DAB 402 – CAPSTONE PROJECT

Literature Review – Detailed data Assessment

Credit Card Fraud Detection



GROUP **13**

|  |  |
| --- | --- |
| **NAMES** | **STUDENT ID:** |
| *Jai Surya* | 0731608 |
| *Rajit Kumar* | 0730468 |
| *Amita Mehta* | 0730478 |

***Date – 03/26/2020***

**Topic: Credit Card Fraud Detection**

**Problem Statement:**

Electronic figuring and correspondence represent probably the most unpredictable difficulties building has ever confronted. They run from securing the secrecy and honesty of transmitted data and dissuading fraud to forestalling the situation as of late performed in the Bruce Willis film "Live Free or Die Hard," in which programmers bring down the transportation framework, at that point correspondences, lastly the force matrix. The most intricate test building has ever confronted is electronic correspondence and figuring. Digital Crime is the most difficult issue in the current time. As indicated by U.S.A. government in excess of 600 billion measure of misrepresentation happened yearly and it is expanding by 1.2 billion. What's more, in excess of 200 billion measures of misrepresentation occurred in the financial segment. South Africa has as of late been beset by misrepresentation in credit and banking data from internet banking endorsers. Mastercard extortion is the point at which somebody utilizes your Visa or credit record to make a buy you didn't approve.  Fraudsters can likewise take your Mastercard account number, PIN and security code to make unapproved exchanges, without requiring your physical charge card. Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection.

**Summary 1: The Effects of Cyber Threats on Customer’s Behavior in e-Banking Services**

1. The current project has clearly described the causes of cyber threats and the measures that must be taken to prevent cybercrime. In this project we have seen that the cybercrime is the major problem in the financial institutions in 21st century. The cybercrimes occur mainly for Identity theft, phishing, vishing, malware, hacking and cracking, social engineering, automating online banking fraud etc. The common security measure that must be taken for preventing from cybercrimes are: Securing the device using for online banking, protecting personal data, use strong password, upgrade system and software.

According to a survey it is proved that 70% customers are not aware or got limited awareness about cyber threats. Therefore, the online banking users need to keep extra care over their usage towards banking services, E-banking customers should be taken care and should educate them more about the cyber threats and secure process for online banking environment.

[<http://www.ijeeee.org/vol7/414-IM023.pdf>](http://www.ijeeee.org/vol7/414-IM023.pdf)

**Summary 2: Cybercrime In Banking Industry And Its Impacts On Banking Industry**

2. This project described the outline of cybercrime in banking industry and its effects on banking industry globally. The major cybercrimes occur at credit card frauds and vishing. Banks should take adequate measures to educate customers through their websites about this banking fraud and secure banking options, the banks should work cooperatively with other banks to avoid cybercrimes. Banks should take strong measures for eradicating cyber fraud completely by hiring strong IT background employees with more knowledge in technology and cybercrime prevention tactics.

[[file:///C:/Users/AMITA%20MEHTA/Downloads/cybercrime-in-banking-industry-and-its-impacts-on-banking-industry.pdf](C:\\Users\\AMITA MEHTA\\Downloads\\cybercrime-in-banking-industry-and-its-impacts-on-banking-industry.pdf)](file:///C:\Users\AMITA%20MEHTA\Downloads\cybercrime-in-banking-industry-and-its-impacts-on-banking-industry.pdf)

**Summary 3: Anonymized credit card transactions labeled as fraudulent**

This project contains the data of credit card transaction made in September 2013 by European cardholders. The data contains 20 columns and 284,807rows. First column having data of number of seconds elapsed between this transaction and the first transaction in the dataset and rest of the columns made by the PCA use. The data is imbalance as the dataset contain the data of transaction happened in two days, where we found 492 frauds out of 284,807 transactions. It contains numerical data which are the result of pca transformation except amount and time. As they don’t want to disclose the personal information.

First, they balance the dataset and use the column created by the pca transformation for the fraud prediction. For class imbalance ratio, they use the accuracy using the Area Under the Precision-Recall Curve. They use the logistic regression, KNearest, supply vector and decision tree classifier for the fraud prediction.

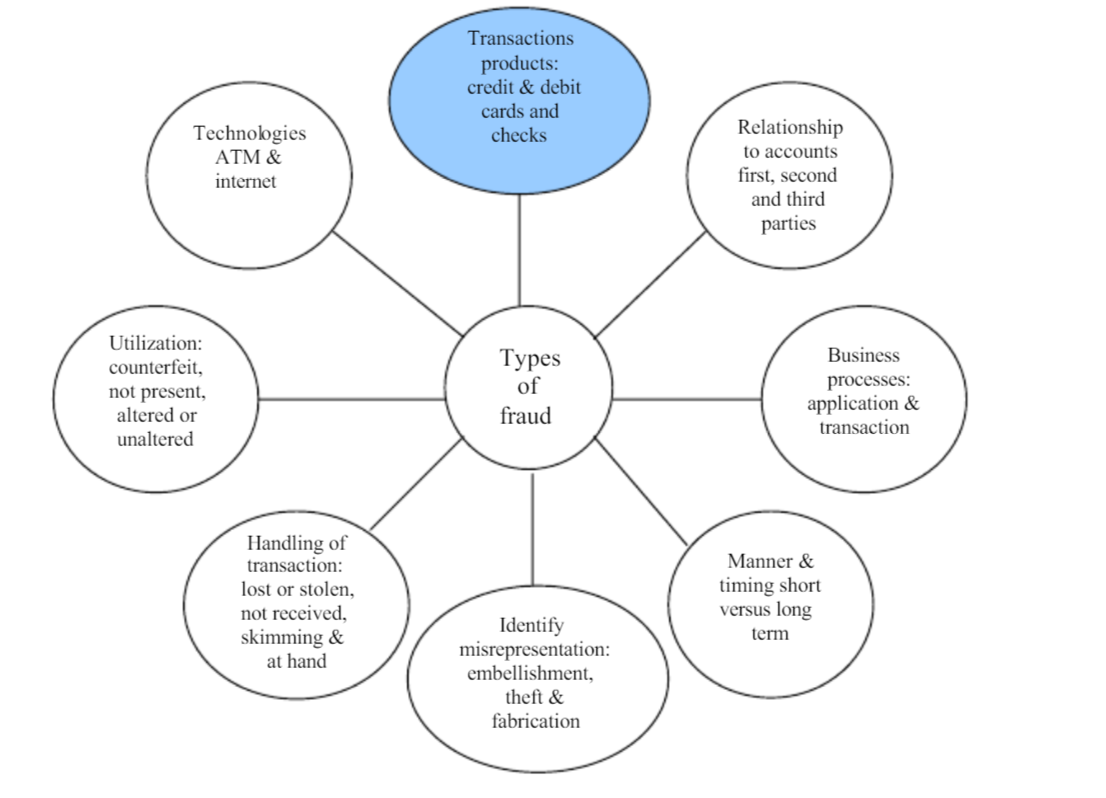
**Reference:** Kaggle.com. (2020). *Credit Card Fraud Detection*. [online]

Available at: <https://www.kaggle.com/mlg-ulb/creditcardfraud> [Accessed 23 Feb. 2020].

**Summary 4:** [**Abstract data set for Credit card fraud detection**](https://www.kaggle.com/shubhamjoshi2130of/abstract-data-set-for-credit-card-fraud-detection)

In this project dataset contains 12 columns and 3076 rows. They iterate through all the columns and modify the data type to reduce the memory usage. They split the data into test and train for the model selection. They use counter vector classifier, logistic regression, gradient boosting classifier and MultinominalNB for the fraud prediction. But the accuracy for all the model are very less to find the best model they use the confusion matrix for the classification report. The main aim of this project, firstly to identify the different types of fraud credit card fraud and secondly, to review alternative techniques that have been used to identify the fraud.

Following chart shows the different types fraud detection in credit card:



**Reference:** Kaggle.com. (2020). *Credit Card Fraud Detection*. [online]

Available at: <https://www.kaggle.com/aherparesh/credit-card-fraud-detection> [Accessed 23 Feb. 2020].

# **Summary 5: A Review of Data Mining-Based Financial Fraud Detection Research**

This project is regarding the rapid development of smart phones and the plethora of smart phone applications becoming developed, the lines between the cellular network and the internet are being blurred, rendering the phone a not-so-trusted device. In this article they show how existing smart phone banking applications can be tampered to capture user information and password. In this article they use the column which contain the data of the smart phone i.e. with which network the device was connected. And fraud happened. They use clustering for pre-processing and then use the logistic regression, decision tree, knn models for the prediction.

**Reference:** Ieeexplore.ieee.org. (2020). *Cost Sensitive Credit Card Fraud Detection Using Bayes Minimum Risk - IEEE Conference Publication*. [online]

Available at: [https://ieeexplore.ieee.org/abstract/document/6784638](https://ieeexplore.ieee.org/abstract/document/6784638%20) [Accessed 24 Feb. 2020].

**Summary 6: Automating Online Banking Fraud**

This project has described about the automates transfer system (ATS’s), which is highly used by cybercriminals in conjunction with Spy Eye Zues malware variants as a part of web inject files. We have also seen why some countries are targeting as compare to others. This project predicted that ATS could be a better source of the income and cybercriminals Will continue to improve ATS. ATS performs fraudulent transactions in the background and so it is hard to determine ATS infection. The cybercriminal underground is the place to find people coding Web Inject files and ATSs.

A Web Inject file is basically a text file with a lot of JavaScript and HTML code. This file allows cybercriminals to target specific organizations (e.g., banks) and inject specific code into victims’ browsers so they can modify the web pages the users access in real time. Web Inject file users can easily make fake pop-ups that ask victims for specific credentials (e.g., social security numbers and mothers’ maiden names) appear. Web Inject files have all of the code required to fool victims into thinking the pop-ups they see are real.

In this project, it clearly described that It is suggestible to check the bank account via checking balances over the phones or monitoring bank statements sent through emails instead of checking them in online.

At the end financially institution will get benefited from analyzing ATS attack method to identify whether they must modify or supplement the current security control.

**Reference:** (2020). Retrieved 24 February 2020,

[from https://www.trendmicro.co.uk/media/misc/automating-banking-fraud-via-ats-research-paper-en.pdf](from%20https:/www.trendmicro.co.uk/media/misc/automating-banking-fraud-via-ats-research-paper-en.pdf)

**Summary 7:** **BANKRUPTCY PREDICTION SYSTEM FOR CREDIT CARD USING MACHINE LEARNING TECHNIQUES: A SURVEY**

In this article we studied that they are classifying the transaction, they are predicting that a transaction is high risk transaction or low risk transaction. They have dataset with 100000 rows and 20 columns, and they are using naive Bayes classifier.

They first collected the data then did some pre-processing after that they selected the features of their interest using feature selection. Then they did classification using naive Bayes classifier after that all they used confusion matrix to check the performance.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dataset** | **No. of Features** | **Total Instances** | **No. of Instances (Yes)** | **No. of Instances (No)** |
| USCD-FICO | 20 | 10,0000 | 97346 (97.35%) | 2654 (2.65%) |
|  |  |  |  |  |

**Reference:** Irjeas.org. (2020). [online]

Available at[: http://www.irjeas.org/wp-content/uploads/admin/volume7/V7I1/IRJEAS04V7I101190319000002.pdf](https://stclairconnect-my.sharepoint.com/personal/w0730468_myscc_ca/Documents/:%20http:/www.irjeas.org/wp-content/uploads/admin/volume7/V7I1/IRJEAS04V7I101190319000002.pdf)