A COMPREHENSIVE ANALYSIS ON DETECTING FRAUD IN FINANCIAL TRANSACTIONS USING MACHINE LEARNING APPROACHES

M.Jayalathalakshmi[1] [1]Research Scholar, Department of Computer Science and Applications,Sri Chandrasekharendra Saraswathi Visa Mahavidyalaya, Deemed to be University Kanchipuram, Tamilnadu, 631561, India. Email- jayalathalakshmi@gmail.com

Dr. S.Prakasam[2] [2]Associate Professor, Sri Chandrasekharendra Saraswathi Visa Mahavidyalaya, Deemed to be University Kanchipuram, Tamilnadu, 631561, India. Email- 2sp@kanchiuniv.ac.in

Abstract

Detecting and preventing fraudulent conduct in financial transactions involves keeping a watch on consumer behavior and transactions. For some businesses, it's also a need for Anti-Money Laundering (AML) compliance and an integral aspect of their loss prevention plan. We used 8 articles for this survey analysis. Artificial Bee Colony (ABC), Principal Component Analysis (PCA), K-Nearest Neighbors (KNN), Logistic Regression, Decision Tree, and Random Forest are some of the Machine Learning approaches included in this survey, which aims to identify instances of financial transaction fraud. In order to improve the detection of relevant patterns for fraud, ABC optimization is used to boost feature selection by imitating the behavior of bees. In order to reduce the number of dimensions, PCA is used. This method anonymise sensitive data while keeping important characteristics. Apply Logistic Regression for likelihood-based transaction classification and KNN for similarity metrics. Random Forest is an ensemble technique that combines several decision trees to enhance prediction accuracy and reduce over-fitting, in contrast to Decision Trees that partition data into branches based on the importance of attributes. It's a basic yet effective model. The assessment highlights the algorithms' strengths and shortcomings in identifying fraudulent financial transactions by comparing their performance and efficacy.

Keywords: Financial Transactions, Fraud Detection, Machine Learning, Credit card

1. INTRODUCTION

The use of credit cards for online purchases is now fundamental to the success of online marketplaces, as they enable customers to buy products and services instantly from any location using any Internet-enabled device, whether it a smart-phone, tablet, or desktop computer. Customers' credit card information is vulnerable to fraud due to the obvious threats connected with this activity. A portion of electronic payments made via the Internet are associated with fraud, according to a new study from the European Payments Council (Afriyie, J. K., et al. 2023). Researchers have been working on models based on AI, data mining, fuzzy logic, and machine learning in an effort to detect different fraudulent activity in credit card transactions. All of the aforementioned solutions have the same objective of avoiding credit card fraud, but each option has its own pros and cons. In order to identify fraudulent purchases made with credit cards, this study analyze the data using supervised machine learning algorithms (Devi, J. V., & Kavitha, K. S. 2017).

Fraudulent transactions have recently surged, which has a major influence on economies. The widespread use of e-commerce and online buying puts customers' vital information, like credit card passwords and CVV numbers, at persistent risk and vulnerability (Geetha, N., & Dheepa, G. 2022). Criminals easily obtain crucial data, which allows them to ramp up their activities. These internet deceitful practices can impact financial systems. With an increase in fraud cases comes an increase in

identity theft via social media. The first, prevention, acts as a barrier to ward off fraudulent assaults; the second, detection, is the more important tactic in the fight against CCF. Detections happen when preventions don't work. Consequently, detections aid in the prompt identification and notification of problems. A combination of human interaction and automated tools connected with academic degrees is a typical fraud detection system.

The overall number of electronic payment transactions in Europe has risen at an organic rate of 9.7 percent each year since 2018, according to the European Central Bank (ECB). From an AI standpoint, the complicated and intriguing problem of bank card fraud is of paramount importance to both consumers and financial institutions. All see that poor fraud management lead to disastrous results (Itri, B., et al. 2021). Credit cards have numerous uses and advantages when used safely and properly. However, fraud is the intentional use of misleading information or outright deceit to acquire an unfair advantage over another party. Consumers and financial institutions alike rest easy knowing that Credit Card Fraud Detection (CCFD) systems are in place to spot and stop fraudulent purchases made using credit cards (Salim, A., et al. 2024).

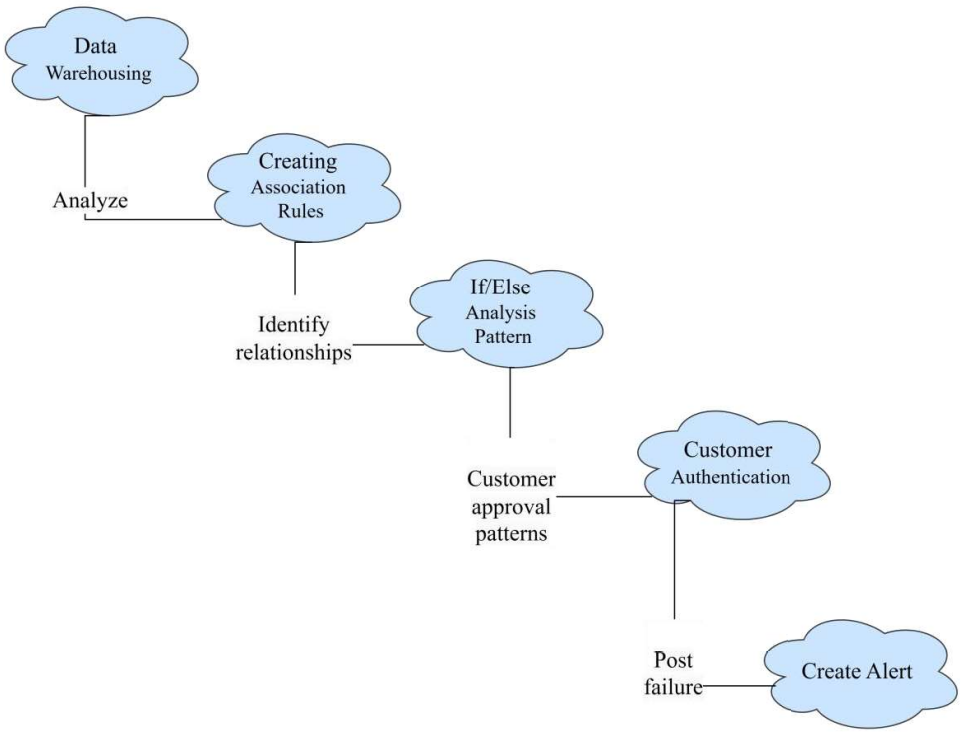

Figure 1: Fraud Detection

Data analysis used to identify fraudulent behavior, as shown in the flowchart. Data warehousing is the first step, which involves collecting and analyzing data. The next step in finding data linkages is to create association rules. The approval patterns of customers are used to analyze their behavior using an If/Else Analysis Pattern. The procedure proceeds to Customer Authentication in order to confirm identification in the event that Authentication fails. An alert is sent out to identify any questionable behavior that might indicate fraud.

2. BACKGROUND STUDY

Afriyie, J. K., et al. (2023) these authors used three distinct supervised machine learning classification models—Logistics Regression, Decision Tree, and Random Forest—to determine whether or not a certain online credit card transaction constituted fraud. These authors balanced the dataset before creating the models using the under sampling strategy to make sure the model doesn't favor the majority class and to avoid over-fitting the data. In terms of accuracy (96.0%), area under the curve (98.9%), and performance relative to the other two models, the Random Forest model emerged as the clear winner when it came to predicting fraudulent transactions.

Alarfaj, F. K., et al. (2022) Banks and other financial institutions face increased Credit Card Fraud (CCF) risk. Scammers are known for creating new deceptions. Strong classifiers handle dynamic fraud. The goal of a fraud detection system should be to properly predict fraud and reduce false positives.

Dalal, S., et al. (2022) Banks need to develop stronger fraud detection and control strategies due to the exponential growth in transaction volumes caused by newly implemented digital-only and online payment and banking systems.

Devi, J. V., & Kavitha, K. S. (2017) several machine learning-based classification methods used in data mining are the subject of this paper's investigation.

Geetha, N., & Dheepa, G. (2022) Artificial Bee Colony (ABC) and Enhanced Neural Network (ENN) are used to offer a transaction-based fraud detection technique. A more current profile of the cardholder's behavior created using comparable cardholder patterns.

Table 1: Comparison on performance metrics of various algorithms used in Fraud Detection in Financial Transactions

Study	Model/Classifier	Accuracy (%)	Area Under Curve (AUC)	Precision (%)
Afriyie et al. (2023)	Logistic Regression	92.5	95.4	92
	Decision Tree	93.1	96.2	93.3
	Random Forest	96	97.9	95.8
Dalal et al. (2022)	Modified XGBoost	97.64	94.2	97.2
Salim et al. (2024)	Random Forest Classifier (RFC)	96.2	96.7	97.3
	Extra Trees Classifier (ETC)	97.3	97.1	98.5
	Gradient Boosting Classifier (GBC)	98.5	94.5	96.95
	Support Vector Machine (SVM)	98.8	95.4	97.9

Table 2: Comparison on algorithms used in Fraud Detection in Financial Transactions

Study	Focus	Methods Used	Key Findings
Devi & Kavitha (2017)	Classification methods for credit card fraud	Support Vector Machine (SVM), Random Forest, Decision Tree	Explored advantages and disadvantages of each classification method. Performance varies depending on data characteristics.
Geetha & Dheepa (2022)	Transaction-based fraud detection	Artificial Bee Colony (ABC), Enhanced Neural Network (ENN)	Proposed a method using ABC for feature selection; showed improved efficiency in detecting fraudulent transactions.
Itri et al. (2021)	Handling unbalanced data for fraud detection	Hybrid algorithm (Borderline, Optimal Learning Strategy (OLS), Random Forest)	Demonstrated significant performance enhancement through oversampling techniques; optimal algorithm combinations yielded better results.
Jagannath et al. (2021)	Predicting Bitcoin prices	Joint Self-Optimization (jSO) algorithm	Achieved high prediction accuracy for Bitcoin prices using a self-adaptive parameter approach.
Alarfaj et al. (2022)	Fraud detection in credit cards	Deep Learning (CNN) and various Machine Learning techniques	Highlighted the need for strong classifiers to reduce false positives; CNNs outperformed traditional algorithms in credit card detection.

3. CONCLUSION

In Conclusion, we used 8 research articles for this survey, research improves credit card fraud detection using Artificial Bee Colony (ABC) optimization, which mimics honey bee foraging. Principal Component Analysis (PCA) anonymised all features except the transaction index and time once the time feature was changed from seconds to minutes and hours. Rather than all available traits, features are chosen depending on their relevance to certain classes. Using Artificial Bee Colony (ABC) optimization—which replics honey bee foraging—this study enhances credit card fraud detection. Using the ABC approach, bees are separated into worker and scout types, therefore facilitating the search for optimal solutions. It uses rules from numerous randomly built decision trees to vote on the most common guess and explore input transaction characteristics.

V REFERENCE

[1]. J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, and J. Eshun, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, p. 100163, 2023.

[2]. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022.

[3]. S. Dalal, B. Seth, M. Radulescu, C. Secara, and C. Tolea, "Predicting fraud in financial payment services through optimized hyper-parameter-tuned XGBoost model," *Mathematics*, vol. 10, no. 24, p. 4679, 2022.

[4]. J. V. Devi and K. S. Kavitha, “Fraud detection in credit card transactions by using classification algorithms,” in *Proc. 2017 Int. Conf. on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, Mysore, India, Sep. 2017, pp. 125–131.

[5]. N. Geetha and G. Dheepa, “Transaction fraud detection using Artificial Bee Colony (ABC) based feature selection and Enhanced Neural Network (ENN) classifier,” *Int. J. Mech. Eng.*, vol. 7, no. 3, 2022.

[6]. B. Itri, Y. Mohamed, B. Omar, and Q. Mohamed, “Composition of feature selection methods and oversampling techniques for banking fraud detection with artificial intelligence,” *Int. J. Eng. Trends Technol.*, vol. 69, no. 11, pp. 216–226, 2021.

[7]. N. Jagannath, T. Barbulescu, K. M. Sallam, I. Elgendi, A. A. Okon, B. McGrath, and K. Munasinghe, “A self-adaptive deep learning-based algorithm for predictive analysis of bitcoin price,” *IEEE Access*, vol. 9, pp. 34054–34066, 2021.

[8]. A. Salim, S. N. Mjeat, D. A. Q. Shakir, and M. A. Alfwair, “Credit card fraud detection model based on correlation feature selection,” *J. Cybersecurity & Inf. Manag.*, vol. 14, no. 2, 2024.