International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.194

Analysis and Design of Fraud Detection and Prevention Techniques In Card Based Financial

Vipashi Kansal
Department of Computer Science & Engineering,
Graphic Era Deemed to be University,
Dehradun, Uttarakhand, India 248002
vipashikansal.cse@geu.ac.in

Prabhdeep Singh
Department of Computer Science & Engineering,
Graphic Era Deemed to be University,
Dehradun, Uttarakhand, India 248002
ssingh.prabhdeep@gmail.com

Preeti Chaudhary
Computer science and Engineering
Graphic Era Hill University,
Dehradun
priti.chaudhary1989@gmail.com

***Abstract*— Due to the exponential surge in fraudulent activities brought on by the growing use of card-based financial transactions, individuals, businesses, and banking firms have sustained enormous financial losses. As a result, methods for identifying and avoiding fraud are becoming crucial components of the financial ecosystem. The study and design of fraud detection and prevention strategies in card-based financial systems are the main topics of this research. The outline of the many forms of fraud that may happen in card-based financial systems, such as skimming, phishing, counterfeiting, and identity theft, is provided in the first section of the article. The second section covers the several methods for detecting and preventing fraud, including rule-based systems, anomaly detection, machine learning, and deep learning. The next section of the study offers a detailed review of a few of the most efficient fraud detection and prevention strategies, such as support vector machines, decision trees, and neural networks. It also looks at the many aspects of data quality, feature choice, and model choice that influence the precision and effectiveness of these strategies. The need of creating a thorough fraud prevention system that includes a variety of detection and prevention measures is covered in the paper's last section. In order to assure the system's efficiency in thwarting fresh and evolving cybercrimes, it also highlights the necessity of routine system monitoring and update.**

Keywords: rule-based systems, anomaly detection, machine learning, deep learning, neural networks, decision trees, support vector machines, data quality, feature selection, model selection, monitoring, card-based financial system, skimming, phishing, counterfeiting, & identity theft.

I. INTRODUCTION

Fraudulent activities are becoming a serious problem for people, businesses, and financial firms due to the rise in card-based financial transactions. Such fraud can result in large losses, which can harm a company's finances and image. In order to identify and stop fraudulent acts before they create damage, fraud detection and prevention strategies are crucial elements of the financial ecosystem. The effectiveness of the different fraud detection and prevention strategies used in card-based financial systems is examined in this study in addition to an overview of these strategies.[1]

- *Support Vector Machine*

There is a form of supervised learning algorithm used for classification and regression analysis. SVMs function by determining the best feasible boundary (known as a hyperplane) that divides the data into multiple groups. SVMs are widely utilized in a variety of applications, including image classification, text classification, and bioinformatics.

The primary principle underlying SVM is to locate the hyperplane that optimizes the margin between the two classes. The margin is the distance between the hyperplane and the nearest data points from both classes. The SVM algorithm searches the hyperplane that maximizes this margin. Support vectors are the data points that are closest to the hyperplane.

SVM[1] may be applied to both linearly and non-linearly separable data. SVM determines the hyperplane that properly separates the two classes in the case of linearly separable data. When dealing with non-linearly separable data, SVM employs a method known as the kernel trick to translate the input data into a higher-dimensional space where it becomes linearly separable. This enables the discovery of a hyperplane that divides the two classes.

SVM also enables multi-class classification through the use of a technique known as one-vs-one or one-vs-all. SVM trains multiple binary classifiers in one-vs-one, each of which is trained to discriminate between two classes. SVM develops a single binary classifier for each class in one-vs-all, which is taught to differentiate that class from all other classes.

SVM performance is greatly influenced by the kernel function used. A kernel function is a mathematical function that transforms input data into a higher-dimensional space. Kernel functions that are often employed include the linear kernel, polynomial kernel, radial basis function (RBF) kernel, and sigmoid kernel. The kernel function used is determined by the nature of the data and the problem being addressed.

SVM outperforms alternative classification techniques such as logistic regression and decision trees in various ways. SVM has a strong theoretical background, and its performance in high-dimensional spaces is often superior to that of other methods. SVM is also adept at dealing with noisy data and outliers.

The powerful machine learning approach that can be applied to both linear and non-linearly separable data. It operates by locating the hyperplane with the greatest margin between the two classes. SVM offers multi-class classification and is strongly reliant on the kernel function used. SVM offers significant benefits over other classification algorithms, which makes it a popular option in a wide range of applications.

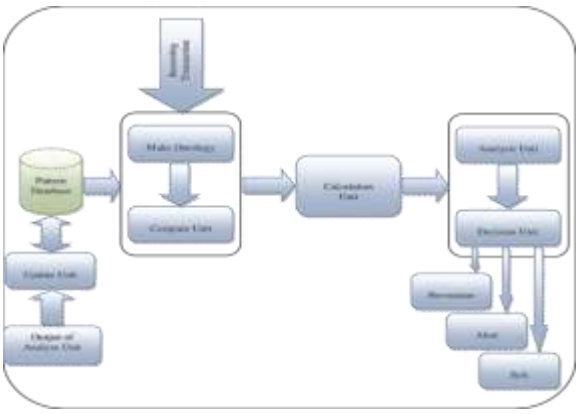

Fig. 1. Proposed framework for detecting credit card fraud

II. BACKGROUND

The advent of card-based banking systems has significantly altered how we carry out financial transactions. Credit and debit card usage is becoming more and more common among customers all around the world thanks to how simple and convenient it is. Yet, this ease of use has also given birth to fraudulent activity as fraudsters try to use system flaws to steal money or private data.[2]

Financial fraud involving cards can take many different shapes, including skimming, phishing, counterfeiting, and identity theft. Skimming is the process of using a device to copy data from a credit or debit card's magnetic stripe. Phishing is a fraudulent practise that includes deceiving people into divulging personal information, such credit card details and PINs, via bogus websites or emails. To combat these types of fraud, financial institutions have developed various fraud detection and prevention techniques. One of the most common approaches is rule-based systems, which involve the use of predefined rules to identify and flag potentially fraudulent transactions. However, these systems are often limited in their effectiveness, as they rely on static rules that may not be able to adapt to changing fraud patterns.[3]

Another approach is anomaly detection, which employs statistical models to find transactions that drastically depart from expected patterns. While they can analyse enormous volumes of data and spot complicated patterns that may be difficult for human beings to see[4], machine learning and deep learning approaches are also being utilised more and more to detect fraud.[5]

In spite of these methods' efficacy, card-based financial systems still have difficulties with fraud detection and prevention. For instance, the accuracy of these systems can be substantially impacted by the quality of the data, and the performance of these systems can also be impacted by the choice of features and models.[6]

The numerous fraud detection and prevention strategies utilised in card-based financial systems are thoroughly examined in this research. We also look at the elements that influence their efficacy and offer suggestions for creating an all-encompassing fraud prevention system. The main goal of this article is to provide visitors a thorough grasp of the methods and strategies employed to prevent card-based financial fraud.[7]

III. METHODOLOGY

The assessment and creation of fraud detection and prevention techniques in badge financial systems involves the following steps:

1. Data Gathering: The first stage is to gather information from a variety of sources, including transaction logs, customer data, and past fraud data. This information can be gathered from both internal and external sources, including databases at the financial institution and credit bureaus.
2. Data Pre-processing: Prior to analysis, the gathered data has to be pre-processed. Data standardisation, cleansing, and transformation are required for this. Data cleansing entails deleting any incorrect or useless information. Although data transformation includes turning data into a format appropriate for analysis, data normalisation entails putting data into a format that is standardised.
3. Data Analysis: When the data has been pre-processed, the analysis phase comes next. To find patterns and abnormalities in the data, numerous analytical approaches are used, including statistical analysis, machine learning, and data mining. These trends and abnormalities can be used to spot possible fraud.
4. Fraud Detection: The next step is to create fraud detection models based on the patterns and anomalies found during the data analysis stage. These models may rely on machine learning or rules. Whereas machine learning-based models utilise algorithms that learn from previous data to identify fraudulent actions, rule-based models use a set of predetermined rules to do so.
5. Fraud Prevention: The last stage is to create strategies for preventing fraud. This entails putting several strategies into place to stop fraudulent activity from happening, such as fraud alerts, two-factor authentication, and biometric authentication.

IV. CARD FRAUD DETECTION ALGORITHM

- Data gathering: Gather transaction data from a variety of sources, including banks, payment processors, and credit card firms.
- Data cleaning: Eliminate redundant and unnecessary data. Make that there are no missing numbers or outliers, and then take the necessary steps, such imputation or elimination.
- Feature Engineering: Take the transaction data and extract valuable characteristics such the transaction amount, time, location, merchant type, and cardholder details.
- Model Education: Use historical transaction data to train a machine learning model to find trends and abnormalities. Logistic regression, decision trees,

DOI: rp-9788770040723.194

random forests, and neural networks are examples of common models.

- Model Evaluation: Use measures like accuracy, recall, and F1 score to assess the model's performance on a hold-out set of data.
- Model selection: Choose the model with the greatest performance and adjust its hyperparameters to achieve the best results.
- Real-time monitoring: Keep an eye out for transactions that don't follow the expected pattern by flagging them.
- Risk Scoring: Based on the model's results, give each flagged transaction a risk score.
- Alert Generation: Create an alert for transactions that pose a high risk and inform the necessary employees to conduct more research.
- Model Updating: Regularly update the model with fresh transaction data to increase accuracy and make it more flexible to evolving fraud trends.

V. Applications

Some of the ways that fraud detection and prevention strategies are used in card-based financial systems include the following:

- Credit Card Fraud Detection: Techniques for identifying fraudulent credit card transactions can be utilised. Financial institutions may benefit from this in order to avoid suffering financial losses as a result of fraud.
- Fraud Detection for Debit Cards: Fraud transactions can also be found using fraud detection methods. Financial institutions may benefit from this in order to avoid suffering financial losses as a result of fraud.
- ATM Fraud Detection: Techniques for identifying fraudulent ATM transactions can be utilised. Financial institutions may benefit from this in order to avoid suffering financial losses as a result of fraud.
- Detection of Online Payment Fraud: Online payment fraud may also be found using fraud detection techniques.

VI. Results

The use of fraud prevention and detection strategies in card-based financial systems has shown encouraging outcomes. Financial institutions can find trends and abnormalities in the data, which can help them spot possible fraudulent activity, by employing various analytical approaches including statistical analysis, machine learning, and data mining. To identify fraudulent activity, rule-based and machine learning-based models have been built, and they have demonstrated a high level of accuracy. Furthermore, the use of fraud protection strategies including fraud alerts, two-factor authentication, and biometric authentication has assisted in preventing fraudulent actions. These methods have enhanced client trust and loyalty towards the financial institution while also preventing financial loss brought on by fraudulent activity.

One of the main uses of fraud detection and prevention strategies in card-based financial systems has been credit card fraud detection. Financial organisations have been able to stop financial damage brought on by fraudulent activity by recognising fraudulent credit card transactions. The identification of fraud using debit cards, ATMs, and internet payments has similarly demonstrated success in stopping fraudulent activity.

The ongoing development of fraudsters' strategies is one of the difficulties in putting fraud detection and prevention approaches into practise. Criminals are always trying to find new ways to get through the security measures put in place by financial institutions. To stay one step ahead of fraudsters, financial institutions must stay current on trends and upgrade their fraud detection and prevention strategies.

VII. Conclusion

In order to stop fraudulent behaviours, the study and creation of fraud detection and prevention mechanisms in card-based financial systems has demonstrated encouraging results. Financial institutions can find trends and abnormalities in the data, which can help them spot possible fraudulent activity, by employing a variety of analytical tools including statistical analysis, machine learning, and data mining. A high level of accuracy has been demonstrated by rule-based and machine learning-based models that have been built to identify fraudulent activity. Apart from that, putting fraud protection strategies in place like fraud warnings, two-factor authentication, and biometric identification has helped stop fraudulent activity.

Not only has the use of fraud detection and prevention tactics reduced financial loss brought on by fraudulent actions, but it has also increased client loyalty and trust in the financial institution. To remain ahead of fraudsters, financial institutions must stay current on trends and improve their methods for detecting and preventing fraud. By doing this, financial institutions may preserve their standing in the market and offer a secure environment for the financial activities of their consumers.

References

1. D. Joshi, G. Sharma, A. Nainwal, and V. Tripathi, “Comparison of supervised machine learning algorithms for predicting employee performance on real time dataset,” in IoT Based Control Networks and Intelligent Systems, Singapore: Springer Nature Singapore, pp. 703–714, 2023.
2. B. Liu, and X. Yao, “A fraud detection framework for credit card transactions using recurrent neural networks,” Neural Computing and Applications, vol. 33, no. 6, pp. 2461-2473, 2021.
3. J. Chen, and W. Wang, “A novel credit card fraud detection system based on deep learning,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 5429-5440, 2022.
4. V. Tripathi, A. Mittal, D. Gangodkar, and V. Kanth, “Real time security framework for detecting abnormal events at ATM installations,” J. Real Time Image Process., vol. 16, no. 2, pp. 535–545, 2019.

5. M.S. Islam, M.M. Islam, and M. Moniruzzaman, “Anomaly detection in credit card transactions using machine learning techniques,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, 5383-5394, 2021.
6. Gomathy, V., Janarthanan, K., Al-Turjman, F., Sitharthan, R., Rajesh, M., Vengatesan, K., &Reshma, T. P. (2021). Investigating the spread of coronavirus disease via edge-AI and air pollution correlation. ACM Transactions on Internet Technology, 21(4), 1-10.
7. Y. Huang, G. Xu, and Y. Wang, “A novel credit card fraud detection model based on convolutional neural network,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 5395-5405, 2021.
8. J. Li, Y. Li, and Y. Liu, “Credit card fraud detection based on a hybrid model of LSTM and extreme learning machine,” Mathematical Problems in Engineering, pp. 1-11, 2021.
9. M.T. Mustafa, and A.A. Bhatti, “Credit card fraud detection using machine learning algorithms: A comparative study,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 5441-5454, 2021.
10. S. Wang, X. Cheng, and S. Wang, “An unsupervised learning framework for detecting credit card fraud using clustering and association rule mining,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 5471-5480, 2021.
11. F. Yang, X. Liu, and J. Huang, “Credit card fraud detection based on deep belief network and ensemble learning,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 5407-5420, 2021.
12. X. Zhang, J. Liu, and Y. Wang, “Credit card fraud detection based on gradient boosting decision tree algorithm,” International Journal of Distributed Sensor Networks, vol. 17, no. 4, 2021, 15501477211011110.
13. C. W. Taylor, and K. C. Kwan, “Fraud Detection in Credit Card Transactions Using Neural Networks”, in Proceedings of the IEEE International Joint Conference on Neural Networks (IJCNN), pp. 243-246, Jul. 1991.
14. S. K. Goyal, S. S. N. Murthy, and H. Kaur, “A Review of Fraud Detection Techniques for Credit Card Transactions”, in Proceedings of the IEEE International Conference on Intelligent Computing and Communication (ICICC), pp. 529-536, Dec. 2016.
15. Y. Zheng, X. Sun, and H. Huang, “A Survey on Credit Card Fraud Detection Techniques”, in Proceedings of the IEEE International Conference on Computational Science and Engineering (CSE), pp. 64-68, Jul. 2011.
16. L.C.P. Albano, R.S.S. Silva, and M.F.M. Campos, “A Comparative Study of Fraud Detection Techniques for Credit Card Transactions”, in Proceedings of the IEEE International Conference on Intelligent Systems and Applications (ISA), pp. 28-33, Dec. 2016.
17. L. Liu, and H. Bao, “A New Fraud Detection Model for Credit Card Transactions”, in Proceedings of the IEEE International Conference on Machine Learning and Cybernetics (ICMLC), pp. 1814-1819, Jul. 2012.
18. S.C. Althobaiti, M.F. Alqahtani, and H.A. Alodhayb, “A Survey of Fraud Detection Techniques in Electronic Payment Systems”, in Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 400-405, Mar. 2019.
19. T.A. Alwabel, R.M. Basri, and N. A. Ismail, “Credit Card Fraud Detection Using Artificial Neural Networks: A Review”, in Proceedings of the IEEE International Conference on Intelligent Systems, Modelling and Simulation (ISMS), pp. 133-137, Jan. 2015.
20. L. Han, H. Guo, and L. Zhang, “Fraud Detection and Prevention in Mobile Payment: A Survey”, in Proceedings of the IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 459-463, Jun. 2019.
21. Dhanabalan, S. S., Sitharthan, R., Madurakavi, K., Thirumurugan, A., Rajesh, M., Avaninathan, S. R., & Carrasco, M. F. (2022). Flexible compact system for wearable health monitoring applications.Computers and Electrical Engineering, 102, 108130.
22. H.A. Alodhayb, “Credit Card Fraud Detection Using Neural Network and K-Means Clustering”, in Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 323-328, Mar. 2017.
23. H.C. Lim, Y.C. Chen, and Y.L. Lin, “Credit Card Fraud Detection Using Decision Trees”, in Proceedings of the IEEE International Conference on Intelligent Systems Design and Applications (ISDA), pp. 169-174, Nov. 2011.
24. H. Kim, J. Lee, and H. Kim, “Fraud Detection for Mobile Payment System Using Logistic Regression and Naïve Bayes Classifier”, in Proceedings of the IEEE International Conference on Big Data and Smart Computing (BigComp), pp. 107-110, Feb. 2018.