**CHAPTER ONE**

**INTRODUCTION**

**1.1 Background to the Study**

From the moment payment systems came to existence, there have always been people who will find new ways to access someone ‘s finances illegally. This has become a major problem in the modern era, as all transactions can easily be completed online by only entering your credit card information. Fraud is as old as mankind itself and can take an unlimited variety of different forms. As a result, fraud detection has become an important and urgent task for businesses. Necessary prevention measures can be taken to stop this abuse and the behavior of such fraudulent practices can be studied to minimize it and protect against similar occurrences in the future. The solutions to the fraud can be categorized into prevention and detection are usually operated to prevent fraud. (Shakya, 2018).

When fraud cannot be prevented, it must be recognized as quickly as feasible and appropriate action taken. The action conducted following a fraudulent incident is known as fraud detection. It is the process of determining whether or not a transaction is valid. It entails tracking the behaviors of large groups of people in order to predict, detect, and avert unwanted conduct such as fraud, intrusion, and defaulting. The current era's rapid technical growth has fueled a demand for more innovative payment options. Payment methods such as cheques and cash were previously used. Credit card usage has risen dramatically over the world, and many people now believe in going cashless and rely solely on internet transactions. Thanks to credit cards, digital transactions have become easier and more accessible. A payment card, such as a credit card or debit card, is used to perpetrate fraud, and this practice is referred to as credit card fraud. The goal could be to pay into another account that is under criminal control or to receive goods or services, (Mohammed, 2022).

Credit card fraud can be authorized where a legitimate customer uses their own credit card to make a payment to an account that is managed by a criminal or unauthorized where the account holder does not give consent for the payment to occur and a third party completes the transaction. The compromise can occur in several ways and can usually occur without the knowledge of the cardholder. A compromised account's credentials may be kept by a fraudster for months prior to any theft, making it challenging to pinpoint the point of penetration. Stolen cards can be reported swiftly by cardholders. Unauthorized use might not be discovered by the cardholder until they get a statement. Until the cardholder contacts the issuing bank and the bank places a block on the ./account, the credit card can be used for unauthorized purchases. For early reporting, most banks offer free, 24-hour telephone numbers. Even so, before the card is cancelled, a thief may use the card to make illicit purchases.

**1.2 Problem Statement**

The ease of payment credit cards has brought to the marketing world is immeasurable. Transactions can now be made without any hassle. The world at large is taking advantage of this technology and now, almost all transaction are made with credit cards. This plight has brought about a need for more a secure way to handle these transactions. Fraudsters have been taking advantage of the technology to rob people of their money and they need to be stopped. When a credit card is copied or stolen, the transactions made by them are labeled as fraudulent. These fraudulent transactions should be prevented or detected in a timely manner otherwise the resulting losses can be huge.

**1.3 Aims and Objectives**

The aim of this project is to Designing a system for detecting and preventing credit card fraud. The specific objectives are:

to create a credit card fraud detection system

to enable the credit card fraud detection system to detect fraud in real-time transaction

Anomaly Detection: Develop sophisticated anomaly detection techniques to identify unusual transactions based on factors such as location, transaction amount, time of day, and spending patterns.

to create a fraud alert dashboard and display all the predicted fraudulent transactions.

**1.4 Significance of the Study**

The process of searching for fraud is lengthy due to the amount of data involved. The credit card dataset is classified using the random forest method in the suggested system. An approach for classification and regression is called Random Forest. In a nutshell, it is a group of decision tree classifiers. Random forest has advantage over decision tree as it corrects the habit of over fitting to their training set. A subset of the training set is sampled randomly so that to train each individual tree and then a decision tree is built, each node then splits on a feature selected from a random subset of the full feature set. Even for large data sets with many features and data instances training is extremely fast in random forest and because each tree is trained independently of the others.

**1.5 Scope of the Study**

Several challenges are associated with credit card fraud detection, some of these challenges are: determining which learning strategy to use (e.g., supervised learning or unsupervised learning), which algorithms to use (e.g., Logistic regression, decision trees, etc.), which features to use, how to deal with the class imbalance problem (fraudulent cases are extremely sparse as compared to the legitimate cases). (Shakya, 2018) The profile of fraudulent conduct is dynamic, meaning that fraudulent transactions frequently resemble genuine ones; credit card transaction databases are infrequent and severely biased; selection of features (variables) for the models that is optimal; appropriate metric to assess the effectiveness of strategies on distorted credit card fraud data.

**1.6 Definition of some Operation Terms**

**Credit Card Fraud:** Credit card fraud refers to the unauthorized use of a credit card or its associated information to make fraudulent transactions

**Detection:** Detection is the process of identifying potential instances of credit card fraud within a set of transactions or activities.

**Prevention**: Prevention involves taking proactive measures to stop fraudulent transactions from occurring in the first place.

**Transaction Monitoring**: Transaction monitoring is the continuous real-time or near-real-time analysis of credit card transactions to identify any suspicious or abnormal activities.

**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 Introduction**

Many works have been done related to credit card fraud. In this review, we will synthesize some of the articles to identify works that have already been done. This section discussed machine learning using (supervised methods) such as Logistic Regression, Decision Tree, Random Forest, XGBoost, (unsupervised methods) such as K – Means Clustering, and Autoencoder in Keras. The modeling of a data set using machine learning with Credit Card Fraud Detection. The authors try to detect transactions that are 100% fraudulent as they minimize the incorrect fraud classification. The focus was on analyzing and preprocessing datasets and deploying multiple anomaly detection algorithms like the Local Factor Isolation Forest algorithm on the PCA transformed Credit Card Transaction Data. The results show that the algorithm reaches over 99.6% accuracy, but its precision is about 28% when using a tenth of the data set. Nevertheless, as the entire dataset is inputted into the algorithm, the precision increases to 33%. We expect this rise inaccuracy because of the enormous disparity between valid and genuine transactions. (Awoye'mi, 2012).

The first problem is the constantly changing profiles of standard and fraudulent transactions, and credit card fraud datasets are highly skewed. They further investigate data performance using the naïve Bayes, k-nearest Neighbor, and logistic regression on highly skewed credit card fraud data. 284,807 transactions of the European cardholders were sampled in the research. The researchers applied three techniques to the raw and preprocessed data as the work is implemented in Python. The performance of the methods is assessed based on accuracy, sensitivity, specificity, precision, Matthew’s correlation coefficient, and flat classification rate. The findings show optimal accuracy for naïve Bayes, k-nearest neighbor, and logistic regression classifiers as they indicate 97.92%, 97.69%, and 54.86%, respectively. After comparing the methods, it was evident that the k-nearest Neighbor is better than naïve Bayes and logistic regression techniques. (Mohari, 2021).

Those fallacious activities conducted through credit cards could be tackled with Data Science, Machine Learning together with Deep Learning techniques. One advantage of this is that it helps banks and other financial institutions detect frauds as early as possible before it causes excellent damages. On the other hand, the hackers need a minute amount of data to carry out their malicious acts; this makes the victims vulnerable to danger. There are different techniques and methods of unsupervised learning a graph-based, semi-supervised credit card fraud detection scheme. Globally, it has been recorded those billions of US dollars have been lost to fraudulent activities. To stop these despicable acts, automated Fraud Detection Systems (FDS) can first deny a transaction before it is granted and a graph based FDS called APATE, which uses a limited set of confirmed fraudulent transactions to spread evil influence through a network. They further re-designed APATE to be a perfect fit for to e-commerce field reality. These improvements significantly impact accomplishment as it multiplies precision at 100 by three, both on fraudulent credit cards and transaction prediction. This new technique was tested in real life for three months on e-commerce credit card transactions set of data obtained from a large credit card issuer. Feedback was also introduced here, but it does not significantly improve as the impact can be increased if more cards are examined, where accurate online transaction data of an Internet financial institution in researching credit card fraud detection operation. They studied the performance learning algorithm on original the original data set and the Undersampling using and SMOTE and XGBoost.

**2.2**  **Autoencoders Neural Networks (ANN)**

An Artificial Neural Network (ANN) is an interconnected gathering of processing nodes, for example, "neurons," that together play out an (ordinarily nonlinear) change of contributions to specific ideal outputs. This technique uses a set of neurons connected, and the neurons contribute to the decision-making. ANN uses human thoughts and processing techniques and also capabilities of computers to make predictions for some transactions as fraudulent. It takes it bearing from the previous patterns of operations from the datasets and uses the same design to predict if an existing transaction is fraudulent or not. An autoencoder (an unsupervised machine learning technique that does not need an explicit label to train on) is an extraordinary kind of neural network whose goal is to recreate the contributions instead of anticipating some response variables. (Simon, 2021).

This technique is suitable for detecting an anomaly in a model. Anomaly detection in data mining is how data points or observations digress from a normal distribution of others. It can also be called an outlier detector. During the modeling phase, anomalous data can designate a captious incident such as equipment faults, technical malfunction, or a change in consumer behavior. Autoencoder consists of an input layer, output layer, one or more hidden layers, and activation function and hyperparameters. On account of autoencoders, the output layer has a similar measurement as the input layer. We might want the output to be equivalent to the contribution to reproduce the first input. Henceforth we naturally get our training samples when we set y = x, which is why autoencoders are known as unsupervised learning models. (3) One or more hidden layers, (David, 2011).

**2.3 Common Trends In Credit Card Fraud**

Most card users are fully aware of the imminent danger from fraudsters; this has made the card thieves advance their operation mode to beat the continuously updated security walls. Therefore, this aspect would briefly discuss some prevalent patterns of credit card fraud ahmawati *et al.* (2017).

(a) Stolen/Misplaced card: This method is the most prevalent. It has to do with stealing someone's credit card and using it as their own. Indeed, getting information from the front and back of the card without taking the card away is the same as stealing the card. Banks usually inform customers to notify them through the emergency lines anytime their card is stolen or misplaced. The thief can use the information to purchase goods online, and the bank might not notify the owner until the end of the month Rahmawati et al. (2017).

(b) Synthetic Fraud: A synthetic fraud is an act whereby a fraudster applies for a credit card on behalf of someone. The fraudster acquires essential information of their victim like Social Security Number (SSN), date of birth, address, etc., and applies for a credit card on behalf of the victim Jisha & Vimal (2020).

This method is also known as the "false application method."

(c) Data Breach: Since people carry out some of their transactions through the internet, their data is vulnerable to hackers. The hacker might adopt several ways to get the victim's data Rocha & de Sousa Junior (2010).

They can even completely take over someone's phone or computer after visiting some websites. One of the recommended ways to remedy this situation is to avoid saving important information on any device, or better still, to frequently clear data before getting into the wrong hands.

(d) Mail Interception: Fraudsters can also intercept mails intended to go to the user's address. Probably after applying for a new card, the fraudster can manipulate things to get the card before it gets to the owner. The money would have been gone before the card eventually gets to the owner.

**2.3 Anti-Fraud Systems Fraud System**

so far has been seen as serious economic threat. In the light of the above, several studies had been carried out to combat this menace. Alessandro (2010) proposed a multi-agent’s system called Forecaster’s Intelligent Discussion Experiment System (FIDES). This system integrates the computational power of data mining tools and attack trees with experts' judgments negotiated through a Delphi-based system. Two scenarios are described: in the first one FIDES, supported by cause-effect diagrams, is used to classify alarms generated by the system to help the experts to focus on the dangerous ones; while in the second scenario FIDES is used in a proactive way in order to block or prevent human based frauds. The system combines Think map, Delphi method and Attack trees and it has been built around audit team experts and their needs. The output of FIDES is an attack tree, a tree-based diagram to “systematically categorize the different ways in which a system can be attacked”. Once the attack tree is successfully built, auditors are to choose the path they perceive as more suitable and can then make informed decision as to whether or not to start the investigation.

**2.4 Summary of the Review**

The literature review explores various aspects of credit card fraud detection and prevention systems, focusing on the application of machine learning and deep learning techniques, particularly autoencoders, as well as common trends in credit card fraud. It also discusses anti-fraud systems and their role in combating this economic threat.

Several works have delved into credit card fraud detection using supervised and unsupervised machine learning methods. Supervised techniques such as Logistic Regression, Decision Tree, Random Forest, and XGBoost, as well as unsupervised methods like K-Means Clustering and Autoencoder in Keras, have been employed. These approaches involve the modeling of credit card transaction data to detect fraudulent transactions, aiming to minimize incorrect fraud classifications. The research emphasizes the importance of preprocessing datasets and utilizing anomaly detection algorithms. Results show high accuracy, but precision is influenced by the disparity between genuine and fraudulent transactions (Awoye'mi, 2012). Another study applied naive Bayes, k-nearest Neighbor, and logistic regression on highly skewed credit card fraud data, with optimal accuracy achieved through naive Bayes and k-nearest Neighbor, indicating the potential of these methods in fraud detection (Mohari, 2021).

Overall, the literature review underscores the importance of applying advanced machine learning techniques, like autoencoders, to effectively detect and prevent credit card fraud, as well as the necessity of continuously adapting to emerging fraud trends and employing anti-fraud systems to mitigate risks in financial transactions.

**CHAPTER THREE**

**SYSTEM ANALYSIS AND DESIGN**

**3.1 introduction**

The initial phase of system analysis and design for a Credit Card Fraud Detection System plays a pivotal role in establishing the foundation for a robust and efficient solution. This phase involves comprehensively examining the intricacies of the system's requirements, encompassing the types of transactions under scrutiny, data sources integration, pattern recognition algorithms, real-time monitoring necessities, and security parameters to adhere to stringent industry standards like the Payment Card Industry Data Security Standard (PCI DSS). Concurrently, the system design aspect concentrates on architecting a scalable and responsive framework that can seamlessly ingest and process an extensive influx of transactions, utilizing advanced machine learning and artificial intelligence techniques to dynamically adapt to emerging fraud patterns. The integration of the system with pre-existing financial infrastructures is thoughtfully addressed, ensuring harmonious interaction and data exchange. Moreover, emphasis is placed on the user interface, crafting an intuitive and user-friendly dashboard that empowers operators to efficiently monitor transactions, receive alerts, and execute requisite actions promptly. This comprehensive approach to system analysis and design underlines the pivotal role it plays in fortifying the security, reliability, and overall effectiveness of the Credit Card Fraud Detection System in today's digitally-driven financial landscape. The initial phase of system analysis and design for a Credit Card Fraud Detection System plays a pivotal role in establishing the foundation for a robust and efficient solution.

**3.2 Disadvantages of The Existing System**

These are the disadvantages collectively underscore the need for innovation and enhancement in credit card fraud detection systems

**Limited Adaptability:** Existing systems often rely on rule-based algorithms that struggle to keep pace with rapidly evolving fraud techniques, leading to a time lag in identifying emerging threats and vulnerabilities.

**False Positives:** The reliance on predefined rules can result in a high number of false positives, where legitimate transactions are flagged as suspicious, causing operational inefficiencies and potentially frustrating users.

**Isolated Systems:** Many existing systems operate in isolation, hindering seamless data sharing and collaboration across different departments or organizations, which can impact the effectiveness of fraud detection efforts.

**Delayed Response:** Lack of real-time processing capabilities can lead to delayed fraud detection and response, allowing fraudsters a longer window of opportunity to exploit vulnerabilities.

**Scalability and Performance Issues:** As transaction volumes increase, existing systems might struggle to handle the growing load, leading to performance degradation and potentially compromising the accuracy and speed of fraud detection efforts.

**3.3 Advantages of The Proposed System**

**Advanced Machine Learning Algorithms**: The proposed system leverages cutting-edge machine learning and artificial intelligence algorithms to dynamically adapt to evolving fraud patterns, improving accuracy and reducing false positives.

**Real-time Monitoring:** The system offers real-time transaction monitoring, enabling immediate detection and response to suspicious activities, thereby minimizing the window of opportunity for fraudsters.

**Integrated Data Sources:** By integrating data from various sources, including transaction history, user behavior, and external threat feeds, the system provides a holistic view of user activities, enhancing fraud detection accuracy.

**Seamless Collaboration**: The proposed system promotes collaboration by allowing data sharing and insights across different departments or organizations, enhancing the overall effectiveness of fraud detection efforts.

**Scalability and Performance**: With a scalable architecture designed to handle increasing transaction volumes, the system maintains optimal performance levels even as the workload grows, ensuring efficient fraud detection.

**3.4 The Proposed Method**

The proposed method for the Credit Card Fraud Detection System employs a comprehensive approach that encompasses data preprocessing, feature engineering, machine learning model training, real-time monitoring, dynamic adaptation, and user-friendly interfaces. Raw transaction data is transformed and enriched with relevant features, facilitating the training of a machine learning model that learns patterns of normal behavior and identifies anomalies indicative of fraud. This trained model operates in real-time, continuously assessing incoming transactions, and is designed to dynamically adapt to evolving fraud techniques through continuous feedback and retraining. The system generates alerts for human intervention when suspicious transactions are detected, fostering a collaborative approach to fraud prevention. With a user-friendly interface, the method empowers operators to make informed decisions while maintaining the efficiency of legitimate transactions.

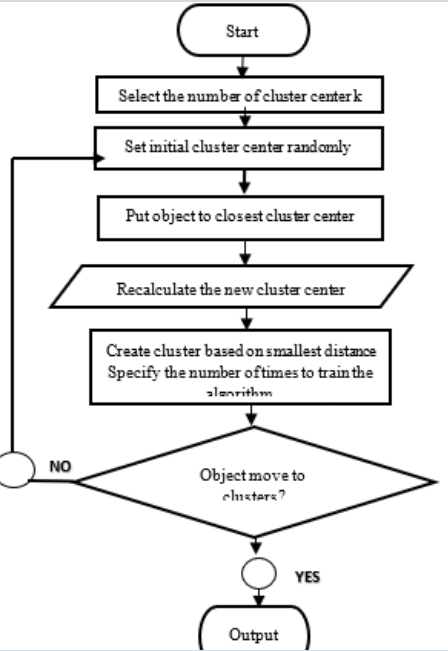
**3.5 Method Of Data Collection**

The proposed method for data collection in the Waterfall model of the Credit Card Fraud Detection System adheres to a sequential and phased approach. The initial phase involves meticulously identifying and acquiring transactional data from diverse sources, such as transaction logs, user profiles, and external threat intelligence feeds. Subsequently, in the analysis phase, the gathered data is cleansed, transformed, and organized into a structured format, ready for subsequent stages. This well-prepared dataset then serves as the foundation for feature extraction, capturing relevant attributes like transaction amounts, frequencies, and user behavior patterns. The method progresses to the design phase, where the structured dataset is integrated into the machine learning model's training process, allowing the system to learn normal transaction behaviors and detect deviations that indicate potential fraud.

**3.6 System Design**

The system design phase in the development of the Credit Card Fraud Detection System involves translating the requirements and analysis findings into a comprehensive blueprint for the system's architecture and components. This phase encompasses both high-level and detailed design aspects, ensuring that the proposed system's functionalities are effectively realized.

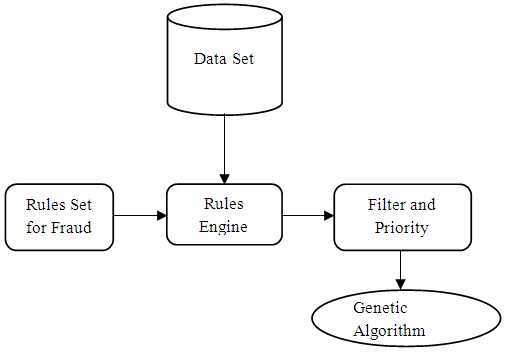
**3.6.1 Algorithm and Diagram**



**Output**

*Fig. 3.1 The Flowchart of the system*

**3.6.2 System Architecture**

****

*Fig. 3.2 The System Architecture of Credit Card Fraud Detecting System*

**3.6.3 Input and Output Design**

**Table 3.1.: Admin Login**

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N0.** | **Field** | **Data Type(Size)** | **Description** |
| 1. | Username | Varchar (20) | The Username of the Admin. |
| 2. | Password | Varchar (20) | The password of the Admin. |

**Table 3.2: Customers Account Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N0.** | **Field** | **Data Type(Size)** | **Description** |
| 1. | Surname | Varchar (15) | The username of the customer |
| 2. | First name | Varchar (15) | The first name of the customer |
| 3. | Type | Varchar (20) | The type of the customer |
| 4. | Phone | Varchar (11) | The phone number of the customer |
| 5. | Email | Varchar (20) | The Email address of the customer |
| 6. | Transdate | Date (8) | The transaction date of the customer |
| 7. | Amount | Float (12.2) | Opening amount of the customer |
| 8. | Account No. | Varchar (20) | The account number of the customer |
| 9. | Address | Varchar (40) | The address of the customer |
| 10. | Nextofname | Varchar (30) | The name of next kin of the customer |
| 11. | Next phone | Varchar (11) | The phone of next kin of the customer |
| 12. | Next address | Varchar (100) | The address of next kin of the customer |
| 13. | Card No. | Varchar (20) | The card number of the customer |

**Table 3.4: User Pin**

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N0.** | **Field** | **Data Type(Size)** | **Description** |
| 1. | Pin | Varchar (12) | The pin number of the customer |
| 2. | Account No | Varchar (12) | The account number of the customer |

**Table 3.5: Transactions**

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N0.** | **Field** | **Data Type(Size)** | **Description** |
| 1. | Sn | Int (4) | The transaction serial number of the customer |
| 2. | AccName | Varchar (20) | The account name of the transaction of the customer |
| 3. | AccNo. | Varchar (20) | The account number of transaction of the customer |
| 4. | DR | Float (12) | The database report transaction of the customer |
| 5. | CR | Float (12) | The credit card report of the customer |
| 6. | Date | Date (8) | The date of the transaction of the customer |
| 7. | Balance | Float (12) | The balance of the transaction of the customer |

**3.7 System Requirement Specification**

**3.7.1 Hardware Requirement**

i. Stable Power Source

ii. 1.44 GHz Processor

iii. Monitor

iv. 1GB RAM

v. Keyboard

vi. Mouse

vii. Printer

**3.7.2 Software Requirement**

i. Operating system: Windows 7, 8.1 and 10

ii. Programming language compiler: PHP and My SQL

iii. Xamp server

iv. MySQL server

v. Apache

vi. Browser

**3.7.3 Personnel Requirement**

i. Computer Literate

**CHAPTER FOUR**

**RESULTS AND DISCUSSION**

**4.1 Introduction**

Designing a system for detecting and preventing credit card fraud is a complex and multifaceted task that requires a combination of technology, data analysis, and security protocols. In this chapter, we will outline the key components and considerations for designing such a system.

**4.2 Results**

**Admin login**

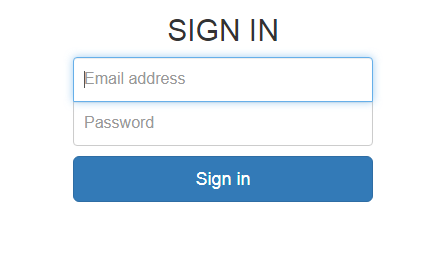
****

Figure 4.1: Admin Login Interface

Figure 4.1 shows the admin interface which provides a secure login portal for system administrators or authorized personnel to access and manage the system. Admins use their unique credentials to log in and gain access to the system's control panel.

**Dashboard**

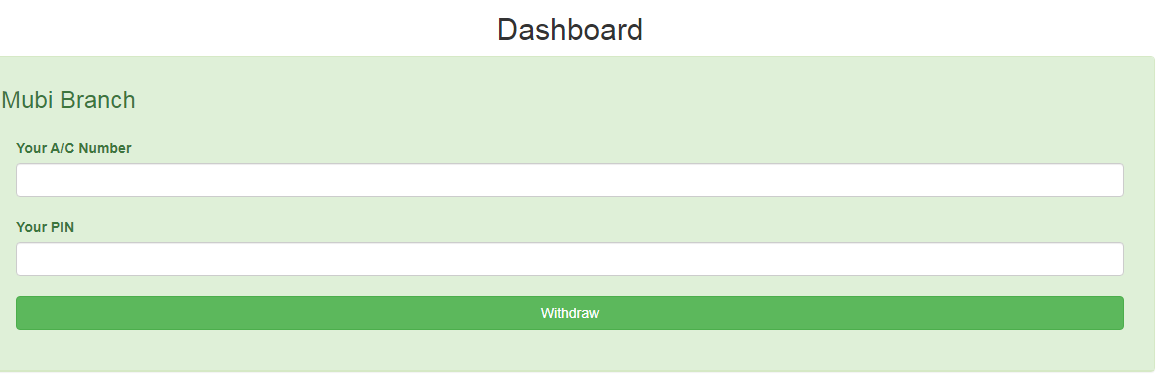


Figure 4.2: Admin Login Interface

Figure 4.2 above shows the dashboard interface which offers an intuitive and visually informative platform for system administrators and authorized personnel to monitor and manage the system effectively.

**Fraud Alert**

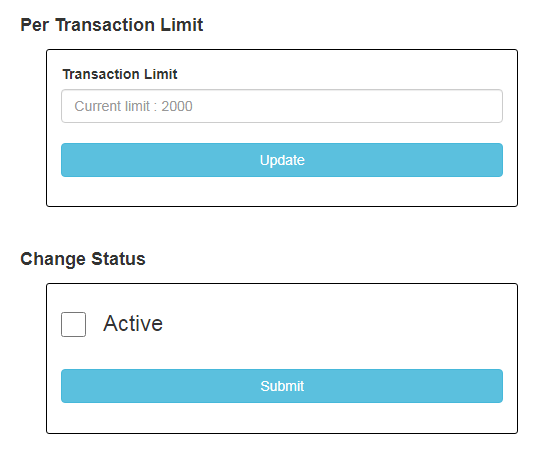


Figure 4.3: Fraud Alert

Figure 4.3 shows the Fraud Alert section which is designed to identify and notify stakeholders about potentially fraudulent activities in real-time.

**Transactions History**

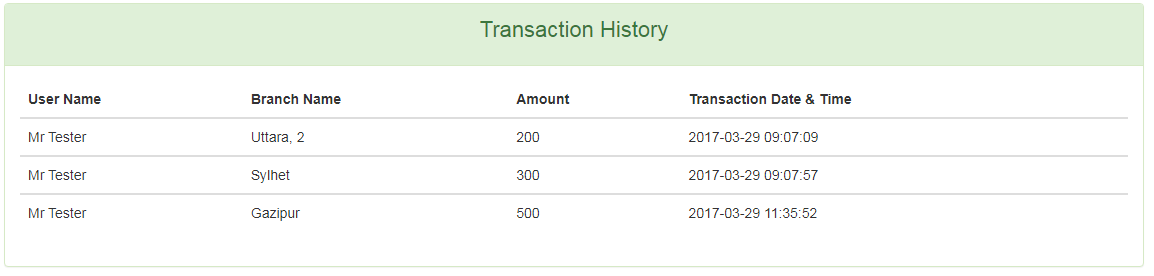


Figure 4.4: Transaction History

Figure 4.4: shows the transaction history, which stores details of each transaction, including legitimate and potentially fraudulent ones.

**Blocking History**

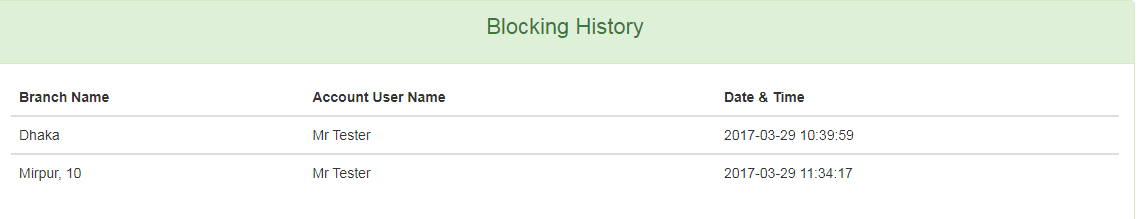


Figure 4.5: Blocking History

Figure 4.5 shows the Blocking History that keeps a record of actions taken to block credit cards due to suspected or confirmed fraud.

**4.3 Discussion**

Figure 4.1 The "Admin Login" section is a crucial part of a Credit Card Fraud Detection and Prevention system. It provides a secure login portal for system administrators or authorized personnel to access and manage the system. Admins use their unique credentials to log in and gain access to the system's control panel. Within this section, administrators can configure system settings, monitor transactions, view alerts, and make critical decisions related to fraud prevention and detection. It serves as the central point of control for the entire system.

Figure 4.2 The dashboard interface in a Credit Card Fraud Detection and Prevention system is a critical component that provides an at-a-glance overview of the system's performance and key metrics. It offers an intuitive and visually informative platform for system administrators and authorized personnel to monitor and manage the system effectively.

Figure 4.3 The "Fraud Alert" section is designed to identify and notify stakeholders about potentially fraudulent activities in real-time. When the system's algorithms detect suspicious transactions or patterns, they trigger fraud alerts. These alerts can include information about the transaction, such as the amount, location, and time, as well as any unusual user behavior. Alerts are sent to both system administrators and cardholders, allowing them to take immediate action, such as blocking the card or investigating the transaction for potential fraud.

Figure 4.4 The "Transactions History" section maintains a historical record of all credit card transactions processed through the system. It stores details of each transaction, including legitimate and potentially fraudulent ones. This history is valuable for auditing, analyzing trends, and investigating past incidents of fraud. It helps in building a comprehensive database of transaction data, which can be used to improve the accuracy of fraud detection algorithms over time.

Figure 4.5 The "Blocking History" section keeps a record of actions taken to block credit cards due to suspected or confirmed fraud. When a card is blocked or suspended, the system logs the event, including the reason for the block, the date and time, and any actions taken by administrators or cardholders. This historical data helps in tracking and managing cases of fraud and assessing the effectiveness of the prevention measures in place. It can also be useful for legal and investigative purposes when dealing with fraudulent activities.

**4.4 User manual**

Installation/setup

Open your XAMPP/WAMP’sControl Panel and the “Apache” and “MySQL”.

If you are using XAMPP, copy the extracted source code folder and past it into the XAMPP’s “htdocs” directory. And If you are using WAMP, past it into the “www” directory.

Browse the PHPMyAdmin in a browser. i.e. <http://localhost/phpmyadmin>

Create a new database naming “idcard”.

Import the provided SQL file. The file is known as “db\_idcard.sql” located inside the extracted source code folder.

Browse the Id card in a browser. i.e. http://localhost/Credit-Card-Fraud-Detecting-System

**CHAPTER FIVE**

**SUMMARY, CONCLUSION AND RECOMMENDATIONS**

**5.1 Summary**

Summary The main contribution this work offers is the proposition of a generalized strategy to Designing a system for detecting and preventing credit card Fraud Detection System during the fraud detection process, regardless of the dataset or data stream provided. The process begins with the reception of the dataset, which undergoes an initial preprocessing step designed to bolster the model building process. The categorical and non-numerical features in the dataset are encoded into a numerical value, while retaining the original categorical groupings. The dataset undergoes a proposed feature selection algorithm which intends to discover high performing features and bolster the model building process. The pruned dataset is split into train, evaluation, and test subsets through stratified sampling to retain the class distribution. Each subset is transformed through scaling and data imputation, with the information discovered during 63 the scaling of the train subset shared amongst the other subsets. The transformed train and evaluation subsets are used to train and tune the classification models alongside the hyper-parameters to tune. Once the tuning process is completed, the top performing models for each model type are passed along to a final performance evaluation with the test subset. The model that achieves the highest performance for on the test set can then be employed in the Fraud Detection System for credit card fraud detection.

**5.2 Conclusion**

The parties involved in credit card fraud appear to be locked in a constant pursuit to outwit the other as the increased use of credit cards further complicates matters. The financial impact and evolving nature of credit card fraud has continued to motivate financial institutions and researchers to explore methods that go beyond commonly employed methods. While it is not expected that all credit card fraud will completely disappear, efforts to discover methods that help detect it can reduce the number of cases and its impact. This is the motivation for this work: to contribute to the cause through the analysis of the commonly employed methods, exploration of the more modern approaches, and proposition of a generalized strategy. A summary of the work completed and contributions to the topic are described below.

**5.3 Recommendations**

There are additional tasks that go beyond the scope of this work, but can substantially improve on it. As previously mentioned, the generalized strategy proposed for credit card fraud detection aims to function across any given dataset or data stream. Discovering additional datasets for credit card fraud detection can help support and progress the proposed strategy through testing its performance even further. A commonly used strategy to handle unbalanced data is to employ sampling techniques. This work uses stratified sampling when creating the various data subset for training, evaluating, and testing as well as bootstrap sampling to build Random Forest. However, there are many other sampling techniques that may improve the overall performance of the models built. Some proposed alternative sampling techniques to explore include sampling. The implemented machine learning models used in this work consisted of Naive Bayes, Nearest Neighbor, Random Forest, and Neural Network. There are many other models that can be analyzed for their performance for credit card fraud detection on the dataset employed. The generalized strategy proposed can benefit from tuning and deploying additional high-performing 65 models. There are aspects of the tuning process that can be further explored. The range of values for hyper-parameters tuning can be expanded to search a larger space. There are also additional hyperparameters that were not considered in this work that can be explored.

**5.4 Contribution of Knowledge**

**Credit card fraud** is an inclusive term for [fraud](https://en.wikipedia.org/wiki/Fraud) committed using a [payment card](https://en.wikipedia.org/wiki/Payment_card), such as a [credit card](https://en.wikipedia.org/wiki/Credit_card) or [debit card](https://en.wikipedia.org/wiki/Debit_card).[[1]](https://en.wikipedia.org/wiki/Credit_card_fraud#cite_note-1) The purpose may be to obtain goods or services or to make payment to another account, which is controlled by a criminal. The [Payment Card Industry Data Security Standard](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard) (PCI DSS) is the data security standard created to help financial institutions process card payments securely and reduce card fraud.[[2]](https://en.wikipedia.org/wiki/Credit_card_fraud#cite_note-2)

Credit card fraud can be authorized, where the genuine customer themselves processes payment to another account which is controlled by a criminal, or unauthorized, where the account holder does not provide authorization for the payment to proceed and the transaction is carried out by a third party. In 2018, unauthorized financial fraud losses across payment cards and remote banking totaled £844.8 million in the United Kingdom. Whereas banks and card companies prevented £1.66 billion in unauthorized fraud in 2018.

**5.5 Area for Further Study**

The size of most credit cards is 85.60 by 53.98 millimeters (3+3⁄8 in × 2+1⁄8 in) and rounded corners with a radius of 2.88–3.48 millimeters (9⁄80–11⁄80 in). Little, Ken. 2007.  conforming to the [ISO/IEC 7810 ID-1](https://en.wikipedia.org/wiki/ISO/IEC_7810#ID-1) standard, the same size as [ATM cards](https://en.wikipedia.org/wiki/ATM_card) and other [payment cards](https://en.wikipedia.org/wiki/Payment_card), such as [debit cards](https://en.wikipedia.org/wiki/Debit_card).  Robert D. Hershey Jr. (26 April 1998).

Credit cards have a printed Luthi, Ben (7 October 2019). Or embossed [bank card number](https://en.wikipedia.org/wiki/Bank_card_number) complying with the  numbering standard. The card number's *prefix*, called the [Bank Identification Number](https://en.wikipedia.org/wiki/Bank_Identification_Number) (known in the industry as a Jennifer Bayot (22 February 2005).  Is the sequence of digits at the beginning of the number that determine the bank to which a credit card number belongs. This is the first six digits for MasterCard and Visa cards. The next nine digits are the individual account number, and the final digit is a validity [check](https://en.wikipedia.org/wiki/Luhn_algorithm) digit. Cothern, Lance (26 June 2019).

**REFERENCE**

Abdechalin, A., & Traore, I. (2009). Identity Application Fraud Detection using Web Mining and rule-based decision tree. *International Journal of Computer and Network Security,* 1(1), 31-44.

Abhinav, S., Amlan, K., & Shamik, S. (2008). A Revealing Introduction on to Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing, 5(1), 37-48.*

Abhinav, S., Kundu, S., Shamik, S., & Arun, K. (2008). Credit Card Fraud Detection Using Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing*, 5(1). 83-86

Aburrous, M., Hossain, M., Dahal, K., & Thabtah, F. (2010). Intelligent Phishing Detection system for e-banking using fuzzy data mining. *Expert System Application,* 37(12), 7913-7921.

Adebayo, O. G., & Ajinaji, O.T. (2014). Bank Frauds and Forgeries in Nigeria. A study of the causes, Types, Detection and Prevention. *IOSR Journal of Economics and Finance, 4(2), 41-50.*

Adebisi, (2009). Credit Card Fraud Detection Using Hidden Markov Model. *International Journal of Computer Science and Engineering*, 4(2), 57.

Adekanye, F. (2008). Fraud in Banking Transactions. *The Nigerian Bankers, 6(1), 7-15.*

Adewunmi, W. (1999). Fraud in Banks Lagos; Nigerian Institute of Bankers, 26-36.

Adeyemo, K.A., (2012). Frauds in Nigeria Banks. Nature, Deep-Seated causes, Aftermaths and Probable Remedies. *Mediterranean Journal of Social Sciences, 3(2), 279-289.*

Adnan, M., &Khatib, A. (2012). Electronic Payment Fraud Detection Techniques, *World of Computer Science and Information Technology Journal,* 2(4) 137-141.

Ahhinav, S., Amlan, K., Shanlik, S., Run, K. (2008). *IEEE Transactions on Dependable and Secure Computing,* 5(1) 37.

Akoroda, G.C.O. (2004). Frauds and Forgeries. *WAJFEM Regional course on Banking Supervision, Lagos.*

Akshada, K; Chhajed, k.k; & Kapse, A.S. (2017). Review on Fraud Detection in Electronic Payment Gateway. *International Journal of Engineering and Technology*, 4(1), 841- 844.

Alashi, S.O., (1994) Fraud Prevention and Control. Role of Government and its Agents.

*Journal of the institute of Bankers of Nigeria (July-December, 1994) pp11-15.*

Aleskerov, E., Fieisleben, B., & Bharat, R. (1997). CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, *Department of Electrical Engineering and Computer Science, University of Siegen,* 220-226.

Alessandro B (2012): Fraud Detection in the Banking Sector. A Multi-agents Approach*. International conference on management and service & science, 24-26 August, Wuhan, 1-4.*

Alexopoulos, P., & Kafentzis, K. (2007). Towards a Generic Fraud Ontology in E- Government,*ICE-B,* 269-276.

**Appendix A**

<?php

    ob\_start();

    session\_start();

    // Check previous session untill is destroyed

    if (isset($\_SESSION['username'])) {

        // logged in

        header('Location: settings.php');

    }

?>

<!DOCTYPE html>

<html>

<head>

    <meta name="viewport" content="width=device-width, initial-scale=1">

    <title>Login | Credit Card</title>

    <!-- Load all static files -->

    <link rel="stylesheet" type="text/css" href="assets/BS/css/bootstrap.min.css">

    <link rel="stylesheet" type="text/css" href="assets/css/styles.css">

</head>

<body class="container">

    <!-- Config included -->

    <?php include 'helper/config.php' ?>

     <!-- Here will be checking for login -->

     <?php

        if($\_SERVER['REQUEST\_METHOD'] == 'POST') {

            $email = $\_POST['email'];

            $password = $\_POST['password'];

            $get\_login\_sql = "SELECT \* FROM users WHERE email='".$email."' AND password='".$password."'";

            $login\_success = $conn->query($get\_login\_sql);

            if($login\_success->num\_rows == 1){

                // Check the session and add into session

                $\_SESSION['valid'] = true;

                $\_SESSION['timeout'] = time();

                $\_SESSION['username'] = $email;

                // Redirect to settings page

                header('Location: settings.php');

            }else {

                echo '<p class="error-message">Credientials are not correct!!</p>';

            }

        }

     ?>

    <!-- Login view -->

    <form class="form-signin"method="POST" action="">

        <h2 class="form-signin-heading">SIGN IN</h2>

        <label for="inputEmail" class="sr-only">Email address</label>

        <input type="email" id="inputEmail" name="email" class="form-control" placeholder="Email address" required autofocus>

        <label for="inputPassword" class="sr-only">Password</label>

        <input type="password" id="inputPassword" name="password" class="form-control" placeholder="Password" required>

        <button class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>

    </form>

</body>

<footer>

    <!-- All the Javascript will be load here... -->

    <script type="text/javascript" src="assets/JS/jquery-3.1.1.min.js"></script>

    <script type="text/javascript" src="assets/JS/main.js"></script>

    <script type="text/javascript" src="assets/BS/js/bootstrap.min.js"></script>

</footer>

</html>

<!-- Check for a valid transaction -->

<?php

    session\_start();

    if(isset($\_SESSION['account'])) {

        // Do something if anything special you need.

    }else{

        header("Location: index.php");

    }

?>

<!DOCTYPE html>

<html>

<head>

    <meta name="viewport" content="width=device-width, initial-scale=1">

    <title>Credit Card Faurd Detecting System</title>

    <!-- Load all static files -->

    <link rel="stylesheet" type="text/css" href="assets/BS/css/bootstrap.min.css">

    <link rel="stylesheet" type="text/css" href="assets/css/styles.css">

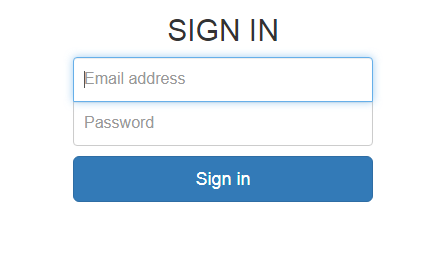
</head>

<body class="container">

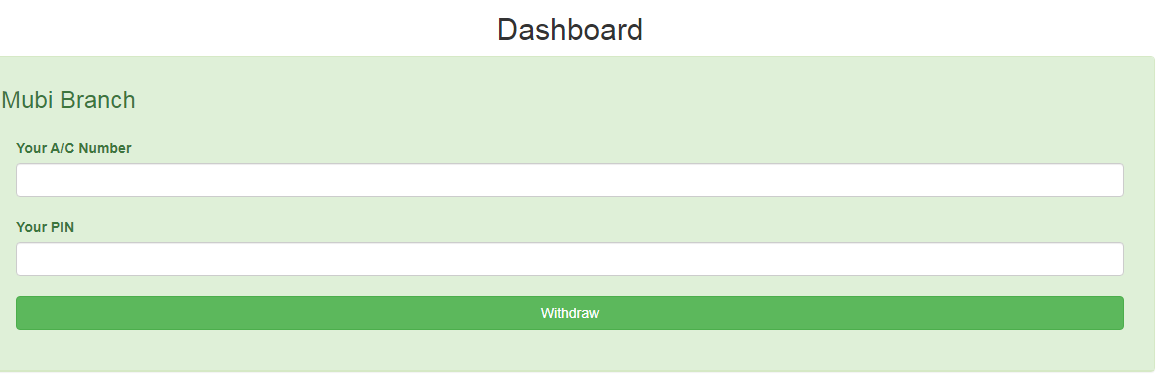
    <!-- Navbar included -->

    <?php include 'helper/navbar.html' ?>

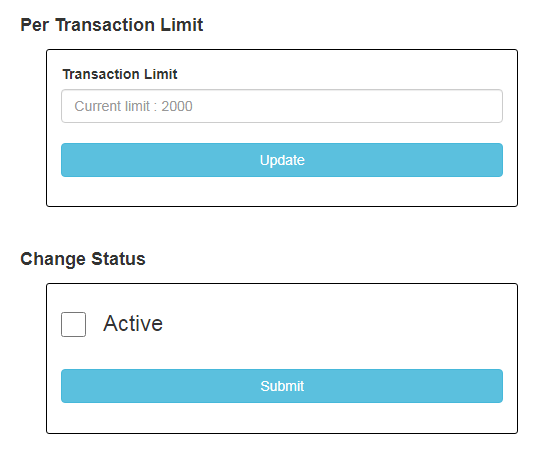
**Appendix B**

****

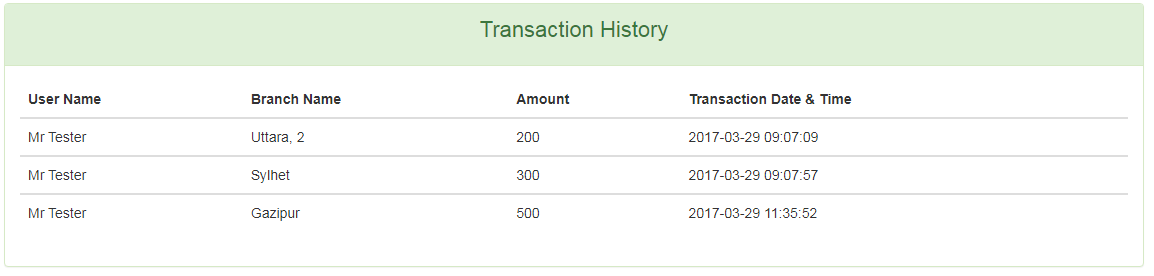
**Admin login**



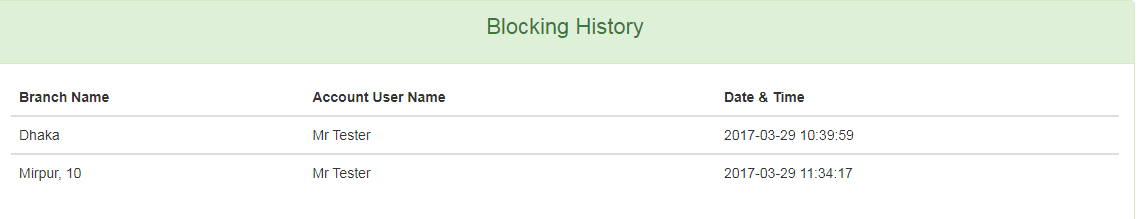
**Fraud Alert**



**Transactions Structure**



**Transactions History**



**Blocking History**