International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 10, Issue 4, pp: (1-8), Month: October - December 2022, Available at: www.researchpublish.com

DEBIT AND CREDIT CARD FRAUD DETECTION USING K-N-N IN MACHINE LEARNING

Ahmad Alammar[1], Yazeed Al Moayed[2], Nasir Ahmed Algeelani[3]

Faculty of computer science and Information technology
AL-Madinah International University
Kuala Lumpur, Malaysia

DOI: https://doi.org/ 10.5281/zenodo.7260970

Published Date: 28-October-2022

Abstract: **We have thousands of banks around the world and these banks revenue through a very small profit from each transaction. So from the bank perspective, they have no idea who is performing these transactions whether they are trusted or untrusted. All they know is that the transaction details have a correct card number and CVV and the user has input the transaction details successfully. but they still lack the ability to detect whether these transactions are coming from an authorized person or not. So whenever a fraud incident happens then the data analysis team needs to study the data and investigate the data and decide whether the transaction was trusted or not. If it was a fraudulent transaction, then the bank needs to compensate the user. This paper will discuss several fraud detection mechanisms that exist in the market already and will propose a new machine learning mechanism that helps to detect fraudulent transactions and helps industries to mitigate the fraud incident.**

Keywords: **K-N-N algorithm, machine learning, Fraud Detection.**

I. INTRODUCTION

The card payment business generates revenue through volume very large number of transactions with little profit margin per transaction. Fraud is rare (on the order of 1 fraud per thousand transactions, depending on the context), this can significantly reduce the margin profit of the financial institution since the refund of the amount of a single transaction can be equal to the sum of the marginal profit of a large number of legitimate transactions. That is why they exist in the market different computer tools that can study each customer's transactions and, through some mechanism, produce an alarm when any of them seem suspicious [1].

For example, these could be alerted by employing an application to the cardholder about the alarm generated, calling him to verify the integrity of the purchase, or eventually blocking its plastic. However, the management of alerts has a direct cost associated (salary of analysts, cost of calls, etc.) and indirect, but also relevant (inconvenience to clients, loss of trust in the institution), which can be a potential source of losses for the entity. It creates tension between the extreme cases of not generating too many alarms (then there is no detection of almost no fraud) and avoiding most fraud (at a cost, possibly unsustainable analysis) [2].

The search for balance between these two extremes is a non-trivial and extremely important problem: spending more and more time and resources. That poses an interesting challenge at the scientific level to develop new and better detection models.

Also, in recent years, as there are advancements in technology, and most of them are using credit or debit cards for buying their needs and buying online products, the fraud associated with it is also rising gradually and the risk of stealing card information in increasing especially when the user inputs his card details to unknown website to try to purchase items online.

In the present world, almost all enterprises and companies from small to big industries are using credit online payment cards as a mode of payment. Credit card fraud is happening in all organizations such as the appliance industry, automobile industry, banks, and so on.

Many of the processes like data mining, machine learning, and algorithmic approaches are applied to identify fraud in credit card transactions but did not get considerable results. Hence, there is a need for effective and efficient algorithms to be developed that work significantly. We try to avoid the fraudster using our credit card before the transaction gets approved by using artificial neural network algorithms and compared with a few other machine learning algorithms.

II. PROBLEM STATEMENT

In this research paper, the main problem is online credit card fraud which increases rapidly every day. Even though attempts are being made to counter online fraud [3], many efforts are required to deal with them. Machine learning is one of the detectors for the issue. If this type of research exists, it corresponds to particular jobs of companies in the financial sector and will be focused on very specific situations and realities. In other words, they are not scalable or standardized and use the same tools and features for fraud detection that can be replicated in other companies in the same sector.

III. LITERATURE REVIEW

A. Machine Learning

Machine learning investigates how computers and artificial intelligence allow developing techniques to learn or improve their performance based on data and optimize their process in discovering new patterns given to their learning [4].

- **Machine Learning Algorithms**

Given machine learning [5], it is reasonable to assume that a hidden process explains the data we observe. Although we do not know the details of this process, we know that it is not completely random. This represents the possibility of finding a good and useful approximation, although we cannot identify it to complete the process. The mathematical models of nests in the parameters can be used for this task. The learning part and the model ensemble method choose the non-unknown parameters that optimize a performance criterion concerning the observed data. Machine learning algorithms in 2 groups [6].

Supervised Learning is a synonym for classification. Supervision in learning comes from the labeled examples in the training data set.

Unsupervised Learning is essentially a synonym for grouping. The learning process is not supervised since the input examples are not labeled by class. Usually, we can use grouping to discover classes within the data.

B. KDD Process

Knowledge Discovery in Databases (KDD) is a field of statistics and computer science, employing various techniques and tools such as data mining, machine learning, and artificial intelligence to discover identities, car patterns, unusual trends, and being able to discover potentially useful and novel information. The KDD process encompasses several stages in its realization, from selecting data to the analysis and evaluation of the models [9].

- **Selection and Sample:** The selection of the information comes from various physical or tangible sources, including such as electronic mail, photographs, videos, databases, printed records, and web records, among others, for which a consistent information cube is built and reliable for its due process and stage. in our case the selection will be from any data source that provides the set of transaction history of the user then clean and transfer data from unlabeled to labeled rows, the features that we will extract from the dataset is (location, transaction amount, deviceId).

- **Processing:** The processing evaluates the quality of the information of the data extracted from different sources, and techniques are used to carry out the cleaning procedure of the erroneous, missing, duplicate, inconsistent, and outlier data. Post-processing is the final evaluation of cleaning, thus obtaining a suitable structure for its proper transformation.

- **Transformation:** The stage of transformation and generation of new variables from existing ones consists of consolidation, normalization, and discretization for the next stage of Data Mining.

- **Data Mining:** Modelling stage, discovering and potentiating useful and novel information, and extracting unusual patterns utilizing highly efficient tools and algorithms. “The Royal Academy de ne an” algorithm such as the ordered set of operations that allows finding the solution of a problem and the method of notation in the different forms of calculus [10]. Process and selection of a KDD stage algorithm:

1. Selection of the algorithm for the task to be carried out.

2. Search through computational procedures for the efficient algorithm given to your data.

3. Implementation of the algorithm to the task.

- **Evaluation and Analysis:** At this stage, we can identify and describe the unusual patterns by the models and algorithms used to extract useful, valuable, and novel information for its numerical or visual interpretation with theoretical and statistical foundations.

C. Fraud Pattern

Once the fraudster is in possession of the necessary information, he proceeds to try to carry out transactions in such a way that it is approved and can gain an economic advantage. How the fraudster conducts these transactions depends on what data concrete coughs have. To carry out a transaction, at least the card number and expiration date. A fraudster who succeeds in obtaining these two simple numbers (maybe just looking over your shoulder victim in a store) can, for example, shop for some internet sites or by phone, since they are scenarios of (card not present): the merchant has no way of checking if the customer actually has the card in his power [7].

To avoid this situation, many issuers put a printed random number on the back of the card and require the merchant to request this number in the card, not present scenarios. Another security measure is to require that the delivery address matches the customer's address. Anyway, not all businesses do these verifications. Therefore, it is generally considered this scenario to be much riskier than when the information on the card is captured by an electronic terminal. Fraudsters do not commit fraud with any type of merchandise, but rather those that are easy to resell to obtain a direct benefit are of interest: merchandise electronics, jewelry, brand clothing, or the like. Remember that the type of merchandise is identified by the MCC.

D. Detection Mechanism

- **Fraud Filter Using Address Verification System (AVS)**

This is a detection mechanism that rejects orders that do not meet certain criteria. Fraud filters can be set at checkout, for example, by filtering orders with a negative AVS match or placing them with a card issued in certain country Fraud filters can also be applied within the company's fraud prevention system, such as the immediate rejection of orders above a certain value if the device is located in a geographic region of risk.

- **Exposed Fraud**

It is a term used by Riskified [8] to indicate fraud attempts where the scammer does not try to hide their identity. For example, someone buying products online uses the billing address details of a stolen credit card but provides their own shipping address.

- **Partial View of the Data**

In general, acquirers only know those transactions carried out by their merchants, but not all cardholder transactions they share stopped there. Symmetrically, issuers only know those transactions made by their cardholders, but not all transactions made in the shops where they buy. International brands only know transactions that go through your network, but not local transactions. In turn, the known data of each transaction are those exchanged with the ISO 8583 protocol. In this protocol, data such as card number, business name, etc., are simple attributes of each transaction. The data additional to those of this protocol are known only to the issuer or acquirer to which the cardholder or respective merchant belongs to the mind. Some of this data may be of interest for fraud detection, for instance:

1. Amount available in the account.

2. Account credit limit.

3. Identification of the natural person responsible for the account in order to be able to associate the behavior of different accounts that belong to the same person.

4. Cardholder address information, including credit card history changes of direction.

5. With which MCC can you sell the business, which would allow you to consider all the possible MCCs of the trade and not only that of the transaction?

6. Date of the founding of the business, which is important due to the problem of businesses (migratory) (created temporarily for the sole purpose of committing fraud).

7. Information regarding the name and physical location of the most trustworthy business worthy than those exchanged in ISO messaging.

8. History of payments made by the cardholder, including if there are any rejected payments (for having been made with bad checks, for example).

9. Due date of the next pending payment of the cardholder.

- **The Smart Analyzer**

The Smart Analyzer is a product that PayTrue Solutions want to develop to assist in maintaining the effectiveness of the Detection Engine configuration. This section explains the main requirements of the Smart Analyzer, for which resolution defined the present project. Smart Analyzer users are responsible for reducing losses due to fraud of the financial institution. With this objective, they will use the Smart Analyzer periodically (for example, weekly or monthly) to discover possible modifications to the current configuration of the Detection Engine.

This operative Supports running the Smart Analyzer to take several hours if necessary. In turn, the necessary tests should not affect the normal operation of the financial institution. For this reason, the Smart Analyzer must function offline, that is, disconnected from the flow of transactions of the financial institution. Remember that the Detection Engine works online. In order to run the Smart Analyzer, it is reasonable to expect your user to have access to a database with several months of transactions classified as fraudulent or legitimate.

Usually, this database is a copy of the database of operational data of the financial institution. The Smart Analyzer suggests modifications to the Detection EnGine that the risk analyst will consider; those modifications that result in interest or novel will include them in the configuration of the Detection Engine. On the other hand, the analyst may know rules that he considers interesting, for example, because they were suggested to him from new patterns of fraud observed in other financial entities. It is important that you can experiment with these rules to check whether or not they improve the Detection configuration Engine. In addition to the rules, you may be interested in adjusting the score calculation defined risk or thresholds. For this, the Smart Analyzer should allow you to test the operation of these rules on its transaction database in a mode of use known as a sandbox. Ultimately, the risk analyst is ultimately responsible for managing the configuration ratio of the Detection Engine. For this, both the suggestions of the Smart Analyzer as the recommendations of other risk analysts financial entities. All these functionalities must be offered by the Smart prototype Analyzer developed as part of this project [12].

- **K-N-N Algorithm**

The K-N-N is a suite of various products for a financial institution that wishes to control fraud committed with means of payment. The tool will read the transaction history of the user and cluster the trusted and suspicious transactions in clusters, then flag the user and send an SMS OTP in case of any suspicious transactions [11].

the tool has the following features:

1. Detection Engine Aimed at detecting fraud by generating alerts for possible fraudulent transactions.

2. It is a statistical reports module for the analysis of fraudulent activity behavior. Let us assist analysts risk in understanding fraud situations from a reporting tool that allows you to navigate over the data.

Only those transactions classified as fraudulent by some rules are processed in this phase. In general, it happens that the rules classify many transactions as legitimate and fraudulent actions. There may be rules that have as little as 3% correct. That is, they only get correct when classifying a fraudulent transaction about 1 / 30 times. To further refine the result, the Detection Engine generates alerts only for those l transactions whose risk score exceeds a certain threshold. This p- score ∈ [0, 1] is calculated from the properties of the transaction. The specific way of doing the calculation may vary. It can be calculated as a linear combination of transaction properties (Location, Transaction Amount, device ID), defined by extension in the form of an N-dimensional matrix (with N equal to the number of properties of the transaction) or by any means desired.

IV. RESEARCH METHODOLOGY

The KDD knowledge extraction methodology has given the guideline to execute the present investigation in an organized manner. This chapter talks about the way in which the data set is generated, the time window in which these data are framed, and the way in which the selected algorithms act to extract knowledge that leads to the confirmation of the proposed thesis.

A. Project Data

The type of project is research-action. This type of project is characterized by the coexistence between cognitive aspects and an intention to achieve objective and measurable effects.

The cognitive part is given by the objective of knowing how the selected variables manage to describe debit and credit card fraud detections using machine learning. In addition, the objective and measurable part is given by the model obtained to be able to help organizations and companies deal with credit and debit frauds by using machine learning.

This research is being framed in the type of retrospective study (when analyzing information already registered in the computer systems of the company understudy).

1. Study Area

This research will be carried out in one of the banks that has the following criteria:

- It has little more than 18 years of operation.
- It has several financial products (Credit, Savings, Fixed-term investment, and insurance sales).
- It has an approximate workforce of 350 active employees working in its 28 Branches.
- It has several service channels, the main one is the Branch, but it also has
- Financial correspondents are doing online transactions.
- It has a segregation of functions (operational profiles) for its different financial transactions.
- In addition to storing your business transactions from a few years to date, it also
- It has audit records in which it stores to date, time, branch, employee, type of transaction, and amount, among others.
- It has an operating scheme of limits allowed by profile, with which it has authorizations implemented (by higher levels).

The works of the present investigation will be carried out between the second semester of 2021 and the first semester of 2022.

In the company under study, there are operational and staff areas that handle confidential information about fraud carried out against the institution. They spoke with those responsible for each area involved in this aspect to identify the data that could be used for this research.

2. DATASET

To complete the initial data set, information will be extracted:

A. Historical operations of the Credit module (from 2001 to 2021).

B. Historical operations of the Savings module (from 2001 to 2021).

C. Audit trails (from 2014 to 2021).

D. Reporting of credit or debit frauds by employees (from 2010 to 2021).

V. DISCUSSION

After implementing and running the K-N-N model, The result will be a transaction score, so when the user key-in his card details including card number and CVV, and expiry date in the website attempting to purchase online items, then the merchants will first try to verify the card details if it passes or not, once the card details verified then the merchant will call k-n-n tool to get the transaction score and it will send location id of this transaction and transaction amount and the device id that this transaction has been performed from, then the tool will do the online clustering and compare the new transaction with the historical transaction and then it will get the score of this transaction which is X score, and the initiation must set the threshold for this value if the transaction score exceeds the threshold then this transaction marked as trusted.

If the score is less then this transaction is marked as suspicious or fraudulent transaction the bank or institution will take further steps to verify the user identity and verify the transaction integrity, as we see using the k-n-n tool was able to calculate the score and detect the fraud transaction and it was able to mitigate the fraud incidents in banks and financial institutions as it will always use transaction history of the user as the source of truth and it will be able to detect if this transaction coming from a trusted source, or trusted deviceId or the transaction amount was also still in the range of previous transaction amount history. And as for the decision tree researcher will input the user transaction history to the decision tree algorithm and which will start by calculating the entropy function and then give the decision based on the new transaction, attached below we will see the result compared between the K-N-N tool and the detection mechanism using address verification tool and decision tree, the metric we will be interested in time taken and filter status.

VI. TEST DATA AND RESULTS

Assume we have data set of 4 records that we extracted from bank X that represents the user transaction history, we will use the data as input for each detection mechanize and compare it with K-N-N and see keep an eye on time take and filter status metrics, below is the data that will be using for the comparison:

TABLE I: TRANSACTION HISTORY SAMPLE DATA

ID	Location	Amount	deviceID
1	Malaysia,Subang Jaya	12 $	serial : Iphone 123.432.344
2	Malaysia,Subang Jaya	34.5 $	serial : Iphone 123.432.344
3	Malaysia,Subang Jaya	45 $	serial : Iphone 123.432.344
4	Singapore , Singapore	5,000 $	Serial: Samsung 3445.334.34

- **AVS (Address verification system) Test Results**

AVS detection system will use the billing address verification for detection of the fraud and to verify the transaction, we will notice that AVS will only be able to verify the address without looking at other factors like amount and deviceID and transaction location.

TABLE II: AVS TEST RESULTS

Fraudster Attempts	Fraudster input	Time taken	AVS results
1	Fraudster triggered transaction #1 with new deviceID and new Location and he managed to get a billing address for this card.	1s > less than 1 second	Fraud Detection Failed, because AVS will only verify the billing address and will not verify other factors.
2	Fraudster triggered transaction #1 with new deviceID and new Location and wrong billing address.	1s > less than 1 second	Fraud Detection Success, because billing address does not match.
Final Results =			**50% AVS Successfully detected fraud. 50% AVS Failed to detect Fraud.**

- **K-N-N Test Results**

K-N-N module will use 3 factors to detect the fraud as we mentioned previously which are location and deviceId and transaction amount, and the algorithm will then classify the trusted transaction in one cluster and the suspicious transaction in other cluster, and any new transaction it will compare it with these two clusters and calculate the score of the transaction.

TABLE III: K-N-N TEST RESULTS

Fraudster Attempts	Fraudster input	Time taken	K-N-N results
1	Fraudster triggered transaction #1 with new deviceID and new Location and he managed to get a billing address for this card.	1s > less than 1 second	Fraud detection success, because K-N-N will cluster the new location and new deviceID as a suspicious cluster and it will detect it as a fraud transaction until the user verifies his identity.
2	Fraudster triggered transaction #1 with new deviceID and new Location and wrong billing address.	1s > less than 1 second	Fraud detection success, because K-N-N will cluster the new location and new deviceID as a suspicious cluster and it will detect it as a fraud transaction until the user verifies his identity.
Final Results =			**100% K-N-N Successfully detected fraud.** **0% K-N-N Failed to detect Fraud.**

As a result, shown in K-N-N and AVS, we noticed that K-N-N was able to detect all the fraud transaction attempts and block the card immediately.

VII. CONCLUSION

With the study carried out, we started by stating the problem statement and go briefly with the introduction and compare different detection algorithm that is currently used in the market we found the K-N-N shows the best results so far for detecting fraud transaction by generating the score for the transaction and based of the transaction score threshold we can determine if the transaction is fraudulent or suspicious.

REFERENCES

[1] Kewei, X., Peng, B., Jiang, Y., & Lu, T. (2021, January). A hybrid deep learning model for online fraud detection. In 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE) (pp. 431-434). IEEE.

[2] J. Kummer, T. F., Singh, K., & Best, P. (2015). The effectiveness of fraud detection instruments in not-for-profit organizations. Managerial Auditing Journal.

[3] Raghavan, P., & El Gayar, N. (2019, December). Fraud detection using machine learning and deep learning. In 2019 international conference on computational intelligence and knowledge economy (ICCIKE) (pp. 334-339). IEEE.

[4] Telikani, A., Tahmassebi, A., Banzhaf, W., & Gandomi, A. H. (2021). Evolutionary machine learning: A survey. ACM Computing Surveys (CSUR), 54(8), 1-35.

[5] Mueller, J. P., & Massaron, L. (2021). Machine learning for dummies. John Wiley & Sons.

[6] Uddamari, N., & Ubbana, J. (2021). A Study on Unsupervised Learning Algorithms Analysis in Machine Learning. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(14), 1946-1957.

[7] Xie, Y., Liu, G., Cao, R., Li, Z., Yan, C., & Jiang, C. (2019, February). A feature extraction method for credit card fraud detection. In 2019 2nd International Conference on Intelligent Autonomous Systems (ICoIAS) (pp. 70-75). IEEE.

[8] Baesens, B., Höppner, S., & Verdonck, T. (2021). Data engineering for fraud detection. Decision Support Systems, 150, 113492.

[9] Ojugo, A. A., & Nwankwo, O. (2021). Spectral-cluster solution for credit-card fraud detection using a genetic algorithm trained modular deep learning neural network. JINAV: Journal of Information and Visualization, 2(1), 15-24.

[10] Abdulahi Hasan, A., & Fang, H. (2021, May). Data Mining in Education: Discussing Knowledge Discovery in Database (KDD) with Cluster Associative Study. In 2021 2nd International Conference on Artificial Intelligence and Information Systems (pp. 1-6).

[11] Nasim Matar, Ahmed Hassan, Yousef El-Ebiary, Farah, Yasser Tarshany, Yazeed Al Moaiad. (2022). Cyber Attack Detection Using K-means Machine Learning. International Journal of Special Education, 3(37), 6521-6536.

[12] Yazeed Al Moaiad, Yasser Mohamed Abdelrahman Tarshany, Nasir Ahmed Algeelani, Wafa Al-Haithami. (2022). Cyber Attack Detection Using Big data analysis. International Journal of Computer Science and Information Technology Research, 3(10), 26-33.