTIVES (PEOS)**

**PEO 1:** Compete on a global scale for a professional career in Artificial Intelligence and Data Science.

**PEO 2:** Provide industry-specific solutions for the society with effective communication and ethics.

**PEO 3:** Hone their professional skills through research and lifelong learning initiatives.

### **PROGRAM OUTCOMES**

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.

### **PROGRAM SPECIFIC OUTCOMES (PSOs)**

- **PSO 1:** Capable of working on data-related methodologies and providing industry-focussed solutions.
- **PSO2:** Capable of analysing and providing a solution to a given real-world problem by designing an effective program.

## **ABSTRACT**

In the digital era, credit card fraud has become increasingly sophisticated, posing substantial challenges to financial institutions and customers. This study presents an innovative approach to crime detection in credit card transactions, focusing on real-time fraud prevention. The proposed system integrates multiple data sources and employs a combination of rule-based filters and machine learning models to detect anomalies and unusual patterns indicative of fraud. By analyzing transaction history, user behavior, and contextual data, the system dynamically adapts to evolving fraud tactics.



## TABLE OF CONTENTS

<b>CHAPTER No.</b>	<b>TITLE</b>	<b>PAGE No.</b>
	<b>ABSTRACT</b>	<b>viii</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	1.1 INTRODUCTION	1
	1.2 OBJECTIVE	1
<b>2</b>	<b>PROJECT METHODOLOGY</b>	<b>2</b>
	2.1 PROPOSED WORK	2
	2.2 BLOCK DIAGRAM	3
<b>3</b>	<b>JAVA PROGRAMMING CONCEPTS</b>	<b>4</b>
	3.1 CONTROL STATEMENT	4
	3.2 OOPS CONCEPT	4
<b>4</b>	<b>MODULE DESCRIPTION</b>	<b>5</b>
	4.1 TRANSACTION MODULE	5
	4.2 FRAUD DETECTION SYSTEM	5
	4.3 MAIN MODULE	5
	4.4 JAVA STANDARD LIBRARY MODULE	6
<b>5</b>	<b>CONCLUSION</b>	<b>7</b>
	<b>REFERENCES</b>	<b>8</b>
	<b>APPENDICES</b>	<b>9</b>
	Appendix A – Source code	<b>9</b>
	Appendix B – Screen shots	<b>12</b>

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 INTRODUCTION**

The objective of this project is to develop a robust and efficient fraud detection system for credit card transactions that can identify and flag potentially suspicious activities in real time. By implementing predefined rules, such as monitoring high transaction amounts and high-risk locations, the system aims to enhance transaction security while minimizing false positives. The solution ensures genuine transactions are processed seamlessly, providing a reliable mechanism to prevent financial fraud and safeguard user accounts. Additionally, the modular design allows for easy integration of advanced detection methods, such as machine learning, to adapt to evolving fraud patterns in the future.

### **1.2 OBJECTIVE**

This project focuses on building a credit card fraud detection system that efficiently processes transactions and flags suspicious activities to prevent financial fraud. The system employs a rule-based approach to identify anomalies, such as unusually large transaction amounts or transactions originating from high-risk locations. It consists of modular components: a transaction class to represent transaction details, a fraud detection system to implement fraud detection logic, and a main module to simulate the end-to-end process. The program ensures genuine transactions are approved while suspicious ones are flagged for further review. Designed with scalability and adaptability in mind, the project lays the groundwork for future enhancements, such as integrating real-time data streaming or machine learning algorithms for improved fraud detection accuracy.

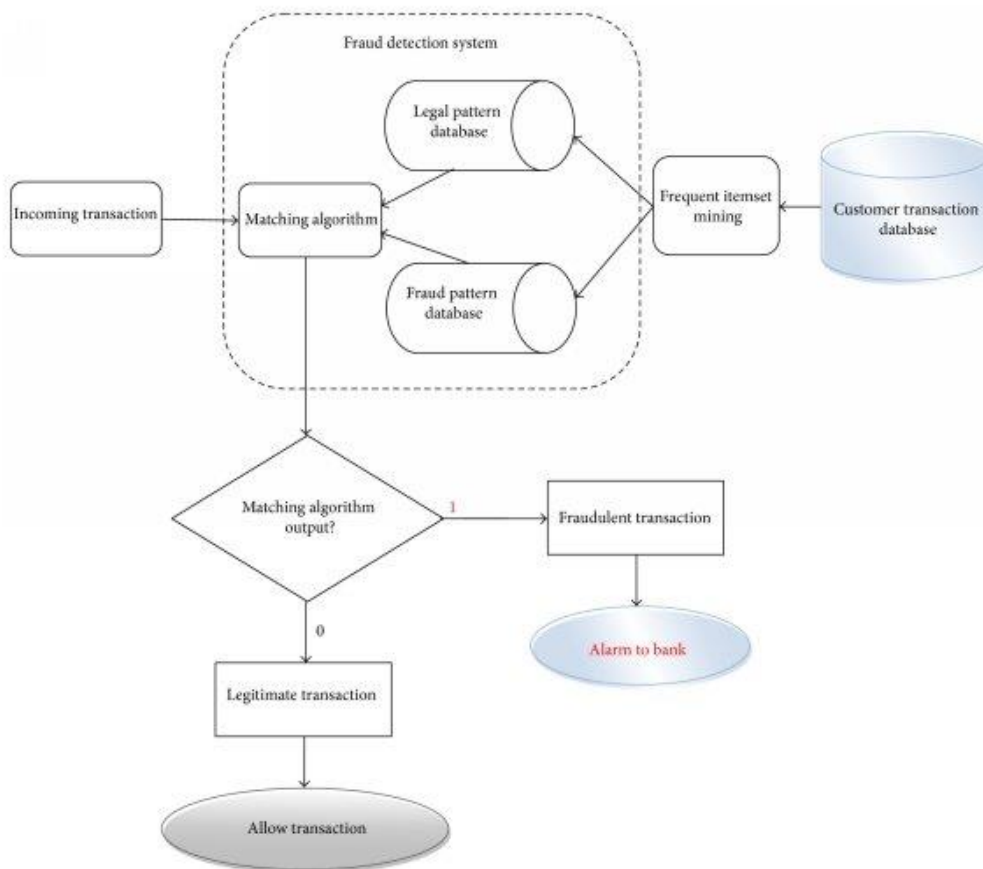
## **CHAPTER 2**

### **PROJECT METHODOLOGY**

#### **2.1 PROPOSED WORK**

The proposed work for this project involves designing and implementing a credit card fraud detection system capable of real-time analysis of transactions to identify and flag potential fraudulent activities. The system will use a rule-based approach as its foundation, evaluating transaction attributes such as amount, location, and timing to detect anomalies. To enhance accuracy, additional rules and validation checks will be incorporated. The system will also include a modular architecture, allowing for future integration of machine learning models for dynamic fraud pattern detection.

## 2.2 BLOCK DIAGRAM



# **CHAPTER 3**

## **JAVA PROGRAMMING CONCEPTS**

### **3.1 OOPS CONCEPTS**

1.Encapsulation 2.Abstraction 3.Modularity

### **3.2 JAVA BASICS**

1.Classes and Objects 2.Methods 3.Variables and Data types

### **CONTROL STATEMENT**

1.If 2.For loop

### **COLLECTION FRAMEWORK**

1.Arraylist

2.List

### **STRING MANIPULATION**

1.String comparison 2.String Formatting

### **BASIC ERROR HANDLING**

### **REAL TME SIMULATION**

### **MAIN METHOD**

## **CHAPTER 4**

### **MODULE DESCRIPTION**

#### **4.1 TRANSACTION MODULE**

Represents individual credit card transactions and their details.

Attributes include:

transactionId - Unique identifier for the transaction.

creditCardNumber - The credit card used for the transaction.

amount - The monetary value of the transaction.

location - Location where the transaction occurred.

timestamp - The time of the transaction.

#### **4.2 FRAUD DETECTION SYSTEM MODULE**

Implements the logic for detecting and flagging suspicious transactions.

**Flagged Transactions List:** Maintains a list of suspicious transactions (flaggedTransactions).

**Rules for Fraud Detection:**

**Rule 1:** Flags transactions exceeding a threshold amount (> \$5000).

**Rule 2:** Flags transactions from high-risk locations (e.g., "High-Risk Country").

Additional rules can be added as needed.

#### **4.3 MAIN MODULE**

Acts as the entry point of the program and simulates the fraud detection process.

**Key Features:**

Creates an instance of FraudDetectionSystem.

Simulates sample transactions by creating Transaction objects.

Processes transactions using the FraudDetectionSystem.

Outputs approved transactions and flagged suspicious transactions.

#### **4.4 JAVA STANDARD LIBRARY MODULE USED**

##### **java.util.ArrayList and java.util.List:**

Used to store and manage the list of flagged transactions dynamically.

##### **java.lang.String:**

Used for string manipulation (e.g., comparing transaction locations).

##### **System.out.println:**

Used for console output, displaying transaction statuses and flagged alerts.

## **CHAPTER 5**

### **CONCLUSION**

In conclusion, the developed fraud detection system provides an effective solution for identifying and preventing fraudulent credit card transactions by applying predefined rules and logic to assess transaction risk. The system ensures minimal disruption to legitimate transactions while accurately flagging suspicious activities for further investigation. Although the current approach is rule-based, incorporating advanced machine learning techniques and real-time transaction processing could further improve detection accuracy and scalability. Overall, this system lays the foundation for a robust, reliable tool in combating credit card fraud, with potential for further optimization and integration into larger financial networks.



## REFERENCES:

1. Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. *Statistical Science*, 17(3), 235-255.
2. Bhattacharyya, S., et al. (2011). Data Mining for Credit Card Fraud Detection: A Comparative Study. *Decision Support Systems*, 50(3), 602-613.
3. Fraud Prevention Resources (Federal Trade Commission):  
Guidelines for financial institutions to prevent and detect fraud. FTC Fraud Resources.
4. Apache Kafka: Real-time stream processing framework. Available at: [Apache Kafka](#).
5. Mastercard's AI-powered fraud detection solutions. [Mastercard AI Fraud Detection](#)

## **APPENDICES**

### **APPENDIX A – SOURCE CODE**

```
import java.awt.*;
import java.awt.event.*;
public class CreditCardFraud extends Frame implements ActionListener {
    Label lblCardNumber, lblAmount, lblMerchant, lblResult;
    TextField txtCardNumber, txtAmount, txtMerchant;
    Button btnCheckFraud;
    public CreditCardFraud() {
        setTitle("Crime Detection in Credit Card Fraud");
        setSize(400, 300);
        setLayout(null);
        setVisible(true);
        lblCardNumber = new Label("Card Number:");
        lblCardNumber.setBounds(50, 50, 100, 20);
        add(lblCardNumber);
        lblAmount = new Label("Amount:");
        lblAmount.setBounds(50, 80, 100, 20);
        add(lblAmount);
        lblMerchant = new Label("Merchant:");
        lblMerchant.setBounds(50, 110, 100, 20);
        add(lblMerchant);
        lblResult = new Label("");
        lblResult.setBounds(50, 200, 300, 20);
        lblResult.setForeground(Color.RED);
        add(lblResult);
        txtCardNumber = new TextField();
        txtCardNumber.setBounds(160, 50, 150, 20);
```

```

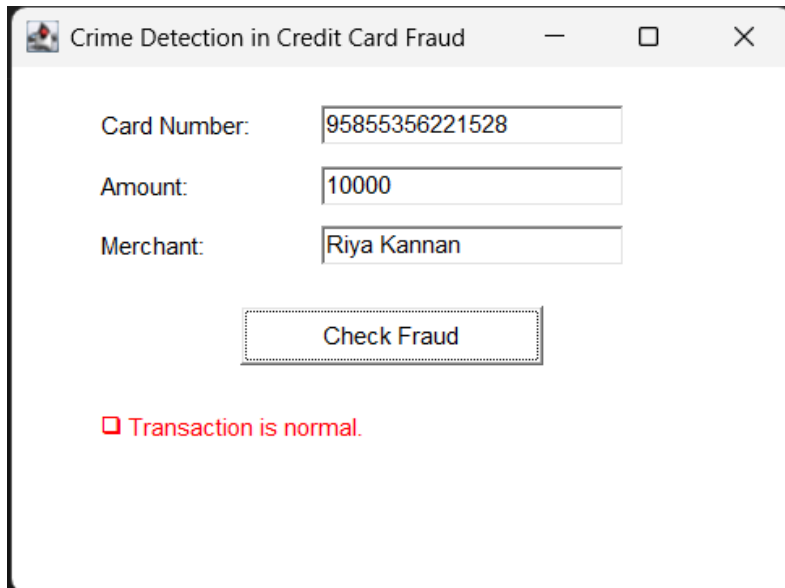
add(txtCardNumber);
txtAmount = new TextField();
txtAmount.setBounds(160, 80, 150, 20);
add(txtAmount);
txtMerchant = new TextField();
txtMerchant.setBounds(160, 110, 150, 20);
add(txtMerchant);
btnCheckFraud = new Button("Check Fraud");
btnCheckFraud.setBounds(120, 150, 150, 30);
btnCheckFraud.addActionListener(this);
add(btnCheckFraud);
addWindowListener(new WindowAdapter() {
    public void windowClosing(WindowEvent e) {
        dispose();
    }
});
}
@Override
public void actionPerformed(ActionEvent e) {
    if (e.getSource() == btnCheckFraud)
        String cardNumber = txtCardNumber.getText();
        String merchant = txtMerchant.getText();
        String amountText = txtAmount.getText();
        try {
            double amount = Double.parseDouble(amountText);
            if (amount > 10000) {
                lblResult.setText("Fraud Detected: Amount exceeds $10,000!");
            } else {
                lblResult.setText(" Transaction is normal.");
            }
        }
    }
}

```

```
    }  
    } catch (NumberFormatException ex) {  
        lblResult.setText(" Invalid amount entered.");  
    }  
}  
  
public static void main(String[] args) {  
    new CreditCardFraud();  
}  
}
```

## APPENDIX B - SCREENSHOTS

### TRANSACTION IS SAFE

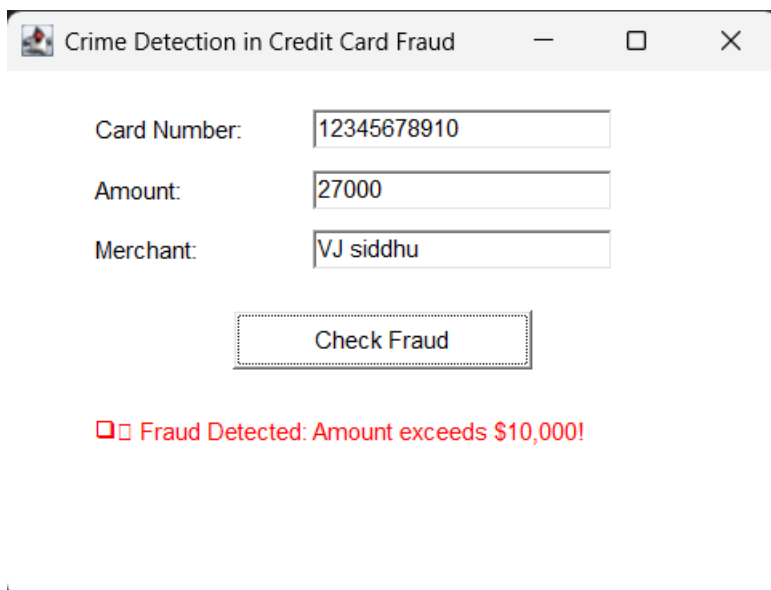


The screenshot shows a window titled "Crime Detection in Credit Card Fraud". It contains three input fields: "Card Number:" with the value "95855356221528", "Amount:" with the value "10000", and "Merchant:" with the value "Riya Kannan". Below these fields is a button labeled "Check Fraud". At the bottom of the window, a red message reads "Transaction is normal.".

Card Number:	95855356221528
Amount:	10000
Merchant:	Riya Kannan

Transaction is normal.

### FRAUD ALERT FOUND



The screenshot shows the same application window as above, but with different input values: "Card Number:" is "12345678910", "Amount:" is "27000", and "Merchant:" is "VJ siddhu". The "Check Fraud" button is still present. At the bottom, a red message reads "Fraud Detected: Amount exceeds \$10,000!".

Card Number:	12345678910
Amount:	27000
Merchant:	VJ siddhu

Fraud Detected: Amount exceeds \$10,000!