ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 6, June 2022

Credit Card Fraud Detection Using Machine Learning Algorithms

[1] Abhishek, [2] Devi Naveen

[1] CSE Department, New Horizon College of Engineering, Bangalore Karnataka, India.
[2] Sr. Assistant Professor, CSE Department, New Horizon College of Engineering, Bangalore, Karnataka, India.
Corresponding Author Email: [1] abhishek.1nh18cs701.cse@gmail.com, [2] devinaveen74@gmail.com

Abstract*— With the advancement of technology, the use of credit cards for shopping is also increasing. Since credit cards are the most popular payment method, errors on these credit cards are also increasing. This white paper presents the techniques used to detect credit card fraud as an overview paper. Fraud detection should be performed as soon as it is executed. Fraud detection methods are constantly evolving to prevent or prevent criminals from taking over their strategies. The transaction was determined to be normal, abnormal, or suspicious based on the initial assumptions. When a transaction is determined to be suspicious, their beliefs are further strengthened or weakened by comparing their similarities to fraudulent or real transactions using Bayesian learning.

Index Terms*—About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

Recently, the popularity of online shopping is increasing day by day. According to a 2005 survey by AC Nielsen, one in ten people in the world's population uses online shopping. Because credit cards are the most popular payment method. As a result, the number of credit card users is increasing, and the number of credit card fraud users is also increasing.

Purchasing using a credit card is divided into 1) the purpose of using the physical card and 2) the purpose of using the virtual card. In the case of a physical card, payment is made by presenting the card directly to the cardholder. While the real card is working, an attacker must steal the card, forge a signature, and buy it. To use a virtual card, all you need is card information such as card number, expiration date, and security code. This is done through online purchases over the Internet or over the phone. To commit fraud with this type of purchase, you need to know the details of the card[1]. Payment for online purchases is usually made by credit card. Credit card fraud is increasing day by day. Financial losses from credit card fraud are also increasing day by day.

Security means avoiding fraud when using your credit card. The secure use of credit cards is also known as security. In credit card fraud cases, fraud cases such as lost card, card theft, card theft, application fraud, non-receipt of spending, and mail order spending fraud were found.

Credit card details must be kept secret. To protect your privacy, please do not disclose your credit card details. The ways to get information about stolen cards are phishing websites, theft of credit card details, fake card details, and intercepted cards. For safety reasons, avoid the above cases. Valid and invalid transactions are checked for credit card security. Most fraudulent credit card cases are related to card number theft, not credit card theft. Therefore, keep your credit card safe.

Fraudulent credit card purchases in online or internet mode

In online mode, only map data is required. Online card transactions do not require manual processes such as card signing, PINs, and card imprints. In these online modes, the real cardholder is unaware that the card details have been stolen or stolen. To find detections of online credit card fraud, you need to analyze your credit card spending behavior, compare it to normal spending behavior, and report discrepancies.

Fraud detection by analyzing the purchase history of existing cardholders to prevent credit card fraud. Credit card payments from credit cards, debit cards, prepaid cards, and smartphone purchase card transactions are considered fraudulent. Fraudulent account activity or transactions by someone whose account is not intended are considered credit card fraud. Operationally, this credit card fraud detection event is held to stop ongoing fraudulent use and incorporate risk management techniques to prevent the same fraudulent activity against future approved credit card purchases. Credit card fraud occurs when the cardholder or the cardholder's issuer uses another person's credit card without knowing that another person has accessed his or her credit card. Fraud detection methods have been introduced to protect criminals from such illegal credit card fraud. Due to the limited number of fraud detection methods, the number of credit card fraud detection methods is small. The dataset is also unavailable and the results are not published. The fraud detection method should consist of a set of log data and a set of data called user behavior. Fraud detection is currently implemented in many ways, including data mining, statistics, and artificial intelligence.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 6, June 2022

1.1 MOTIVATION – TYPES OF FRAUD

The types of fraud covered in this document are credit card fraud, telecom fraud, computer intrusion fraud, bankruptcy fraud, theft fraud, application fraud, and act fraud.

Credit Card Fraud: Credit card fraud is divided into two types:

Offline fraud: Offline scams are carried out everywhere using stolen physical cards.

Online fraud: Online fraud occurs when the internet, phone, online shopping, or cardholder is absent.

Telecommunication fraud: Use of telecommunication services to commit other forms of fraud. Consumers, businesses, and telecom service providers are suffering.

Computer Login: Login is defined as the act of logging in without permission or invitation. "There is a possibility of unauthorized access to information and intentional information. An attacker can be attacked from anywhere, such as an outsider (or hacker) or an insider who knows the design of the system. Fraudulent Fraud means using your credit card while abroad. Fraudulent fraud is one of the most expected forms of fraud.

Theft/fraud - This section is about criminal activity and related fraud. Criminal Fraud refers to anyone other than the cardholder. If the owner provides feedback and contacts the bank, the bank will take steps to proactively detect the thief. Similarly, when using a credit card remotely, fraudulent fraud occurs when only credit card information is required.

Application Fraud – When someone applies for a credit card with false information, it is called a fraudulent application. To be fooled by the app, you need to separate the two cases. If the application has the same data from the same user, it's called replication, and if it's another person's application with the same data, it's called identity theft. Malicious applications are defined as "signs of crime with the generation of personal data.

Internal Fraud: In the banking industry, employees have access to customer data. The data is the same as the information required to access the online bank account of the customer account. Therefore, employees can easily commit fraud. Instead, the financial institution must either require a password or have the bank's PIN encrypted.

II. OBJECTIVE - INTRODUCTION TO TYPES OF SOLUTIONS FOR THE FRAUD

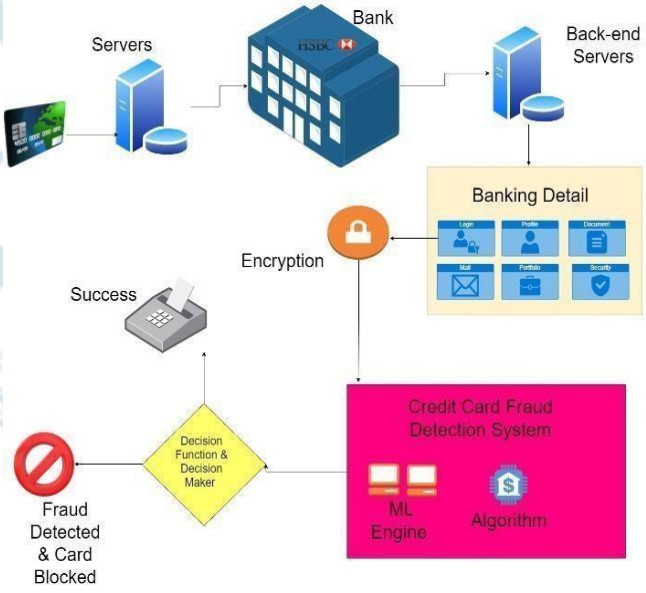
Fraud and data theft should be taken personally and financially as a challenge. Fraud and data theft can cause great frustration.

How to deal with credit card fraud? Fraud is the fraudulent use of your credit card account. Fraud is usually detected when a credit card is lost or stolen, an unusual amount is found on a payment statement, or a phone call or letter is sent about an unpaid transaction, and the credit card company's fraud department is contacted for billing. Inquire about. If you suspect fraud in your account, you should contact your credit card company immediately. Credit card companies can verify fraud, eliminate claims by cardholders or authorized persons, close accounts to prevent further fraud, issue new account numbers with new cards, and relocate old information to new accounts. You can assist in the transfer.

It's also a good idea to check your credit report to make sure there's nothing else suspicious. In most cases, law enforcement involvement is coordinated with financial institutions.

How to combat identity theft? Data theft is a form of fraud in which thieves use personal information to create new accounts or obtain other benefits on behalf of cardholders. This, like other forms of fraud, is common, but can be tricky and can lead to serious problems.

Other signs of identity theft include: If the cardholder does not receive credit or other mail; has received a credit card; has been denied credit without good cause; has received a call or letter about an item the credit cardholder has not purchased; case. For issues not involving the cardholder. Do not assume that such unexplained events are always wrong. See Confirmation for details.



III. LITERATURE SURVEY

Fraud detection is a difficult task and there is no system that accurately predicts any transaction as fraudulent. The features of the fraud detection system are:

1. Should identify the frauds accurately
2. Should detect the frauds quickly.
3. Should not classify as genuine transaction fraud.

Finding Outlier is an important task as outsiders show unusual working conditions when they are important a decrease in performance is possible. Strategies used to detect fraud can be divided into two types.

1. Outstanding tactics where known cases/frauds are known in the past are used to create a model that will produce suspicious points in new practices.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 6, June 2022

2. Unsupervised are those where there are no previous sets where the status of the activities is known as fraudulent or legal.

3.1 Methods - Unsupervised outlier detection technique

An unsupervised external ingestion strategy does not predict the availability of labeled data. This approach requires that these accounts, clients, etc. behave "abnormally". The untested method is useful for applications that do not have prior knowledge of a particular monitoring category in the data set. The advantage of using unsupervised methods and over-controlled methods is that previously detected forms of fraud cannot be detected. The strategy we are currently using are:

Peer Group Analysis - It (PGA) is an unsupervised method for tracking behavior over time in data mining. The main function of the PGA method is to determine the peer group of all current targets (subjects). This tool detects that individual objects begin to behave differently from objects in the past. Each element is selected as a target and compared with all other elements on the web page by external comparison, or internal state by summarizing the past behavior of each element. On the basis of comparison, the most similar target group is selected. This tool is part of the data mining process, which includes a cycle of anomalous behavior detection and detailed examination of these objects. The PGA method was originally used to detect credit card fraud by varying the length of time periods used to identify peer groups.

Break Point Analysis - It is another unattended external fraud detection tool. The point of the pause is the realization or time of the madness. Breakpoint analysis is applied at the account level by comparing sequences of activities to identify variations in activity for a particular account. Breakpoint analysis shows the movement of the window because the transaction may enter the window and remove the oldest transaction from the window. The advantage of breakpoint analysis is that you don't need balance data because you can compare activity between different accounts and identify a complex set of events that may reflect malicious behavior.

K-Means Clustering Techniques- It is a simple and efficient way to combine data. Initially, K and centroid cluster numbers are available. Random elements such as the first focus and the first K element can serve as the first focus. This process is a non-hierarchical approach. Initially, we assume the number of elements is equal to the number required at the end of the set. Repeat until stable (= no group movement):

Place K points in the space represented by grouped objects. These points represent the original centroid group.

1. Assign each object to the group with the most.
2. When all objects are assigned, recalculate the position of the K centroid.
3. Repeat steps 2 and 3 until the center of the figure stops moving. This divides the object into groups, from which you can calculate the metric to minimize.

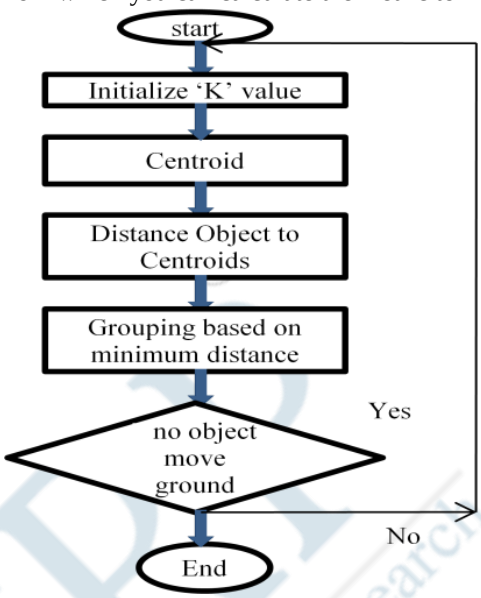


Fig.1. Block diagram of K- means algorithm process [5].

3.2 Other methods - Supervised outlier detection technique

Controlled external collection methods classify the collection of required datasets into general and external categories. The monitoring system detects bad transactions. You can use it to distinguish between known rogue accounts or activities and activities that are known to be legitimate. Identification techniques such as neural networks and statistical neural network analysis can be used to distinguish between rogue and non-fraud activities and assign suspicious scores to activities. The monitored method was trained to distinguish official activities from previously known scams.

When writing a book review on various fraud detection methods, Gass algorithm, Bayesian network, HMM (Hidden Markov Model), GA (Genetic Algorithm), Dempster-Schafer theory and Bayesian learning, Decision Tree, Neural Network (NN), Logistic Regression (LR) like several methods are there.

Gass Algorithm: It is a combination of genetic algorithms and distributed search. The basic premise is that the survival rate of strong members in a society is higher than that of weak members and that the level of well-being increases as generations age. The least qualified member of the generation is eliminated and the strongest member is chosen as the parent of the next generation. This process is repeated until the best solution is found.

Bayesian Networks - Two Bayesian networks have been developed to determine user behavior for fraud detection. The first Bayesian network is designed to model behavior assuming that the user is fraudulent (F), and the second model is built assuming that the user is legitimate. (NF). "Rogue networks" are built using expert information, and "user networks" are built using data from rogue users. During

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 6, June 2022

operation, the user network is modified by specific users based on current data. Publishing evidence on the Internet and disseminating it over the Internet limits both options. This indicates the extent to which a user's behavior is considered fraudulent or non-fraudulent. Bayesian networks can also integrate the expert information used to initially build the model. The user model, on the other hand, is retrained with data in an unregulated way. Therefore, the Bayesian approach combines both expertise and education.

Hidden Markov Model – Hidden Markov models are double built-in stochastic processes used to model the most complex random processes. An incoming credit card transaction is considered fraudulent if it is not authorized by the Hidden Markov model with a sufficiently high probability. The BaumWelch algorithm, like the K – means integration algorithm, is used for educational purposes. HMM, stores data in batches of the low, medium, and high prices. When the first set of possible actions is chosen FDS evaluated whether the action is true or false. HMM maintains a log of work, reducing the workload of its employees while providing a high level of false positives and a high level of lies. The first set of parameters that affect the performance of the algorithm should be chosen carefully.

Genetic Algorithm Evolution-inspired genetic algorithms were first introduced by Holland (1975). Genetic algorithms are evolutionary algorithms that provide better solutions over time. Fraud detection is often an area of e-commerce data mining. GA is primarily used for dynamic selection data mining and is often integrated with other DM algorithms. Excellent results can be obtained when combined with other methods. GA is used to detect credit card fraud and reduce unplanned activity. It is also easily accessible via a computer programming language that is effective in detecting credit card fraud. However, this method is very efficient and expensive.

The Fusion Approach – Using Dempster- Shafer Theory and Bayesian Learning – Dempster- Schafer theory proposes a fraud detection system using to integrate Bayesian Knowledge and learning. Here, proof of current and past behavior is combined and a performance profile of each cardholder is established based on the type of purchase behavior. **T**he advantages are high accuracy, processing speed, reduction of false positives, and improved acquisition rates applicable to e-commerce. The disadvantage of this method is that it is very expensive. The FDS program consists of four sections: official filters, Dempster Shafer appendixes, work history pages, and Bayesian readers. Actions are classified as suspicious or suspicious, depending on the first stage. When an action is perceived as suspicious, the actual distortion or comparison reinforces or weakens the beliefs.

Decision Tree – It is a mathematical formula for obtaining data using independent and logically dependent structures and tree structures. The rules of separation extracted from the decision tree are the IF-THEN principles, and each law must pass all the tests to obtain it. Decision trees often rot complex problems easily and solve small problems through reuse. Decision trees are decision-making tools that produce maps based on material. Decision tree methods are C5.0, C&RT, and CHAID. Data mining technologies, including logging and SVM for credit card fraud, help reduce bank risk.

Neural Network-This method is based on fraud detection methods that are widely used. An active neural network is made up of groups of interconnected artificial neurons. Neural network goals are driven by brain functions, especially pattern recognition and coherent memory. Neural networks identify identical patterns by predicting future values or events based on the associative memory of learned patterns. Used for segmentation and merging. The advantage of neural networks over other strategies is that these models learn from the past and improve their results over time. You can also set up rules based on the current situation and predict future actions.

Two phases of neural network training and detection. Learning from a neural network is called learning. NN training methods are tracked, but not tracked. The model was built using patterns of fraudulent and non-fraud recording during supervised training. While unsupervised learning aims to find those jobs, unsupervised learning does not require any prior knowledge of website scams or scams and is very unusual. NN is ideal for large databases.

Logistic Regression - Two data mining methods, a vector support system, a random forest, and known retroactive regression as part of an effort to detect credit card fraud. Easy to understand, easy to use, and widely used in data mining. Therefore, it provides a useful basis for comparing the effectiveness of new methods.

Supervised learning methods for credit card fraud detection can get two problems. They are:

1. The class size does not match the official function and the fake function, and the legal function is much better than the fake function.
2. Second, develop a traceable monitoring model that can result from fraudulent activity that may go undetected so that you can document misbehavior in the data you use to create the model.

To address the above issues, a fraudulent transaction is one that the agency's auditors have identified as causing an illegal transfer from a credit card bank. This transaction was considered a fraudulent disclosure. This study is based on real data on the results of international credit card transactions.

IV. ANALYSIS OF EXISTING TECHNIQUES

Srivastava et al. Develop a credit card sequence model, demonstrate the effectiveness of the system, and present test results demonstrating the usefulness of reading cardholder spending records. Comparative studies have shown that the system accuracy is close to 80%, despite the high variability

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 6, June 2022

of the input data. Accuracy represents a fraction of the total amount of work purchased with precision (both genuine and fake). The system can also handle a large amount of operations.

Suman and Nutan Outlined current strategies for detecting credit card fraudand communication fraud. This document provides a comprehensive overview of various fraud detection strategies. The various forms of fraud described in this document include credit card fraud, communications fraud, computer hacking, bankruptcy fraud, crime / fraud, application fraud, and ethical fraud. Gas Algorithm, Bayesian Network, Hidden Markov Model, Genetic Algorithm, Integration Method Using Dempster Schaefer Theory and Bayesian Learning, Decision Tree, Neural Network, Logistic Retrospective Method Credit Card Fraud Detection The purpose of this document is to use the user model. Is to identify. Great for detecting fraud.

Delamare et al. Identify types of credit card fraud such as bankruptcy fraud, cash counterfeit fraud, theft fraud, application fraud, and ethical fraud and consider alternatives such as double modeling, decision trees, strategy integration, emotional networks, genetics, and more. List the problems with your bank and credit card companies. The next step in this research program is to evaluate the use of "suspicious" scorecards in real databases. The main challenge is to consider the ethical domains associated with the different types of credit card fraud discussed in this article, assess their moral implications, and develop point models for predicting fraud. to be. The plan is to expand one of the European countries, perhaps Germany, into another EU country.

To solve the problem of data tampering, **Phua et al.** propose a new fraud detection method based on existing fraud detection research and youth reports. Use Angoss Knowledge Seeker software for testing. In this article, the X pass rate is at least 10% better than all averages and pass rates across the test set. When used in a scoring set, Fund Z's probability of success is slightly higher than Y's average probability of success. The challenge for the future is to make one category more relevant than the other.

Esakkiraj and **Chidambaram** developed a virtual model from an online sequence using a hidden Markov model (HMM) to determine whether a user was a regular user or a fake user. The trained system tests new tasks to change and display parameters. Based on the display settings, the system recognizes the allowed options and decides whether to deny the function. Existing online fraud detection systems detect fraud after a transaction is completed. This causes financial losses and the name of the bank is uncertain. This model predicts transaction fraud and prevents money transfers.

As a future operation, some segmentation algorithms work instead of using combinations that can succeed in prediction.

Sahin and Duman Have created a fraud fraud detection model that effectively improves the financial performance system using a decision tree algorithm and seven classification methods using SVMs. This activity demonstrates the benefits of using data mining techniques that combine decision-making and SVM to identify credit card fraud in real-world datasets. In this study, the performance of a classification model built using the well-known decision methods C5.0, C & RT, CHAI, D, and various SVM method (polynomial, sigmoid, linear, SVM using RBF kernel) functions. Indicates the number of. Comparison. When comparing model performance in terms of accuracy, as the amount of training data grows, this proper behavior becomes less noticeable and the performance of the SVM-based model is compared to the tree-based model. However, the amount of fraud detected by the SVM model is less than that of the decision tree model, especially the C & RT model. The C5.0 model is more efficient than the other models in terms of the accuracy of each sample, but the C and RT models capture the most cases of fraud. Therefore, the C & RT and C5.0 models are chosen as a last resort for creating speculative models. For future work, use different versions of the Artificial Neural Network (ANN) and other data mining algorithms such as upgrades to generate a new difference model in the same real database to improve the performance of the new model. Compare. .. The model introduced in this white paper**.**

Bolton's habd outlined outlined two categories: ethical fraud and application fraud. However, this article aims to detect behavioral fraud through longitudinal data analysis. Therefore, here we discuss two methods of credit card fraud detection and apply them to different real-world data sets. This section describes peer group analysis followed by breakpoint analysis, a new tool for monitoring behavior over time in data mining situations. He describes the use of PGAs to detect changes in credit card spending and shows the tendency to find losers through fake research. Shows an example of using a credit card with 858 accounts and weekly expenses for 52 weeks. The PGA may find that this week's spending is unusual for accounts with similar spending styles.

Ferdowsi and **Maeda** presented the problem of finding suppliers in a financial data chain using an unregulated fraud detection method, Peer Group Analysis (PGA). PGAs can find traders who suddenly start selling stocks differently from other similar traders before. Tests are performed with continuous values at regular intervals on issues that cannot be managed in the stock market history with the PGA tool. The test results are presented in clear images, demonstrating that peer-to-peer analysis can help gain different perceptions of colleagues. And tnumbers are used to find the variance correctly. A future challenge is to integrate the alternative with PGA and apply this strategy to additional applications such as bank fraud detection.

Mishra et al. uses a hidden Markov model to present the theory required to detect fraud in the credit card purchase process and show how to use this model to detect fraud. If a transaction coming to your credit card is not accepted by

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 6, June 2022

HMM with a high probability, it is a scam. At the same time, do not allow the actual transaction to be rejected. While object types were considered HMM ranges, values from other ranges generated by visual cues were used. It also describes how to obtain a cardholder's monetary profile and how this information is used to determine display capabilities. It also explained how HMM can determine if an incoming order is a scam and, if so, notify the user immediately. In the proposed model, more than 85% of the actual indicators and false positives account for only 8% of the total number of positives. Comparative studies have shown that the system's accuracy is close to 82% for a wide range of input data**.**

In this article, **Rama Kalyani** and **Uma Devi** propose a credit card fraud detection system using a genetic algorithm. The goal is to improve the way genetic algorithms are used to generate test data and detect fraudulent transactions. This algorithm is a search optimization and promotion method based on genetic and selective properties. It is a heuristic method that solves complex computer problems and evaluates the results according to the principles of this algorithm. This algorithm is used to detect credit card fraud and can predict the likelihood of fraud immediately after purchasing a bank credit card.

Chang et al. Proposed a new learning curve in by developing a new access system (IDS) via a backpropagation neural network (BPN) with query patterns and queries**.**

Patidar and Sharma used neural used neural networks and genetic algorithms to detect fraudulent transactions. Streaming backpropagation control learning algorithms are used to train artificial neural networks. This white paper uses BPN for training purposes and selects parameters that play an important role in making the neural algorithm as accurate as possible (weights, network types, layer numbers, node numbers, etc.). A genetic algorithm was used, and the combination of the genetic algorithm and a neural network (GANN) was successful in detecting credit card fraud. The challenge for the future is to develop a specific system that can manage credit card fraud before the actual transaction takes place.

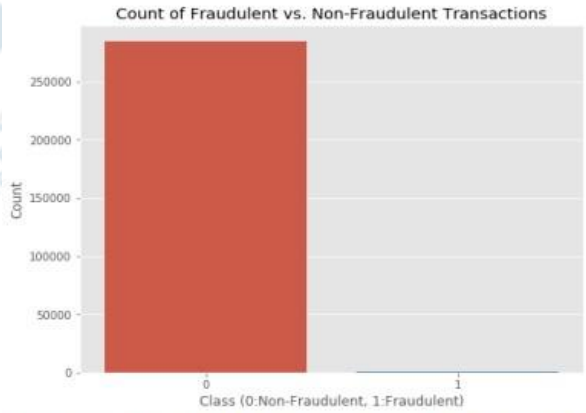
Subashini and **Chitra** built CART 5, a C5.0 segmentation model of a logistic Bayesian network for bank fraud detection using decision trees, SVMs with polynomial function symbols, logistic poles, and credit cards. You have exited split branch mode. . Fraud data set. Official users make false claims and scammers make false claims. C5.0 with J48, SMO and SVM with Bayesian network had a success rate of 72.4%, good splits in SVM used SMO because bad evils were as bad as good splits. Instead of classifying good clients as bad clients. The tracking method achieves a success rate of 73.1% and CART achieves a high success rate of 74.1%. So, depending on the degree of success, the CART outperforms the other models, and the J48 performs better in the "bad to good" category. So, when segmenting your customers, you need to use different classification methods to make the right decisions about them.

Phua et al. compare and evaluate almost all published technical articles and has a review area for automatic fraud detection. This article describes professional scammers, scam types and subtypes, data technology types, performance indicators, methods, and techniques. After reviewing the limitations of fraud detection methods and methods, this article shows that this sector can benefit from other relevant areas such as: B. Unmanned counterterrorism technology, real-time surveillance systems, and document extraction for law enforcement agencies**.**

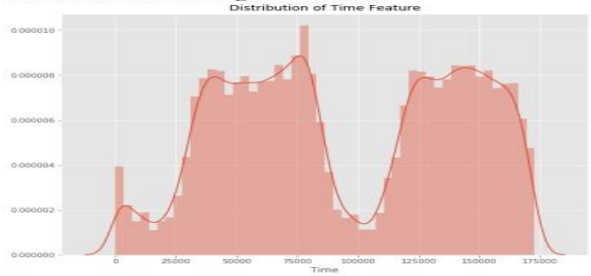
Bagheri et al evaluated the performance of a group of three-phase couplers trained on different data sets. This is a strong combining strategy based on the Dempster Network (ANN) and the Bayesian Belief Network (BBN), which shows that it will have a significant impact on real financial data. ANN uses backpropagation or short backpropagation of the error signal. We compared the results of BBN anime-based on experiments. This shows that BBN detects 8% more fraudulent transactions than ANN. BBN performs better than ANN, training time is about 20 minutes shorter, and ANN takes several hours. However, ANNs detect fraud much faster than BBNs.

V. RESULTS AND DISCUSSION

Class 0 represents valid transactions and Class 1 represents fraudulent transactions. Create various plots to identify and set.



This graph shows that the number of fraudulent transactions is much lower than the legitimate ones.



This graph shows the times at which transactions were done within two days. It can be seen that the least number of transactions were made during night time and highest during the days.

The code prints the number of false positives detected and compares it to the actual value. It is used to calculate the accuracy value and precision of the algorithm. To speed up the test, the percentage of data used is 10% of the total data set. The whole record is also used last and both results are printed. These results appear in the output, along with a classification report for each algorithm as follows: Here, class 0 means the transaction was validated as a valid transaction, and 1 means it was validated as an invalid transaction. This result is consistent with the class value of the false-positive test.

VI. CONCLUSION AND FUTURE WORK

Credit card fraud has increased dramatically in recent years. Fraud Detection Method Fraud detection, fraud detection was a little fast when done with a fraud detection strategy, but now it is easier and faster. The skills learned here are how to quickly catch credit card fraud and deter crime. Future work is to develop improved technology that is much better than existing technology

VII. ACKNOWLEDGMENT

I would like to take this opportunity to thank the doctor. Ashok K. Chauhan, the founder of Amity University, provided the long-awaited support and research infrastructure. We would like to thank Aditya Shastri, Vice President of Banana University, for her continued support.

REFERENCES

[1] A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, "Credit card fraud detection using hidden Markov model", IEEE transactions on dependable and secure computing, vol. 5, no. 1, January March 2008.

[2] Suman and Nutan "Review paper on credit card fraud detection", International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7– July 2013.

[3] L. Delamaire, H. Abdou and J. Poinon, "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[4] Phua, D. Alahakoon and V. Lee, "Minority report in fraud detection: classification of skewed data," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.

[5] S. Esakkiraj and S. Chidambaram, "A predictive approach for fraud detection using hidden Markovv model" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013 C.

[6] Y. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines", International Multiconference of Engineers and computer scientists March, 2011

[7] R.J. Bolton and D.J. Hand "Unsupervised profiling methods for fraud detection", Department of Mathematics Imperial College London {r.bolton, d.j.hand}@ic.ac.uk

[8] Z. Ferdousi and A. Maeda "Unsupervised outlier detection in time series data", Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW'06) © 2006 IEEE.

[9] J.S. Mishra, S. Panda, and A. Kumar Mishra, "A novel approach for credit card fraud detection targeting the Indian market" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, May 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org

[10] K. Rama Kalyani and D. Uma Devi, "Fraud detection of credit card payment system by genetic algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7, July- 2012.

[11] Ray-I Chang, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang and Jen Shiang Kouh "Intrusion detection by back propagation neural networks with samplequery and attribute-query", Research India Publications; (2006). (6-10).

[12] R. Patidar and L. Sharma ,"Credit card fraud detection using neural network" NCAI2011, 13- 14 May 2011, Jaipur, India International Journal of Soft Computing and Engineering (IJSCE) ISSN: 22312307, Volume-1, Issue-NCAI2011, June 2011.

[13] B. Subashini and Dr. K. Chitra "Enhanced system for revealing fraudulence in credit card approval", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 8, August – 2013 ISSN: 2278-0181.

[14] L. Phua, V. lee, K. Smith and R. Gayler, "A comprehensive survey of data mining-based fraud detection research", School of Business Systems, Faculty of Information Technology, Monash University, Clayton campus, Wellington Road, Clayton, Victoria 3800, Australia.

[15] M. A. bagheri, Q. GAO and S. Escalera "Logo recognition based on the dempster-shafer fusion of multiple classifiers", Advances in Artificial Intelligence, Lecture Notes in Computer Science Volume 7884, 2013, pp 1-12.

[16] Maes, S., Tuyls, K., Vanschoenwinkel, B. & Manderick, B. (2002), "Credit card fraud detection using bayesian and neural networks", Proc. of the 1st International.