ARTIFICIAL NEURAL NETWORK APPROACH FOR DETECTION OF CREDIT CARD FRAUD USING CUSTOMER BEHAVIOUR.

Peter Buoye & Mudasiru Hammed

adewuyi.buoye@federalpolyilaro.edu.ng;
hammed.mudashiru@federalpolyilaro.edu.ng

Abstract

Credit cards serve as a good substitute for cash because credit cards are made of plastic and it is distributed by financial institutions like banks to make transactions simple and convenient without having to carry cash. Changes in technology, particularly the internet, have made credit card use more prevalent as well as exposed Credit card to unauthorized users. The abuse by fraudsters can be checked by taking the required preventative steps, and it is possible to research the behavior of such fraudulent operations in order to minimize them and prevent recurrence. The user's behavior and location are scanned as part of the credit card fraud detection so as to look for odd patterns. The patterns contain user traits like spending habits and geographic areas to confirm the user's identification. The system needs to be re-verified if any odd patterns are discovered, since people typically display particular behavioral patterns. Old in pattern discovered based on past purchase data of cardholders is analyzed. A set of patterns containing data on the typical purchase and the amount paid can be used to represent each cardholder. This system was designed on artificial neural network (ANN) algorithm, which provides better accuracy close to 100%. It offers greater accuracy compared to unsupervised learning algorithms.

***Keyword**: Algorithm, Artificial neural network, Credit card, financial institution, fraud detection, unsupervised learning.*

Introduction

A credit card gives a convenient method of payment for goods and services to the owner. The card is issued usually by bank or credit union. This bank will provide the cardholder with a line of credit where they can borrow money to pay for purchases or receive a cash advance. It serves as a good substitute for cash because credit cards are made of plastic and it is distributed by financial institutions like banks to make transactions simple and convenient without having to carry cash. Changes in technology, particularly the internet, have made credit card use more prevalent.

In both small and large companies nowadays, credit cards are used almost universally as a mode of payment. Credit card theft happens in all kinds of firms, including banks, the auto and appliance industries. Several strategies have been put forth by various researchers to reduce fraud in credit card transactions. Due to changes in fraudsters' behavior over the past few decades brought on by the acceleration of technological progress, this credit card has recently grown in popularity (Jumoke and Hammed, 2020).

Fraud in Credit card is the unauthorized use of the card by a person who is believed not to be the right owner of the account. The abuse can be stopped by taking the required preventative steps, and it is possible to research the behavior of such fraudulent operations in order to minimize it and prevent recurrence.

The system described in this paper examines credit card data from users to look for various factors, such as user country and typical purchasing patterns. The system detects an unusual pattern in the transaction process based on the user's prior data. Also, the transaction patterns often change their statistical properties over the course of time. (Maniraj and Aditya, 2019)

This unusual pattern is what the system will detect and study by an artificial neural network to identify user activity patterns along with user location scanning to identify fraudulent act.

Challenge in detecting fraud in card usage is the unavailability of standard dataset to evaluate the proposed fraud detection methods, since data are always private. Not this alone, enormous data is processed everyday and the model

built must be fast enough to respond to the scam in time. This is the reason why this system is using artificial neural network.

Related Works

Fraud is the unlawful use of another person's credit card for one's own benefit without the knowledge of the cardholder or the entities in charge of issuing the card.

All classes of credit card fraud detection systems have different methodologies proposed by earlier studies.

(Makki *et. al.*, 2019) Credit card fraud causes huge financial losses, according to research that offers an algorithm to combat the fraud problem. The authors came to the conclusion that the uneven classification of the dataset is the main reason why the results are inaccurate after executing a number of experiments.

(Sara *et. al.*, 2019) experimentally studied the various weaknesses of existing solutions with the aim to tackle the imbalance classification problem. It was concluded, after using the machine learning algorithms to detect fraud, that the existing approaches give rise to large number of false alarms, which are costly to financial institutions.

(Yasin *et. al.*, 2022) explained how credit card fraud can be detected in ecommerce using data mining. Classification algorithms were used to detect suspicious orders and they arrived at 92% success rate. Artificial Neural Network was used as comparative in their methods.

(Veena and Reddy 2022) suggested a system that employed the Random Forest Algorithm (RFA).This method was based on supervised literacy that used decision trees to bracket portions of the dataset.

(Prusti and Rath, 2019) A program was created using machine learning techniques, like Decision Tree, K-Nearest Algorithm, e,t,c, to evaluate the accuracy of fraud detection. The proposed hybrid system gave an accuracy rate of 82.58%,

(Akila and Reddy, 2017) To handle the unevenness dataset and avoid the noise inherent in the transactions, a non-overlapped risk based bagging ensemble (NRBE) model with misrepresentation location architecture was presented. The bagging model eliminates any irregularities and non-essential elements in the dataset. The creation and danger-based basic student group reaches out to the sacking model.

(Vijay *et. al.*, 2019) worked on a project that created a model employing Random Forest approaches for detecting fraud in credit card transactions. The random forest algorithm (RFA) is a supervised machine learning technique that classifies credit card transactions using a decision tree and then calculates performance using a confusion matrix.

(Taha and Malbery, 2020) described that up gradation in e-commerce and communication technology have made credit card usage more popular way of payment and the fraud associated with transactions is also increasing.

(Asha and Kumar, 2021) compare Machine learning algorithms to predict the occurrence of the fraud in credit card. It was concluded that ANN has the highest accuracy of 0.9992 while KNN has 0.9982 and SVM has 0.9349.

(Hammed and Soyemi, 2020) presented a method that addresses every aspect of detecting and reporting credit card fraud. According to this investigation, the technique is 81.6% accurate with a misclassification error of 18.4%, and the system was able to correctly verify all of the injected incursions utilized for testing.

The artificial neural network which is high in accuracy will be quick enough in solving fraud detection in credit card. Furthermore, it is most effective as a solution to credit card fraud.

Methodology

This study presents a model for detecting credit card fraud based on artificial neural networks. The model is expected to be able to assess credit card transactions and determine whether they are honest or dishonest.

Exploration and Gathering of Data

A data-set that was downloaded from www.kaggle.com is used by the system. The transactions conducted by various customers in a bank during the years of 2010 and 2020 make up the dataset. The target class, which determines legality of the transaction, is derived from 30 of the 31 features that make up the feature set.

The dataset was filtered, cleaned, and preprocessed after being read using a Pandas package. Invalid data records were deleted, and valid data values were added in their stead. After that, the dataset was normalized and scaled. The training dataset and the testing dataset were then created from the original dataset. The model was trained using 70% of the complete dataset, and the accuracy of the model was tested using the remaining 30%. The model results to 89% accuracy using ANN.

Overview of the New System Design

Our comprehensive system design will be provided via the system overview. It provides information about the system architecture that was used. Fig.3.1 depicts the suggested system's design. The architecture shows that in order to log in to the system, a user must first register. After doing so, the user must input their username, password, and email address.

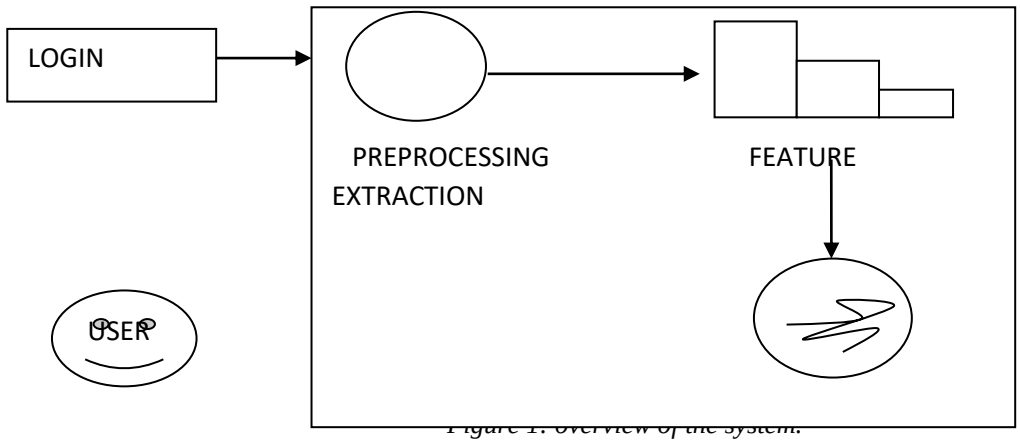

Figure 1: Overview of the system.

Input design The input design is a crucial component of the overall system design that needs to be given extremely careful consideration. The objective of input data design is to make entry as simple, logical, and error-free as possible. The input Form ought to specify the format in which the data fields are to be filled out. Here, data entry is done online using a processor that takes input from the operator via a keyboard in the form of commands and data.

Output design The output analysis guides the format of newly established system, displaying the name and amount and possible responses the computer could produce when it encounters an authorized conclusion.

System flowchart

The system flowchart shows how the system was graphically represented in the new design model

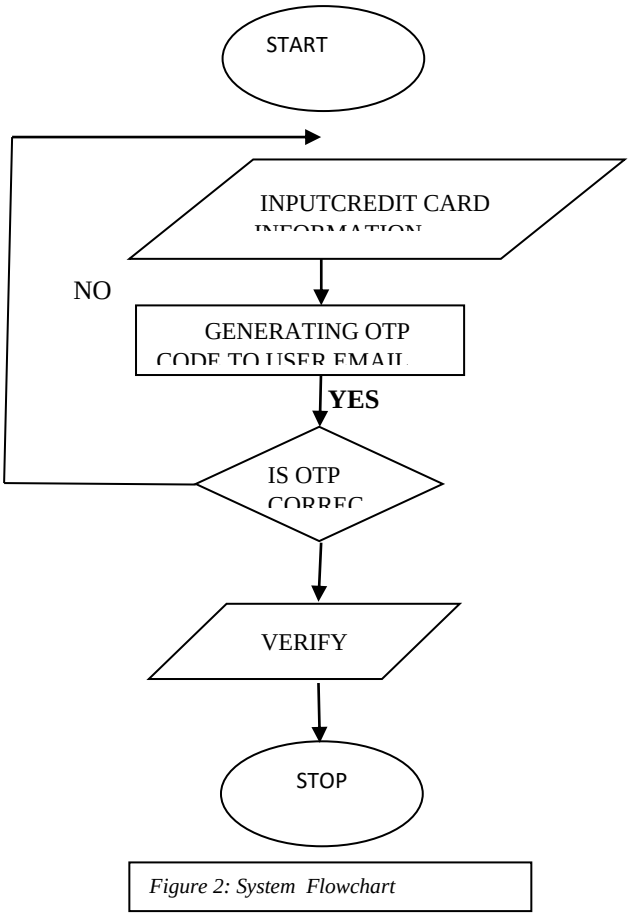

Figure 2: System Flowchart

System Architecture

This system architecture design, explains each level of the application and what it is made up of. The design shows the various operational levels such as client level which happens to be the end users, the application level which also happens to be the main application in use.

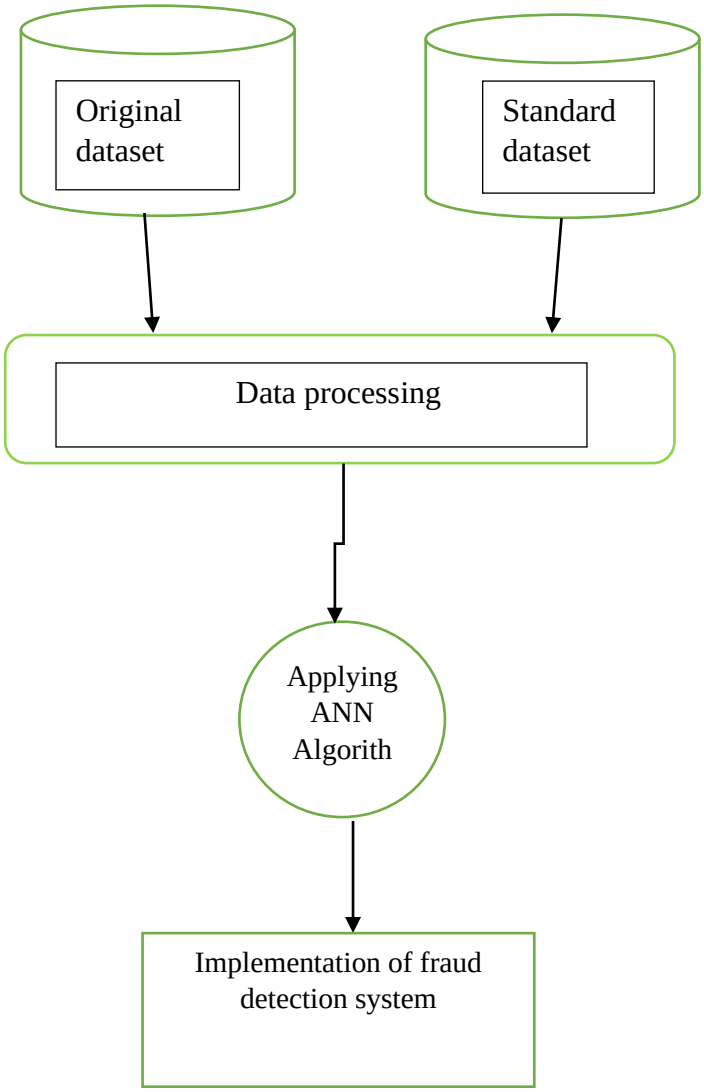

Figure 3: System architecture

Display of Graphical User Interface

The software complexity was broken down into simpler unit and solve problem separately and individually. The interfaces were represented as modules in the artifacts of the design. This makes it easy for modification in order to meet the new technological changes. This is the interface created which allows user to interact with the system.

The sign-up page: In this page, the user fills in the details below to create an account before the user will be able to login to the site. Once the user is registered successfully, the customer will be directed to the login page.

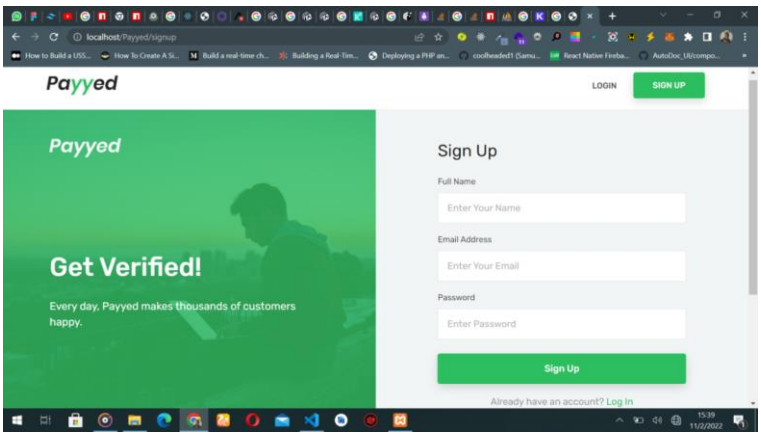

Figure 4: Sign-up page

The login page: A registered user can now login in this page. This is where the user will be directed to on successful registration.

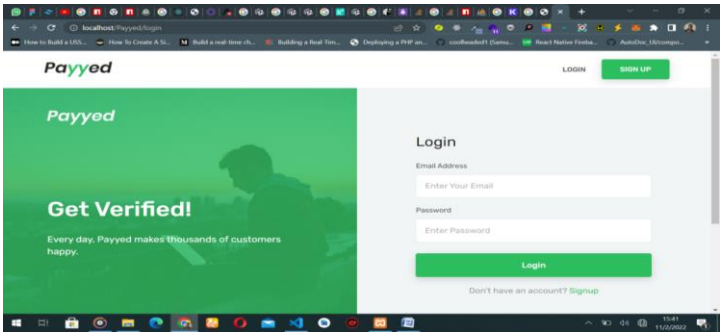

Figure 5: Login page

The set transaction pin and add account page: In the set transaction pin, the user will be ask to set a pin for transaction and the user will be ask to add a bank account that the user uses.

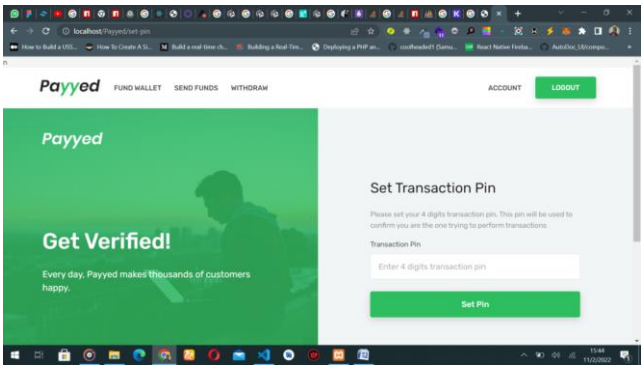

Figure 6: Set transaction pin page

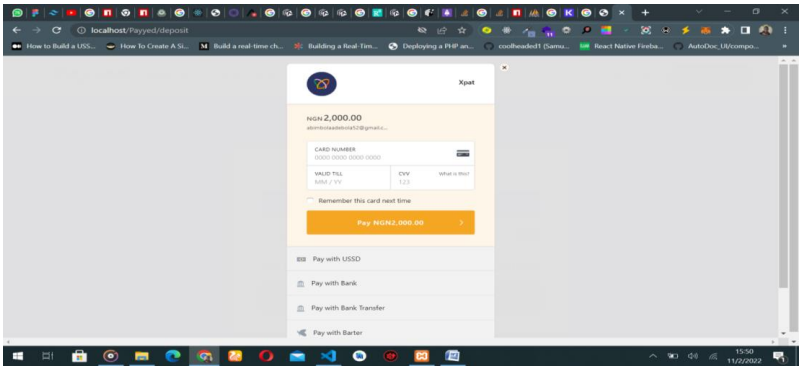

Figure 7: credit card details page

The email notification: If the user performs any transaction, the user will get a notification and if there is any fraudulent activity they get a notification about it.

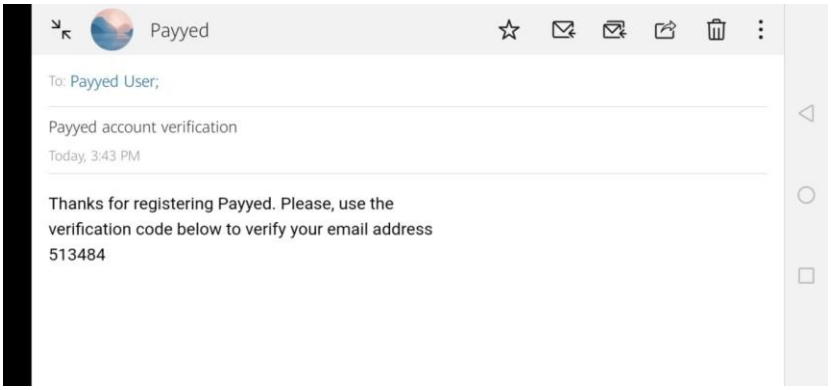

Figure 8:Email notification

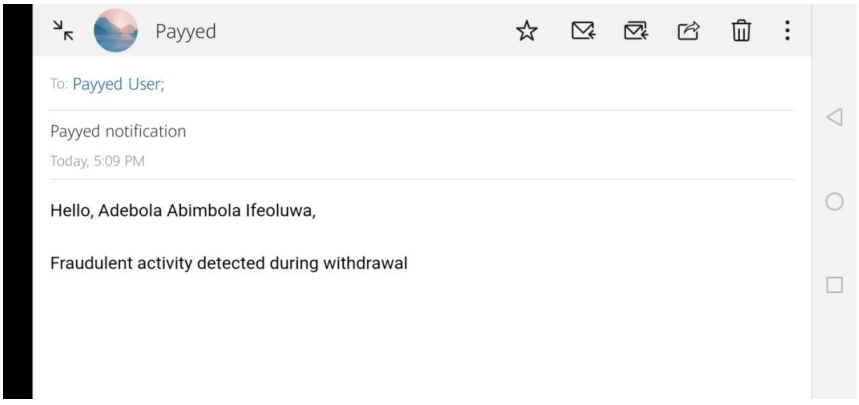

Figure 9: Fraudulent email notification

Conclusion

The prevention and detection of credit card fraud is currently an open problem that consistently attracts interest and investment from banks and financial organizations. Credit card fraud is a critically rising crime that costs billions of dollars worldwide each year. Traditional fraud prevention and detection methods are less adaptable in this situation. In this study, we've talked about the proposed framework and different adaptive fraud prevention techniques. Even though it was challenging to train a model that would function well for spotting fraud in credit card transactions, nevertheless neural network was utilized. In our model, the optimal method for detecting credit card fraud is to use an artificial neural network (ANN), which provides accuracy close to 100%. It offers greater accuracy compared to unsupervised learning algorithms.

Despite the high number of people using web applications, it is still important that the software is trained with different dataset to provide the users with the best possible experience. And can also be upgraded if needed be.

Reference

Asha R.B, and Suresh-Kumar K.R (2021): Credit card fraud detection using artificial neural network. Global Transitions Proceedings 2(1), Pages 35-41

Bejugama,V and Reddy, S.D (2021): Fraud Detection of Credit Card by using Random Forest Approach, Journal of Engineering Sciences 13 (11), pg 588-592.

Vijay .G, Suvarna. M, Disha. C, Om. P, Tanaya. B, Sagar. Y and Gopal. D (2022): Random Forest Classifier for Credit Card Fraud Detection, INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY 9(7), pg 587-593.

Akila, S. and Reddy, U. S. (2017): Credit Card Fraud Detection Using Non-Overlapped Risk Based Bagging Ensemble (NRBE), International Conference on Computational Intelligence and Computing Research

Debachudamani, P. and Santanu, K. R. (2019): Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning techniques, 10th International Conference on Computing, Communication and Networking Technologies.

Yasin, K., Seher, A. and Muhammed, T. Z (2020): 522 Detection of Credit Card Fraud in E-Commerce Using Data Mining, European Journal of Science and Technology No 20, pp. 522-529.

Sara. M. Zainab. A, Yehia. T, Rafiqul. H, Mohand-Saïd. H, and Hassan. Z.(2019): An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection, IEEE Access (7), Page(s): 93010 - 93022

Prusti, D., and Rath, S. K. (2019, October). Web service based credit card fraud detection by applying machine learning techniques. In *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)* (pp. 492-497). IEEE.

Kumar, M. S., Soundarya, V., Kavitha, S., Keerthika, E. S., and Aswini, E. (2019). Credit card fraud detection using random forest algorithm. In *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)* (pp. 149-153). IEEE.

Hammed, M., and Soyemi, J. (2020). An implementation of decision tree algorithm augmented with regression analysis for fraud detection in credit card. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(2), 79-88.

Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, 25579-25587.

Maniraj, S. P., Saini, A., Ahmed, S., & Sarkar, S. (2019). Credit card fraud detection using machine learning and data science. *International Journal of Engineering Research*, *8*(9), 110-115.