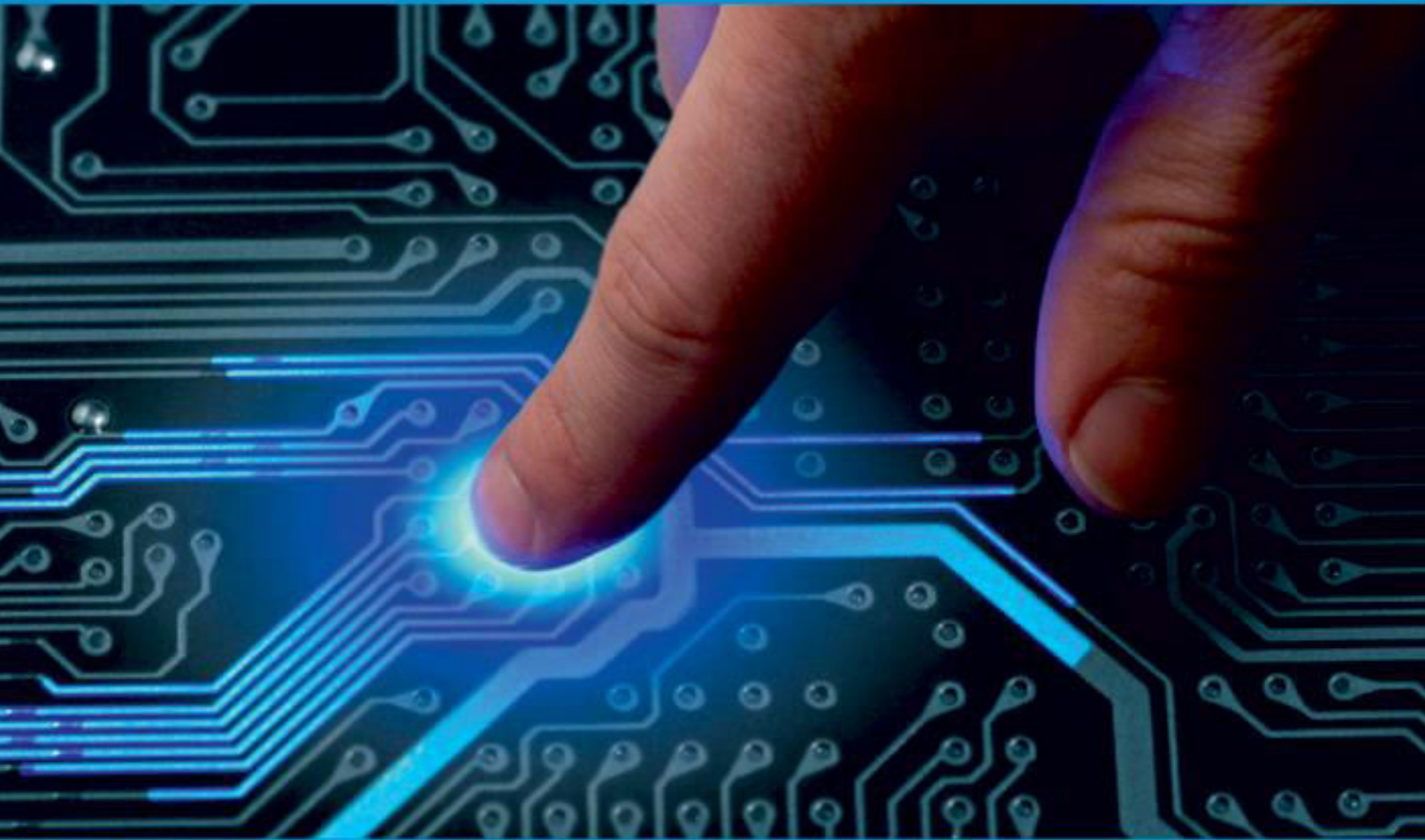




**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.379**

9940 572 462

6381 907 438

ijircce@gmail.com

www.ijircce.com

# Credit Card Fraud Detection System

Monisha R<sup>1</sup>, Pavithra N<sup>2</sup>, Aishwarya K<sup>3</sup>, Sailakshmi N<sup>4</sup>, Rakshitha T<sup>5</sup>

Assistant Professor, Department of Computer Science and Engineering, SJM Institute of Technology, Chitradurga,  
Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, SJM Institute of Technology, Chitradurga,  
Karnataka, India

UG Student, Department of Computer Science and Engineering, SJM Institute of Technology, Chitradurga,  
Karnataka, India

UG Student, Department of Computer Science and Engineering, SJM Institute of Technology, Chitradurga,  
Karnataka, India

UG Student, Department of Computer Science and Engineering, SJM Institute of Technology, Chitradurga,  
Karnataka, India

**ABSTRACT:** In today's economy, credit cards are a crucial factor. It becomes an essential component of domestic, commercial, and international activity. After looking into the challenges of CCFD, we aim to review the most recent methods, datasets, and evaluation standards in this work. The advantages and disadvantages of various fraud detection techniques are listed and contrasted. Additionally, a division of the aforementioned methods into the misuses (supervised) and anomaly detection (unsupervised) categories is provided. Once more, a classification of strategies is suggested based on their capacity to handle datasets that are both numerical and categorical. The most useful and prevalent qualities are then extracted for the various datasets utilised in literature once they have already described and classified into actual and synthetic data. The most useful and prevalent qualities are then retrieved for the various datasets utilised in literature once they have been characterised and classified into actual and synthetic data.

**KEYWORDS:** CCFD – Credit Card Fraud Detection System

## I. INTRODUCTION

This project aims to maintain data leakage protection and ensure merely authorised users may access it. Piracy is now so pervasive online that it represents a serious danger to businesses that produce software. Hackers or intruders can use the system and take the data with the use of harmful software and programmes. Therefore, it becomes necessary to safeguard the data and goods against plagiarism. The development of this project has the identical goal of safeguarding the software's ownership of copyright and facilitating secure transactions.

A lot of study has been done on the CCFD and several strategies, with a focus on neural networks, data mining, and distributed data mining, have been proposed.[1].

## II. RELATED WORK

In [3] The primary objective of this initiative is real-world credit card fraud detection. given that debit cards are now the go-to method of payment for both offline and transactional online, credit card fraud is on the rise. Due to the rising use of credit cards for Online transactions, which has caused a recent rise in credit card scams, e-commerce has expanded dramatically. Credit card datasets are gathered for the training dataset. After that, the user can test the dataset using credit card queries. The provided user's current dataset is classified using a deep neural network technique after a prior dataset is examined. Undoubtedly, a very effective system for detecting credit card scams has been created using techniques like Support Vector Machine (SVM), Deep [4].

III. PROPOSED ALGORITHM

A. Project Description:

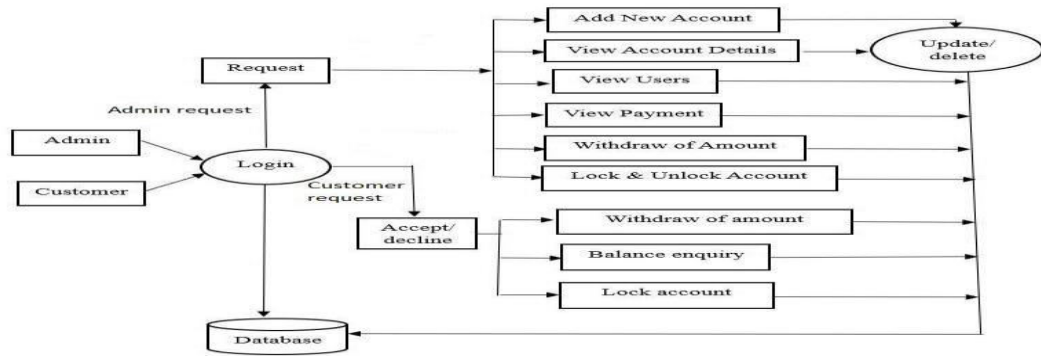


FIGURE1:PROJECT DESCRIPTION

The above diagram shows how the CCFD operates. The website's administrator and user (consumer) both have crucial roles to play. Both parties have login options, and once logged in, the administrator has the following options at their disposal. The administrator can create new accounts, see the users who have already registered, and view any payments that users have completed. The admin has the authority to lock and unlock the account in the event of any unauthorised access to the card. There are several options available to the user, including the ability to withdraw money, check their account balance, and report any unauthorised access.

B. System Architecture:

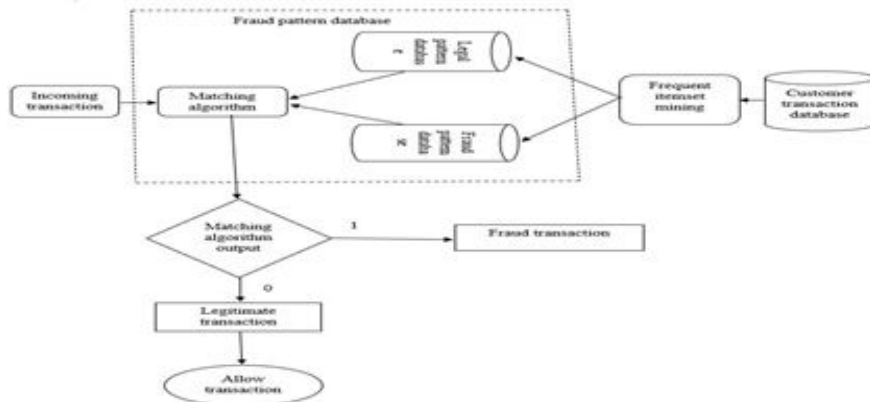


FIGURE 2 : SYSTEM ARCHITECTURE

The above diagram shows the transaction detection process, which enables the system to determine the veracity of the transaction status. When the transaction occurs, the transaction algorithm is being verified; if any threats are detected during the process, the matching algorithm output displays an alert message for the detection of the fraud that had been committed; if no threats are being detected, the system moves forward with the transaction and completes all necessary steps.

C. Admin Module:

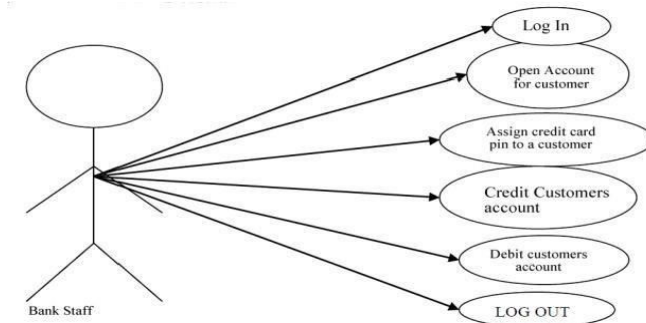


FIGURE 3 : USE-CASE DIAGRAM OF CUSTOMER

The use case diagram for the customers is shown in the diagram above, along with the job that the user is performing. Using his customer id and password, the user can access his account and read the credit card transaction data as well as check the balance of his account. After finishing his task, the user can finally log off of his personal page.

D. Customer Module:

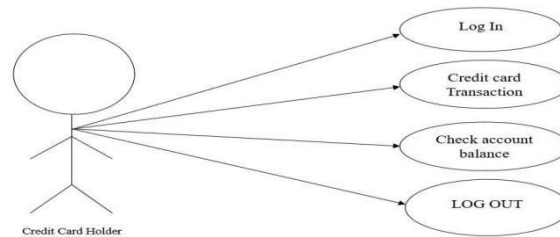


FIGURE 4 :USE-CASE DIAGRAM OF CUSTOMER

The use case diagram for the customers is shown in the diagram above, along with the job that the user is performing. The user can access the credit card transaction information and check the account balance by logging in to his account using his customer id and password. After finishing his task, the user can log off of his own page.

IV. EXPERIMENTAL RESULTS

The suggested system for credit card fraud detection is utilised to identify frauds that take place during credit card transactions as well as any unauthorised use of the card by someone other than the original cardholder. The proposed system below uses machine learning to detect any changes to the original transactions. Once errors are found in the system, the algorithm notices any changes and notifies the admin of any fraud that has been found. The admin then has the authority to halt and hold the transaction that is currently being processed. When any other third party other than the original user uses the credit card, the consumer also receives an alert message.

The results are shown below:

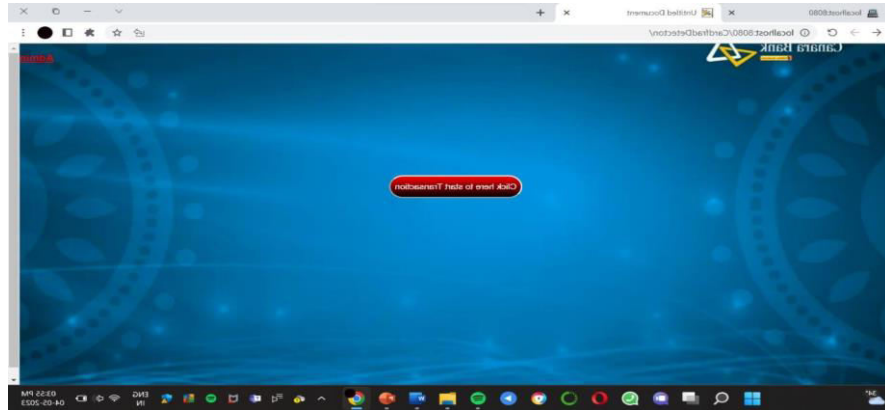


FIGURE 5: Home page of Credit Card Fraud Detection system

The above figure 5 is the home page, where the available credentials are shown.

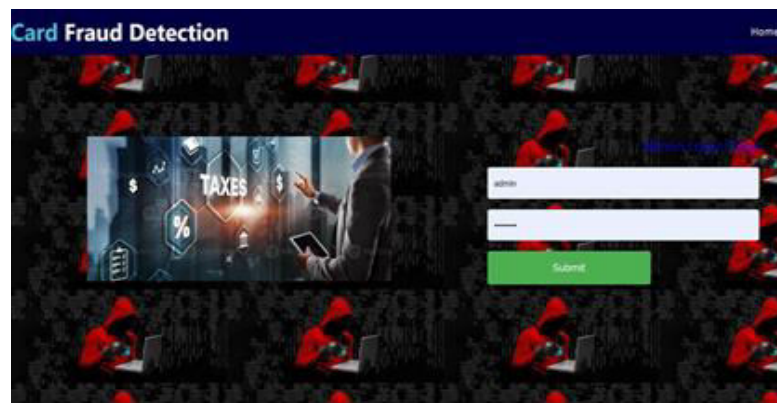


FIGURE 6: Login Credentials of Admin

The above figure 6 is the home page for, login of Admin are shown.



FIGURE 7: Login Credentials of Customer

The above figure 7 is the home page of customer and login credentials are shown.

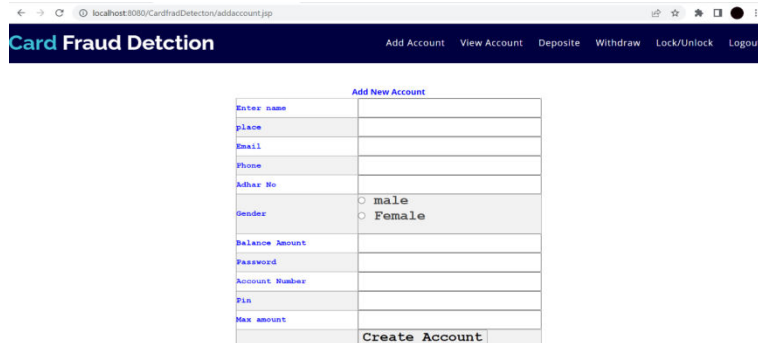


FIGURE 8: Modules of Admin

The above figure 8 is the admin modules, where the sub modules like add account, view account, deposit, lock/unlock options are shown.

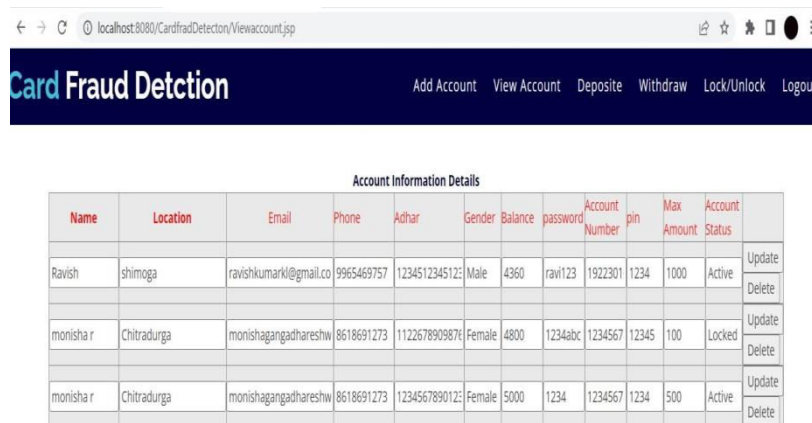


FIGURE9 :Viewing an account details

The above figure 9 is the account information details and transaction history of all the customers are shown.

## V. CONCLUSION AND FUTURE WORK

Nearly all studies on fraud detection that have been published have been surveyed. The adversary, fraud subtypes and types, technical aspects of data, performance indicators, and methods and tactics are all defined. This paper identifies the limitations of fraud detection methods and strategies and demonstrates how other related subjects might help this sector. Future research on fraud detection can benefit from unsupervised methods from counterterrorism work, real-time monitoring systems, text mining from law enforcement, and spam and intrusion detection communities.

## REFERENCES

- [1]. R. J. Bolton and D. J. Hand. Unsupervised profiling methods for fraud detection. In conference of Credit Scoring and Credit Connol VII, Edinburgh. UK, Sept 5-7, 2001.
- [2]. Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, —A review of Fraud Detection Techniques: Credit Card, International Journal of Computer Applications (0975–8887) Volume 45– No .1, May 2012.



- [3]. C. H Sumanth computer Science Engineering Hindustan Institute of technology and science Chennai, India [18113262@student.hindustanuniv.ac](mailto:18113262@student.hindustanuniv.ac). “Analysis of Credit Card Fraud Detection using Machine Learning Techniques”.
- [4]. Vipul Jain department of ISE Siddagangaa institute of Technology Tumkur, India [vipulijain.hp@gmail.com](mailto:vipulijain.hp@gmail.com). “Credit Card Fraud Detection Web Application using Stream lit and Machine Learning”.
- [5]. Helsinki University of Technology, Department of Computer Science and Engineering, 1999.



Impact Factor: 8.379



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details