e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

EXPLORATION OF TECHNIQUES FOR DETECTING CREDIT CARD FRAUD (A SURVEY)

M.L. Nithin*1, N. Keerthana*2, S. Kevin Andrews*3

*1PG Student, Department Of Computer Application, Dr. M.G.R. Educational And Research Institute, Chennai, Tamil Nadu, India.

*2Associate Professor, Department Of Computer Application, Dr. M.G.R. Educational And Research Institute, Chennai, Tamil Nadu, India.

*3Professor, Department Of Computer Application, Dr. M.G.R. Educational And Research Institute, Chennai, Tamil Nadu, India.

DOI : https://www.doi.org/10.56726/IRJMETS52225

ABSTRACT

With the rapid advancement of electronic commerce technology, there has been a significant increase in the usage of credit cards. As credit cards have become the most popular mode of payment, the occurrence of associated fraud cases has also seen a rise. This paper presents a comprehensive review of existing techniques for detecting credit card fraud. Fraud detection aims to swiftly identify fraudulent activities as they occur. Methods for fraud detection are continually evolving to counter criminals who adapt their strategies. Transactions are categorized as normal, abnormal, or suspicious based on initial assessments. If a transaction is flagged as suspicious, its likelihood of being fraudulent or genuine is further evaluated using Bayesian learning techniques.

Keywords: Electronic Commerce, Credit Cards, Fraud Detection, Transaction, Bayesian Learning.

I. INTRODUCTION

The prevalence of online shopping has been steadily increasing. A study by ACNielsen in 2005 revealed that one-tenth of the global population engages in online shopping. Credit cards have emerged as the preferred method of payment. With the expanding user base of credit cards worldwide, incidents of identity theft and fraudulent activities have surged. Credit card purchases can be classified into two categories: physical card purchases and virtual card purchases. In a physical card purchase, the cardholder personally presents the card for payment, requiring the attacker to physically steal the card and forge the signature to complete a transaction. Conversely, virtual card purchases only require the card information, such as the card number, expiration date, and secure code, typically used for online or telephone transactions. Committing fraud in virtual purchases simply necessitates knowledge of the card details. Online purchases are predominantly made using credit cards, leading to a rise in credit card fraud incidents. As credit card usage becomes more widespread, financial losses due to fraud also increase. Security measures are crucial for safe credit card usage and prevention of fraudulent activities. The primary aim of security is to prevent unauthorized use of credit cards. Instances of credit card fraud include issues such as lost or stolen cards, application fraud, counterfeit fraud, mail-order fraud, and non-received item (NRI) fraud. Implementing robust security measures for credit cards is essential to mitigate these fraudulent activities. Maintaining the confidentiality of credit card information is essential. To safeguard credit card privacy, it is imperative to prevent any leakage of details. Various methods used to obtain credit card details include phishing websites, theft or loss of physical cards, counterfeit cards, card detail theft, and interception of cards. To enhance security, it is crucial to mitigate these risks. Credit card security measures are vital for distinguishing between valid and invalid transactions. It's important to note that many fraudulent transactions stem from the use of stolen card numbers rather than the physical theft of the card itself. Therefore, it is essential to handle and store credit cards securely. Internet-based frauds, such as online credit card scams, are gaining popularity due to their inherent characteristics. In these online frauds, transactions are conducted remotely, requiring only the card details without the need for manual signatures, PINs, or card imprints 1 during purchase. Often, the legitimate cardholder remains unaware that their card information has been viewed or stolen by someone else. An effective method for detecting this type of fraud involves analyzing spending patterns for each card and identifying any deviations from the usual

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

spending patterns. Analyzing the historical purchase data of cardholders is considered the most effective method for reducing the occurrence of successful credit card frauds. Transactions conducted using payment cards, including credit cards, prepaid cards, debit cards, and smartphones, are classified as fraudulent if unauthorized. Credit card fraud is characterized as unauthorized account activity by individuals not intended to use the account. Operationally, this refers to an event where action can be taken to halt ongoing abuse and implement risk management measures to prevent similar incidents in the future. Credit card fraud occurs when an individual uses someone else's credit card without the knowledge of both the cardholder and the card issuer. Methods for detecting fraud are devised to prevent such unlawful activities by offenders. However, the development of new fraud detection techniques is hindered by the scarcity of innovative ideas in this field, exacerbated by limited access to datasets and undisclosed results. Detecting fraudulent cases relies on available datasets, often referred to as logged data, and user behavior analysis. Currently, various methods, including data mining, statistical analysis, and artificial intelligence, are utilized for fraud detection.

II. LITERATURE SURVEY

Detecting fraud is a complex endeavor, and there is no foolproof system capable of accurately predicting every fraudulent transaction. Key attributes of an effective fraud detection system include: Accurate identification of fraudulent activities. Swift detection of fraudulent behavior. Avoidance of misclassifying transactions as fraudulent. legitimate Outlier detection plays a crucial role, as outliers signify abnormal operating conditions that could lead to significant performance degradation. Techniques employed in fraud detection can be categorized into two types: Supervised techniques utilize past instances of known legitimate and fraudulent cases to construct a model that generates suspicion scores for new transactions. Unsupervised techniques involve scenarios where no prior sets of known fraudulent or legitimate transactions exist.

III. TYPES OF FRAUD

This paper addresses various types of fraud, including credit card fraud, telecommunication fraud, computer intrusions, bankruptcy fraud, theft/counterfeit fraud, application fraud, and behavioral fraud.

Credit Card Fraud: This type of fraud is categorized into two forms: offline fraud, which involves using a stolen physical card at any location, and online fraud, which occurs over the internet, phone, or during online shopping when the cardholder is not physically present.

Telecommunication Fraud: This involves the misuse of telecommunication services to perpetrate other forms of fraud, affecting consumers, businesses, and communication service providers.

Computer Intrusion: Intrusion refers to the unauthorized attempt to access or manipulate information within a computer system. Intruders, whether external hackers or insiders familiar with the system, pose a threat to information security.

Bankruptcy Fraud: This type of fraud entails using a credit card without the cardholder's presence, presenting a complex challenge for prediction due to its intricate nature.

Theft Fraud/Counterfeit Fraud: This section examines theft and counterfeit fraud, which are interconnected. Theft fraud involves unauthorized usage of a card by someone other than the owner. Prompt feedback from the owner to the bank triggers measures to swiftly address the theft. Similarly, counterfeit fraud occurs when credit card details alone are utilized remotely for transactions.

Application Fraud: Application fraud occurs when individuals apply for a credit card using false information. Detecting application fraud involves categorizing two distinct scenarios: duplicates, where multiple applications originate from the same user with identical details, and identity fraudsters, where applications come from different individuals with similar details. According to Phua et al. [4], application fraud involves the use of possible, synthetic (identity fraud), or real but stolen identity information in application forms, demonstrating identity crime.

Internal Fraud: Within the banking sector, employees have access to customer data, which includes the information necessary for accessing customer accounts through online banking. This accessibility makes it possible for employees to commit fraud easily. To mitigate this risk, financial institutions should implement measures such as requiring a password or PIN for accessing net banking, with the passwords or PINs stored in encrypted formats.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

IV. OVERVIEW OF SOLUTIONS FOR ADDRESSING FRAUD

Dealing with credit card fraud and identity theft should be approached with personal concern and financial vigilance. These instances can lead to significant frustration. How to Handle Credit Card Fraud: Fraud entails the unauthorized use of credit card accounts. Typically, fraud is detected when a credit card is lost or stolen, unfamiliar charges appear on the billing statement, inquiries are received about unrecognized transactions, or contact is made by the credit card company's fraud department. If fraud is suspected on the account, immediate contact with the credit card company is necessary. They can assist in verifying the fraud, removing unauthorized charges, closing the account to prevent further fraudulent activities, issuing a new account number and card, and transferring old information to the new account. It's advisable to review one's credit report regularly to ensure there are no additional suspicious activities. In many cases, law enforcement involvement will be coordinated with the financial institution. Addressing Identity Theft: Identity theft is a specific form of fraud where an individual utilizes personal information to establish new accounts or obtain benefits under the cardholder's name. While not as prevalent as other forms of fraud, it can present greater challenges and lead to more serious complications. Signs of identity theft may include failure to receive bills or other mail, receiving credit cards unexpectedly, experiencing unexplained credit denials, receiving communication regarding unfamiliar transactions, or being served with legal notices or warrants unrelated to the cardholder's activities. It's crucial not to dismiss such occurrences as mere mistakes but to thoroughly investigate them to confirm their nature.

V. UNSUPERVISED OUTLIER DETECTION TECHNIQUE

An unsupervised outlier detection technique operates without relying on the availability of labeled data. This approach aims to identify accounts or customers whose behavior deviates significantly from the norm. Unsupervised methods are particularly beneficial in scenarios where there is limited prior knowledge about specific classes of observations within a dataset. One advantage of employing unsupervised methods over supervised ones is the potential to uncover previously undetected types of fraud. Various techniques currently utilized included.

VI. PEER GROUP ANALYSIS (PGA)

Peer Group Analysis (PGA) is an unsupervised technique utilized in data mining to monitor behavior trends over time. Its primary objective is to identify peer groups for all current target observations or objects. PGA identifies individual objects that exhibit divergent behavior compared to objects they were previously similar to. Each object is selected as a target and compared with all others in the database using either external or internal criteria, summarizing their past behavior patterns. A peer group comprising objects most akin to the target is chosen based on these comparisons. This tool is integral to the data mining process, involving a cyclical approach between detecting objects 3 behaving anomalously and scrutinizing them in detail. In credit card fraud detection, the PGA method is employed by adjusting the length of time windows initially used to establish peer groups.

VII. BREAK POINT ANALYSIS

Break Point Analysis is an additional unsupervised tool utilized for detecting behavioral fraud. A break point refers to an observation or time point used to identify anomalous behavior. This analysis operates at the account level by comparing sequences of transactions to detect changes in behavior for specific accounts. In Break Point Analysis, a fixed- length moving window of transactions is maintained, where each new transaction enters the window while the oldest one is removed. One advantage of Break Point Analysis is that it does not require "balanced" data, as it does not compare transactions across different accounts. This allows for the identification of anomalous sequences of events that may indicate fraudulent behavior

VIII. K-MEANS CLUSTERING TECHNIQUE

K- Means clustering is a straightforward and efficient method for grouping data. Initially, the number of clusters (K) and centroid values are determined. The initial centroids can be any random objects or the first K objects. This technique operates as a non hierarchical method, starting with K objects equal to the final desired number of clusters. The process iterates until stability is achieved (i.e., no object changes groups): Place K points in the space represented by the objects being clustered to serve as initial group centroids. Assign each object to the

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

group with the closest centroid. Once all objects are assigned, recalculate the positions of the K centroids. Repeat steps 2 and 3 until the centroids no longer move. This results in the objects being separated into groups, allowing the calculation of the minimized metric.

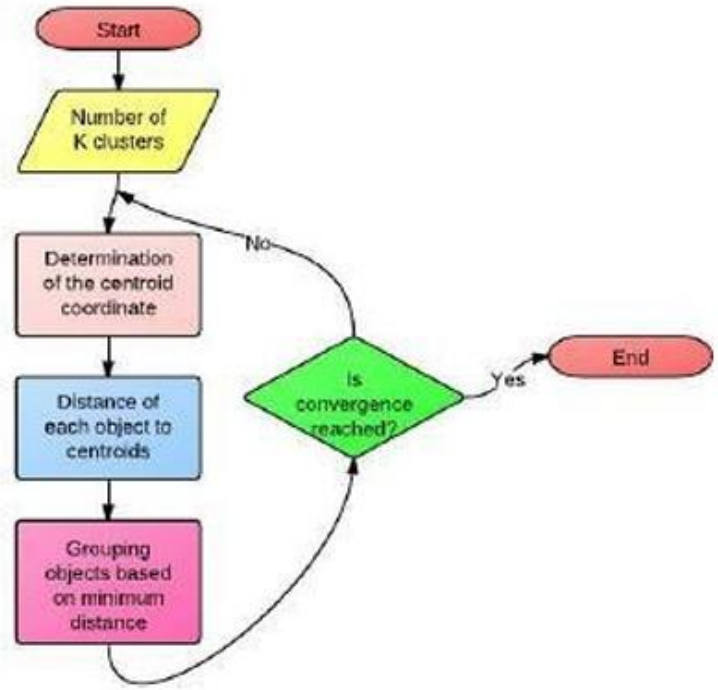

Figure 1: Block Diagram of K- means algorithm process

IX. SUPERVISED OUTLIER DETECTION TECHNIQUE

Supervised outlier detection techniques rely on having access to a dataset containing both normal and outlier classes. These methods are designed to identify fraudulent transactions by distinguishing between accounts or transactions known to be fraudulent and those known to be legitimate. Techniques such as statistical discriminant analysis and neural networks are employed to differentiate between fraudulent and non-fraudulent transactions, assigning suspicion scores to each transaction. Supervised methods are specifically trained to differentiate between legitimate transactions and previously identified instances of fraud. During the literature review on various fraud detection methods, multiple approaches were explored, including the Gass Algorithm, Bayesian Networks, Hidden Markov Model (HMM), Genetic Algorithm (GA), a Fusion approach utilizing Dempster-Shafer Theory and Bayesian learning, Decision Trees, Neural Networks (NN), and Logistic Regression (LR).

Gass Algorithm [2] – The Gass algorithm integrates genetic algorithm and scatter search methodologies. Its fundamental concept revolves around the notion that stronger members of a population have a higher likelihood of survival compared to weaker members. With each successive generation, the average fitness of the population improves. Less fit members of a generation are gradually eliminated, while the fittest members are chosen as parents for the subsequent generation. This iterative process continues until the optimal solution is reached.

Bayesian Networks [2] - In the context of fraud detection, two Bayesian networks are created to characterize user behavior. The first network models behavior assuming the user is fraudulent (F), while the second network is built assuming the user is legitimate (NF). The "fraud net" is developed based on expert knowledge, while the "user net" is established using data from non-fraudulent users. During operation, the user net is customized for a specific user based on current data. By inputting evidence into the networks and propagating it through, probabilities less than two are calculated, indicating the extent to which observed user behavior aligns with typical fraudulent or non - fraudulent behavior. Bayesian networks also facilitate the incorporation of expert knowledge during initial setup, while the user model is iteratively refined in an unsupervised manner using data. Thus, the Bayesian approach combines both expert knowledge and learning.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

Hidden Markov Model [2] - A Hidden Markov Model (HMM) is a doubly embedded stochastic process utilized to model complex stochastic processes. In the context of fraud detection, if an incoming credit card transaction is not accepted by the trained HMM with a sufficiently high probability, it is flagged as a fraudulent transaction [9]. The Baum-Welch algorithm is employed for training purposes, while the K-means algorithm is utilized for clustering. Within the HMM framework, data is organized into clusters based on three price value ranges: low, medium, and high. Initially, probabilities for a set of transactions are chosen, and the Fraud Detection System (FDS) verifies whether each transaction is genuine or fraudulent. HMM's transaction logging capability reduces the workload on employees but also leads to high false alarm rates and high false positives. Therefore, careful selection of initial parameters, which significantly impact algorithm performance, is essential.

Genetic Algorithm [2] - Genetic algorithms, initially conceived by Holland in 1975, are inspired by natural evolution. They serve as evolutionary algorithms that progressively refine solutions over time. In the domain of fraud detection, particularly in E-commerce data mining [10], genetic algorithms (GA) are commonly utilized. Within data mining, GA primarily focuses on variable selection [11] and is frequently combined with other data mining algorithms, resulting in notably effective performance. In credit card fraud detection, GA is employed to reduce the misclassification of transactions, benefiting from its versatility across various programming languages and enhancing its effectiveness. However, this approach demonstrates high performance at a considerable cost.

A Fusion Approach Utilizing Dempster-Shafer Theory and Bayesian Learning [2] - The Dempster-Shafer Theory suggests a Fraud Detection System that integrates information fusion and Bayesian learning. This system combines evidence from both current and past behaviors to establish an activity profile for each cardholder, based on specific shopping behaviors. The benefits of this approach include high accuracy, rapid processing speed, reduced false alarms, improved detection rates, and applicability in E- commerce. However, the main drawback is its high cost. The FDS system comprises four components: a rule-based filter, Dempster–Shafer adder, transaction history database, and Bayesian learner. Transactions are classified as suspicious or legitimate based on their initial characteristics. Once a transaction is flagged as suspicious, its credibility is assessed by comparing it with known fraudulent and genuine transactions.

Decision Tree [2] - Decision trees represent a statistical data mining technique that employs independent attributes and a dependent attribute, which are logically combined in a tree-like structure. The classification rules derived from decision trees are expressed as IF-THEN statements, where all conditions must be met for a rule to be generated. Decision trees typically break down complex problems into simpler ones and address subproblems through iterative analysis. Serving as predictive decision support tools, decision trees establish mappings from observations. Common decision tree methods include C5.0, C&RT, and CHAID. Leveraging data mining techniques such as decision trees and Support Vector Machines (SVMs) for credit card fraud detection aids in mitigating the bank's risk.

Neural Network [2] - Fraud detection approaches utilizing neural networks are widely adopted. An artificial neural network [12] comprises interconnected artificial neurons, drawing inspiration from the brain's functions, particularly in pattern recognition and associative memory [13]. Neural networks identify similar patterns and predict future values or events based on learned patterns stored in associative memory. They find application in classification and clustering tasks. Notably, neural networks excel over other techniques by learning from past data, thus enhancing performance over time. Additionally, they have the capability to extract rules and forecast future activities based on current conditions. The neural network operates through two distinct phases: training and recognition. Training in a neural network refers to the learning process. There are two primary methods for training neural networks: supervised and unsupervised. In supervised training, models are created using samples of both fraudulent and non-fraudulent records. Conversely, unsupervised training identifies transactions that deviate significantly from the norm, without requiring prior knowledge of fraudulent and non-fraudulent transactions in the database. Neural networks are particularly advantageous for handling large transaction datasets.

Logistic Regression [2] - In an effort to detect credit card fraud, logistic regression is utilized alongside support vector machines and random forests, both of which are popular data mining approaches. Logistic regression is well-understood, user-friendly, and commonly employed in data mining, serving as a valuable

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

benchmark for evaluating the performance of newer methods. Supervised learning methods encounter two challenges in fraud detection: Imbalanced class sizes between legitimate and fraudulent transactions, with a vast majority being legitimate. Developing supervised models for fraud that may stem from undetected fraudulent transactions, resulting in mislabeled cases in the data used for model building. To address these challenges, fraudulent transactions are defined as those identified by institutional auditors as causing unauthorized fund transfers from the sponsoring bank of the credit cards. These transactions serve as examples of fraudulent exposure. The study is based on real-life transaction data from an international credit card operation.

X. ANALYSIS OF CURRENT METHODS

Srivastava et al. [1] A model has been developed to illustrate the sequence of credit card transaction processing. Experimental findings highlight the system's effectiveness, showcasing the value of understanding cardholders' spending patterns. Comparative analyses indicate that the system achieves an accuracy rate nearing 80 percent across diverse input data ranges. Accuracy, in this context, refers to the proportion of correctly identified transactions, encompassing both genuine and fraudulent ones. Moreover, the system exhibits scalability to manage substantial transaction volumes.

Suman and Nutan [2] The paper presents an overview of contemporary methodologies utilized for detecting telecommunications credit fraud. card It fraud offers and a comprehensive examination of various fraud detection techniques, encompassing credit card fraud, telecommunication fraud, computer intrusions, bankruptcy fraud, theft/counterfeit fraud, application fraud, and behavioral fraud. The discussed methods for credit card fraud detection include the Gass algorithm, Bayesian networks, Hidden Markov models, genetic algorithms, fusion approaches employing Dempster-Shafer theory and Bayesian learning, decision trees, neural networks, and logistic regression techniques. One of the objectives of this paper is to pinpoint the user model most adept at identifying instances of fraud.

Delamaire et al. [3] Different types of credit card fraud, including bankruptcy fraud, counterfeit fraud, theft fraud, application fraud, and behavioral fraud, have been identified and alternative techniques such as pair-wise matching, decision trees, clustering techniques, neural networks, and genetic algorithms have been reviewed. Furthermore, challenges faced by banks and credit card companies have been outlined. The subsequent phase of this research aims to implement a "suspicious" scorecard on actual data and evaluate its performance. Key objectives include constructing scoring models to forecast fraudulent activity, considering various behavioral aspects associated with the identified types of credit card fraud, and assessing the effectiveness of these models.

Phua et al. [4] A novel fraud detection approach was suggested, drawing inspiration from both existing research in fraud detection and the concept of Minority Report, to address the challenge of skewed data distributions in data mining. Angoss Knowledge Seeker software was utilized for experimentation. The results indicated that success rates X consistently surpassed the averaged success rates W by a minimum margin of 10% on evaluation sets. Additionally, when applied to the score set, bagged success rates Z showed slightly superior performance compared to the averaged success rates Y. Future endeavors will focus on refining classifiers to better suit specific needs.

Esakkiraj and Chidambaram[5] A predictive model has been developed to assess the sequence of operations in online transactions using the Hidden Markov Model (HMM). This model distinguishes between normal user behavior and fraudulent activity. In the trained system, new transactions are evaluated based on transition and observation probabilities. Using the observation probability, the system calculates the acceptance probability and determines whether the transaction should be declined. Unlike traditional fraud detection systems for online banking, which often identify fraudulent transactions after completion, this model predicts fraud during the transaction process, thereby preventing economic losses and enhancing the bank's reputation for security. As a future direction, the study aims to explore more effective classification algorithms in lieu of clustering, which could improve prediction accuracy.

Sahin and Duman [6] The study employs seven classification methods, utilizing decision tree algorithms and Support Vector Machines (SVM), to develop a fraud detection model aimed at enhancing financial transaction systems. It showcases the benefits of employing data mining techniques, particularly decision trees and SVMs,

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

for credit card fraud detection using real-world datasets. The research compares the performance of classifier models constructed with various decision tree methods (C5.0, C&RT, and CHAID) and different SVM methods (with polynomial, sigmoid, linear, and RBF kernel functions). As the volume of training data increases, the overfitting tendencies diminish, and the performance of SVM-based models becomes comparable to decision tree-based models in terms of accuracy. However, SVM models detect fewer fraud cases compared to decision tree models, particularly the C&RT model. Although the C5.0 model demonstrates superior accuracy across samples, the C&RT model identifies the highest number of fraud cases. Consequently, the C&RT and C5.0 models are selected as the final methods for constructing the prediction model. Future research aims to explore alternative data mining algorithms, such as various versions of Artificial Neural Networks (ANN) and logistic regression, to develop new classification models using the same real-world dataset, with a focus on comparing their performance with the models presented in this study.

Bolton and hand [7] This paper delves into two distinct categories of fraud: behavioral fraud and application fraud. However, its primary focus lies in identifying behavioral fraud through the analysis of longitudinal data. It discusses two methods for unsupervised fraud detection in credit card transactions and applies them to real-world datasets. The first method is Peer Group Analysis (PGA), a novel tool for monitoring behavioral patterns over time in data mining contexts. The second method involves Break Point Analysis. The implementation of PGA to detect deviations in credit card account spending behavior is elaborated upon, showcasing its ability to identify outliers through a simulation study. An example is provided, featuring credit card spending data from 858 accounts over a 52-week period, demonstrating how PGA effectively detects unusual spending patterns among accounts with similar spending trends.

Ferdousi and Maeda [8] This paper addresses the challenge of identifying outliers in time series financial data using Peer Group Analysis (PGA), an unsupervised technique for fraud detection. PGA demonstrates its capability to detect brokers who abruptly alter their stock selling behavior compared to previously similar brokers. The experiment evaluates PGA on stock market datasets with continuous values at regular time intervals. Graphical plots of experimental results illustrate PGA's effectiveness in identifying observations that deviate from their peers, supplemented by the application of t-statistics to enhance deviation detection. Future research aims to integrate PGA with other effective methods and extend its application to areas such as banking fraud detection.

Mishra et al. [9] The paper introduces the foundational theory for detecting fraud in credit card transaction processing using a Hidden Markov Model (HMM) and demonstrates its application for fraud detection. Transactions deemed fraudulent are those rejected by the HMM with a sufficiently high probability, while genuine transactions are approved. Various transaction amounts are categorized as observation symbols, and different types of items serve as states within the HMM. A method for establishing the Spending Profile of Cardholders and its utilization in determining observation symbols is proposed. The paper elucidates how the HMM identifies fraudulent transactions and promptly notifies users of detected fraud. In the proposed model, over 85% of transactions are genuine, with a low false alarm rate of approximately 8% of the total transactions. Comparative analyses indicate that the system achieves an accuracy rate nearing 82% across a broad spectrum of input data.

RamaKalyani and UmaDevi [10] They proposal introduces a credit card fraud detection system employing a genetic algorithm. The objective is to devise a method for generating test data and identifying fraudulent transactions through the application of the genetic algorithm. This algorithm, rooted in optimization and evolutionary search principles inspired by genetic and natural selection, serves as a heuristic for solving complex computational challenges. The system leverages this algorithm to analyze credit card transactions promptly, enabling banks to predict the probability of fraudulent transactions soon after they occur.

Chang et al. [11] The authors introduced a fresh learning approach for creating an innovative Intrusion Detection System (IDS) employing Backpropagation Neural Networks (BPN) with sample-query and attribute-query techniques. This paper employs a combination of data reduction and classification, utilizing a query-based learning methodology for its efficiency in time consumption. Experimental results demonstrate that the proposed method's training time is 1447 seconds, significantly less than the training time of the BPN, which

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

exceeds 21746 seconds. Future endeavors aim to expand the application of BPN concepts to develop additional learning methods suitable for a wider array of real-world applications.

Patidar and Sharma [12] In this study, a combination of neural network and genetic algorithm techniques is employed for the detection of fraudulent transactions. For the learning phase of the artificial neural network, a supervised learning feed-forward backpropagation algorithm is utilized. Specifically, a Backpropagation Neural Network (BPN) is employed for training purposes. Subsequently, a genetic algorithm is employed to select key parameters (such as weight, network type, number of layers, and number of nodes) crucial for optimizing neural network performance. By utilizing this integrated Genetic Algorithm and Neural Network (GANN) approach, successful detection of credit card fraud is achieved. Future research endeavors aim to develop systems capable of preemptively controlling credit card fraud prior to any actual transactions taking place.

Subashini and Chitra [13] The study constructed classifier models, including C5.0 and CART decision trees, Support Vector Machines (SVMs) using the Sequential Minimal Optimization (SMO) algorithm with polynomial kernels, Logistic Regression, and Bayesian Network, aimed at detecting fraud in the banking sector using credit card data. Legitimate users are labeled as "good," while fraudulent users are labeled as "bad." C5.0 (using J48), SVM (using SMO), and Bayesian Network achieved a success rate of 72.4%. However, the Bad-to-Good classification is more pronounced in SVM using SMO, indicating that misclassifying a bad customer as good is more detrimental than misclassifying a good customer as bad. Logistic Regression yielded a success rate of 73.1%, while CART achieved the highest success rate at 74.1%. Thus, CART outperforms other models based on success rate, while J48 demonstrates better performance in Bad-to-Good classification. Consequently, employing various classification methods is crucial for making accurate decisions regarding customer classification.

Phua et al. [14] has categorizes, compares and explored almost all published technical and review articles in automated fraud detection. The paper defines the professional fraudster, types and subtypes of fraud, the technical nature of data, performance metrics, methods and techniques. After studying the limitations in methods and techniques of fraud detection, the paper shows that this field can be benefited from other related fields such that the unsupervised approaches from counterterrorism work, actual monitoring systems and text mining from law enforcement, and semi supervised and game-theoretic approaches from intrusion and spam detection communities can contribute to future fraud detection research.

Bagheri et al. [15] The performance of an ensemble comprising three classifiers, each trained on distinct datasets, was assessed. A robust combination strategy rooted in the Dempster-Shafer theory was employed to merge the outputs of these classifiers. The classification outcomes obtained from individual classifiers were contrasted with those derived from fusing the classifiers using the Dempster-Shafer combination method. Employing the DS fusion method notably enhanced the classification performance in comparison to single classifiers trained on specific feature sets.

Maes et al. [16] The paper delves into credit card fraud, its detection, and associated challenges. It provides a concise overview of two machine learning techniques: Artificial Neural Network (ANN) and Bayesian Belief Network (BBN), showcasing their effectiveness on real-world financial data. ANN utilizes backpropagation of error signals, commonly known as backprop. Through conducted experiments, the results of BBN and ANN are compared. It is observed that BBN detects 8% more fraudulent transactions than ANN. BBN outperforms ANN, with a shorter training period of approximately 20 minutes compared to several hours required by ANN. However, ANN detects fraud more swiftly than BBN.

XI. CONCLUSION

In recent years, the prevalence of credit card fraud has escalated, prompting the ongoing development of fraud detection methods to combat evolving criminal tactics. The focus has shifted towards swiftly identifying fraud using advanced detection techniques, facilitating quicker response times. The techniques explored in this study enable rapid detection of credit card fraud, leading to prompt intervention to halt criminal activity. Moving forward, future endeavors will aim to design enhanced techniques surpassing current methodologies.

ACKNOWLEDGEMENT

We express our gratitude to Dr. MGR Educational and Research Institute, Chennai, for their invaluable support and provision of necessary infrastructure for conducting our research. Additionally, we extend our heartfelt thanks to our parents for their unwavering assistance and support throughout this endeavor.

XII. REFERENCES

[1] A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, "Utilizing Hidden Markov Models for Credit Card Fraud Detection," IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 1, January-March 2008.

[2] Suman and Nutan, "A Review 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: An Overview," Banks and Bank Systems, Volume 4, Issue 2, 2009.

[4] Phua, D. Alahakoon, and V. Lee, "Detecting Fraud in Skewed Data: A Minority Report Approach," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.

[5] S. Esakkiraj and S. Chidambaram, "Predictive Fraud Detection Using Hidden Markov Models," International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 1, January 2013.

[6] Y. Sahin and E. Duman, "Credit Card Fraud Detection Using Decision Trees and Support Vector Machines," Proceedings of the 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.

[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 to 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] Ray-I Chang, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang, and Jen Shiang Kouh, "Intrusion Detection with Backpropagation Neural Networks Using Sample-Query and Attribute-Query," Research India Publications, 2006, pp. 6-10.

[11] R. Patidar and L. Sharma, "Neural Network- Based Credit Card Fraud Detection," presented at NCAI2011, May 13-14, 2011, Jaipur, India, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011.

[12] B. Subashini and Dr. K. Chitra, "Enhanced System for Detecting Fraud in Credit Card Approval," International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 8, August 2013, ISSN: 2278-0181.

[13] 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.

[14] M. A. Bagheri, Q. Gao, and S. Escalera, "Logo Recognition Based on Dempster-Shafer Fusion of Multiple Classifiers," Advances in Artificial Intelligence, Lecture Notes in Computer Science, Volume 7884, 2013, pp. 1-12.

[15] S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, "Credit Card Fraud Detection Using Bayesian and Neural Networks," Proceedings of the 1st International NAISO Congress on Neuro Fuzzy Technologies, 2002.