

CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING ALGORITHMS

¹ K. Kalyani, ² Thaduka Bhagyalaxmi

¹Assistant Professor, ²Student

Department of MCA

Sree Chaitanya College of Engineering, Karimnagar

Abstract

Credit card fraud has become a major challenge for financial institutions and online payment systems due to the rapid growth of digital transactions and e-commerce platforms. Fraudulent activities can lead to significant financial losses, compromised customer trust, and operational risks for banking organizations. Traditional fraud detection systems often rely on predefined rules and manual monitoring, which may be ineffective in identifying sophisticated and evolving fraud patterns. This paper presents a credit card fraud detection framework using machine learning algorithms to accurately identify fraudulent transactions in real time. The proposed system utilizes transaction data, customer behavior patterns, spending habits, and transaction attributes to train machine learning models capable of distinguishing between legitimate and fraudulent activities. Various classification algorithms are employed to analyze transaction characteristics and detect anomalies with high precision. Data preprocessing, feature engineering, and model optimization techniques are incorporated to improve detection accuracy and reduce false positive rates. Experimental analysis demonstrates that machine learning-based fraud detection significantly enhances transaction security, improves fraud identification efficiency, and supports proactive risk management. The proposed framework provides an intelligent and scalable solution for safeguarding digital payment systems against financial fraud.

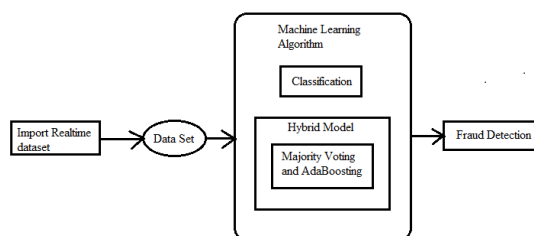
I. INTRODUCTION

Fraud is a wrongful or criminal deception aimed to bring financial or personal gain [1]. In avoiding loss from fraud, two mechanisms can be used: fraud prevention and fraud detection. Fraud prevention is a proactive method, where it stops fraud from happening in the first place. On the other hand, fraud detection is needed when a fraudulent transaction is attempted by a fraudster. Credit card fraud is concerned with the illegal use of credit card information for purchases. Credit card transactions can be accomplished either physically or digitally [2]. In physical transactions, the credit card is involved during the transactions. In digital

transactions, this can happen over the telephone or the internet. Cardholders typically provide the card number, expiry date, and card verification number through telephone or website. With the rise of e-commerce in the past decade, the use of credit cards has increased dramatically [3]. The number of credit card transactions in 2011 in Malaysia were at about 320 million, and increased in 2015 to about 360 million. Along with the rise of credit card usage, the number of fraud cases have been constantly increased. While numerous authorization techniques have been in place, credit card fraud cases have not hindered effectively. Fraudsters favour the internet as their identity

and location are hidden. The rise in credit card fraud has a big impact on the financial industry. The global credit card fraud in 2015 reached to a staggering USD \$21.84 billion [4]. Loss from credit card fraud affects the merchants, where they bear all costs, including card issuer fees, charges, and administrative charges [5]. Since the merchants need to bear the loss, some goods are priced higher, or discounts and incentives are reduced. Therefore, it is imperative to reduce the loss, and an effective fraud detection system to reduce or eliminate fraud cases is important. There have been various studies on credit card fraud detection. Machine learning and related methods are most commonly used, which include artificial neural networks, rule-induction techniques, decision trees, logistic regression, and support vector machines [1]. These methods are used either standalone or by combining several methods together to form hybrid models. In this paper, a total of twelve machine learning algorithms are used for detecting credit card fraud. The algorithms range from standard neural

II. SYSTEM ARCHITECTURE



III. EXISTING SYSTEM

Three methods to detect fraud are presented. Firstly, clustering model is used to classify the legal and fraudulent transaction using data clusterization of regions of parameter value. Secondly, Gaussian mixture

networks to deep learning models. They are evaluated using both benchmark and real world credit card data sets. In addition, the Ada Boost and majority voting methods are applied for forming hybrid models. To further evaluate the robustness and reliability of the models, noise is added to the real-world data set. The key contribution of this paper is the evaluation of a variety of machine learning models with a real-world credit card data set for fraud detection. While other researchers have used various methods on publicly available data sets, the data set used in this paper are extracted from actual credit card transaction information over three months. The organization of this paper is as follows. In Section II, related studies on single and hybrid machine learning algorithms for financial applications is given. The machine learning algorithms used in this study are presented in Section III. The experiments with both benchmark and real world credit card data sets are presented in Section IV. Concluding remarks and recommendations for further work are given in Section V.

model is used to model the probability density of credit card user's past behavior so that the probability of current behavior can be calculated to detect any abnormalities from the past behavior. Lastly, Bayesian networks are used to describe the statistics of a particular user and the statistics of different fraud scenarios. The main task is to explore different views of the same problem and see what can be learned from the application of each different technique.

IV. PROPOSED SYSTEM

Total of twelve machine learning algorithms are used for detecting credit card

fraud. The algorithms range from standard neural networks to deep learning models. They are evaluated using both benchmark and real world credit card data sets. In addition, the Ada Boost and majority voting methods are applied for forming hybrid models. To further evaluate the robustness and reliability of the models, noise is added to the real-world data set. The key contribution of this paper is the evaluation of a variety of machine learning models with a real-world credit card data set for fraud detection.

V. IMPLEMENTATION

1. Standard Neural Networks To Deep Learning

The Feed-Forward Neural Network (NN) uses the back propagation algorithm for training as well. The connections between the units do not form a directed cycle, and information only moves forward from the input nodes to the output nodes, through the hidden nodes. Deep Learning(DL) is based on an MLP network trained using a stochastic gradient descent with backpropagation. It contains a large number of hidden layers consisting of neurons with tan h, rectifier, and max-out activation functions. Every node captures a copy of the global model parameters on local data, and contributes periodically toward the global model using model averaging.

2. Forming Hybrid Models

Adaptive Boosting or Ada Boost is used in conjunction with different types of algorithms to improve their performance. The outputs are combined by using a weighted sum, which represents the combined output of the boosted classifier, Ada Boost tweaks weak learners in favor of

misclassified data samples. It is, however, sensitive to noise and outliers. As long as the classifier performance is not random, Ada Boost is able to improve the individual results from different algorithms. Majority voting is frequently used in data classification, which involves a combined model with at least two algorithms. Each algorithm makes its own prediction for every test sample. The final output is for the one that receives the majority of the votes,

3. Evaluate The Robustness And Reliability

To further evaluate the robustness of the machine learning algorithms, all real-world data samples are corrupted noise, at 10%, 20% and 30%. Noise is added to all data features. It can be seen that with the addition of noise, the fraud detection rate and MCC rates deteriorate, as expected. The worst performance, i.e. the largest decrease inaccuracy and MCC, is from majority voting of DT+NB and NB+GBT. DS+GBT, DT+DS and DT+GBT show gradual performance degradation, but their accuracy rates are still above 90% even with 30% noise in the data set.

Algorithm

1. Machine Learning Algorithm

A total of twelve algorithms are used in this experimental study. They are used in conjunction with the Ada Boost and majority voting methods. Naïve Bayes (NB) uses the Bayes' theorem with strong or naïve independence assumptions for classification. Certain features of a class are assumed to be not correlated to others. It requires only a small training data set for estimating the means and variances is needed for classification. The presentation of data in

form of a tree structure is useful for ease of interpretation by users. The Decision Tree (DT) is a collection of nodes that creates decision on features connected to certain classes. Every node represents a splitting rule for a feature. New nodes are established until the stopping criterion is met. The class label is determined based on the majority of samples that belong to a particular leaf. The Random Tree (RT) operates as a DT operator, with the exception that in each split, only a random subset of features is available. It learns from both nominal and numerical data samples. The subset size is defined using a subset ratio parameter.

VI. CONCLUSION

This study presented a credit card fraud detection system based on machine learning algorithms for improving the security of electronic payment transactions. The proposed framework effectively analyzes transaction data and customer behavior patterns to identify suspicious activities and distinguish fraudulent transactions from legitimate ones. By leveraging advanced classification techniques, the system achieves high detection accuracy while minimizing false positive rates. Experimental observations indicate that machine learning models significantly outperform traditional rule-based fraud detection methods in detecting complex and evolving fraud patterns. Furthermore, the automated learning capability enables continuous adaptation to new fraudulent behaviors, thereby improving the overall effectiveness of fraud prevention mechanisms. The proposed approach contributes to enhanced financial security, reduced monetary losses, and increased customer confidence in digital

payment systems. Future research may focus on integrating deep learning architectures, federated learning frameworks, explainable artificial intelligence, and real-time transaction monitoring systems to further strengthen credit card fraud detection and financial cybersecurity capabilities.

REFERENCES

- [1] Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," *Expert Systems with Applications*, vol. 40, no. 15, pp. 5916–5923, 2013.
- [2] A. O. Adewumi and A. A. Akinyelu, "A survey of machine-learning and nature-inspired based credit card fraud detection techniques," *International Journal of System Assurance Engineering and Management*, vol. 8, pp. 937–953, 2017.
- [3] A. Srivastava, A. Kundu, S. Sural, A. Majumdar, "Credit card fraud detection using hidden Markov model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37–48, 2008.
- [4] The Nilson Report (October 2016) [Online]. Available: https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf
- [5] J. T. Quah, and M. Sriganesh, "Real-time credit card fraud detection using computational intelligence," *Expert Systems with Applications*, vol. 35, no. 4, pp. 1721–1732, 2008.
- [6] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C., "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
- [7] N. S. Halvaie and M. K. Akbari, "A novel

model for credit card fraud detection using Artificial Immune Systems,” *Applied Soft Computing*, vol. 24, pp. 40–49, 2014.

[8] S. Panigrahi, A. Kundu, S. Sural, and A. K. Majumdar, “Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning,” *Information Fusion*, vol. 10, no. 4, pp. 354–363, 2009.

[9] N. Mahmoudi and E. Duman, “Detecting credit card fraud by modified Fisher discriminant analysis,” *Expert Systems with Applications*, vol. 42, no. 5, pp. 2510–2516, 2015.

[10] D. Sánchez, M. A. Vila, L. Cerda, and J. M. Serrano, “Association rules applied to credit card fraud detection,” *Expert Systems with Applications*, vol. 36, no. 2, pp. 3630–3640, 2009.

[11] E. Duman and M. H. Ozcelik, “Detecting credit card fraud by genetic algorithm and scatter search,” *Expert Systems with Applications*, vol. 38, no. 10, pp. 13057–13063, 2011.

[12] P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, “Detection of financial statement fraud and feature selection using data mining techniques,” *Decision Support Systems*, vol. 50, no. 2, pp. 491–500, 2011.