Studies in Systems, Decision and Control 488

Bahaaeddin A. M. Alareeni
Islam Elgedawy *Editors*

Artificial Intelligence (AI) and Finance

Springer

Studies in Systems, Decision and Control 488

Series Editor

Janusz Kacprzyk, *Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland*

The series "Studies in Systems, Decision and Control" (SSDC) covers both new developments and advances, as well as the state of the art, in the various areas of broadly perceived systems, decision making and control–quickly, up to date and with a high quality. The intent is to cover the theory, applications, and perspectives on the state of the art and future developments relevant to systems, decision making, control, complex processes and related areas, as embedded in the fields of engineering, computer science, physics, economics, social and life sciences, as well as the paradigms and methodologies behind them. The series contains monographs, textbooks, lecture notes and edited volumes in systems, decision making and control spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

Indexed by SCOPUS, DBLP, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

Bahaaeddin A. M. Alareeni · Islam Elgedawy
Editors

Artificial Intelligence (AI) and Finance

Springer

Editors
Bahaaeddin A. M. Alareeni
Middle East Technical University, Northern Cyprus Campus
Güzelyurt, Türkiye

Islam Elgedawy
Faculty of Computer Science and Engineering
Alamein International University
New Alamein City, Egypt

ISSN 2198-4182 ISSN 2198-4190 (electronic)
Studies in Systems, Decision and Control
ISBN 978-3-031-39157-6 ISBN 978-3-031-39158-3 (eBook)
https://doi.org/10.1007/978-3-031-39158-3

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Artificial Intelligence Trends in Business Development

Analysis of Credit Cards Fraud Detection: Process and Techniques Perspective

Muath Asmar[1](✉) and Belal Yousef Aqel[2]

[1] Department of Finance, Faculty of Business & Communication, An-Najah National University, Nablus, Palestine
asmar@najah.edu

[2] Master of Business Administration, Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine

Abstract. Credit card fraud detection is the process of identifying and preventing fraudulent transactions before they can cause financial damage. This involves using advanced algorithms and machine learning techniques to analyze transaction data in real-time and detect patterns that may indicate fraudulent activity. Effective fraud detection systems are essential for ensuring the security and integrity of the credit card payment system, protecting both financial institutions and cardholders from financial losses. The main objectives of this study are to explain the process and techniques. This study analyzes a global dataset of credit card transactions using regression analysis and artificial neural networks. A regression research found that new balance origin, new balance destination, old balance origin, transaction type, and amount all statistically effect fraud transactions, while old balance destination and transaction length do not. This study used artificial neural networks to identify credit card fraud detection properties. According to the statistics, Old Balance locations are most importantly considered for credit card fraud. This study shows that the models can detect fraudulent activity using real credit card transaction data, providing significant insights into credit card fraud detection approaches.

Keywords: Credit Cards · Fraud Detection · Artificial Neural Networks · Regression analysis

1 Introduction

Credit card fraud affects banks, companies, and consumers. Fraudulent conduct may bring significant financial and reputational damage. Several credit card fraud detection systems have employed AI and machine learning. These technologies can quickly and accurately identify and halt fraudulent transactions. Credit card fraud detection requires analysis of transaction histories, user behavior patterns, and external data sources. Machine learning algorithms can spot suspicious patterns and behaviors including large transactions, unusual purchasing habits, and purchases in unusual areas.

B. A. M. Alareeni and I. Elgedawy (Eds.): *Artificial Intelligence (AI) and Finance*, SSDC 488, pp. 899–911, 2023.
https://doi.org/10.1007/978-3-031-39158-3_84

Fraudsters are adaptable and will develop methods to bypass preventive systems over time. If fraud prevention fails, we need fraud detection methods. Modern technology, communication, and the internet have increased fraud, costing billions of dollars annually. This paper discusses statistical fraud detection methods and their most popular applications. Statistics and machine learning can identify money laundering, e-commerce, and credit card fraud [1]. Design, holo-grams, magnetic stripes, card verification values (CVV), signature boxes, Pin Code for bankcards, Internet security systems for credit card transactions, authentication (OTP), and one-time passwords prevent fraud. Strong consumer authentication ensures online payments with 3D Secure.

Fraud detection catches fraud after it happens. As fraud prevention efforts have failed, we must detect fraudulent transactions immediately. Telemetry can warn credit card fraud monitoring teams using machine learning. Massive transactions, the same item with several skews and slops, enormous cart items, high-amount transactions with many payments, same address for various cards for the same IP address, and different cards for the same IP address [2]. Comparing observed data to expected values, single arithmetical summaries of certain activity items, basic graphical digests, and past system behavior like credit card use are statistical fraud detection strategies. Transaction detection data varies in kind, amount, time, and location [3]. When online transactions replace in-person purchases at merchant sites, banks lose money when fraud occurs. Business intelligence is needed to detect fraudulent transactions.

Although much has been published about securities market trading operations and post-trade settlement infrastructure [e.g., 4, 5], less is known about e-payment processes, notably credit card fraud detection. This research investigates fundamental credit card fraud and the use of technology in fraud detection to address information gaps, as well as to describe the fraud detective process and identify the statistical tools, business analytics, business intelligence, and machine learning roles in fraud detective for credit cards from a given data set.

This research follows: Sect. 2 covers study background. Section 3 reviews credit card fraud detection literature. Section 4 discusses the empirical model, results, data, descriptive statistics, research method, regression, and artificial neural network analysis. Section 5 describes results. Section 6 concludes and discusses business implications.

2 Study Background

Banks are essential for supporting economic growth and development as a financial intermediary [6]. Credit cards are facilities whereas a bank or finance institutions offers a cardholder (the cardholder) a tiny, rectangular piece of plastic or metal to make online transactions and withdraw cash over their bank account limit. Customer credit history determines this. Credit cards usually feature the bank name, special card number, cardholder name, expiry date, smart chip, and payment network logo on the front. Back: CVV, magnetic strip, specimen signature, hologram, bank contact information, and network logo. Visa, Master, American Express, and Discover's foreign market is dominated by the financial credit card network, which connects banks and points of sale. The three elements that must exist for fraud to occur are pressure, opportunity, and rationalization, according to the Fraud Triangle Theory (FTT) of Cressey [7], and the Fraud Diamond

Theory (FDT), which combines the FTT three elements with the fraudster capability and is regarded as an improved or extended version of the FTT by Wolfe and Hermanson [8] as deliberated in [9]. Regardless of the industry or type, according to the Association of Certified Fraud Examiners, fraud is defined as "Any act, expression, omission, or concealment calculated to deceive another to that person's disadvantage, specifically, a misrepresentation or concealment with reference to some fact material to a transaction that is made with knowledge of its falsity." [10].

Credit cards allow you to borrow money and make online payments. Modern credit card fraud is frequent. Lost or stolen cards, card abuse, identity theft, and merchant exploitation are examples. Credit card theft is the unauthorized use of personal information to update an account, request a new card, or replace an existing card. Credit card fraud is the unauthorized use of another person's credit card to make transactions or obtain cash advances. Credit card and personal information may be stolen from physical cards. EMV (Europay, Master Card, and Visa) introduced chip and microchip technology, making it harder for hackers to steal information from magnetic strips using standard ATM skimming equipment.

Before the information era, thieves could use a real card number to make counterfeit cards. These cards were encoded or embossed on blank plastic cards or on membership or gaming card magnetic strips, and the sales slips did not encrypt the linked information. Even though it was employed in automated teller machines, merchant point of sale (POS) skimming was introduced by swiping the card into the card reader (ATMs). Financial organizations prevent this kind of fraud by adding security measures to cards and machines and deploying devices on equipment. The European Central Bank's eighth card fraud report for Europe from 2015 to 2019 found €1.87 billion in fraudulent card transactions worldwide using cards from Single Euro Payments Area (SEPA) member nations. Delays in debit and credit card payments are more prone to fraud than debit card payments, yet CNP fraud continues to dominate fraudulent transactions. Cross-border SEPA transactions made up over half of 2019's fraud dollar amount [11].

2.1 Credit Cards Frauds Types

Frauds are often performed by a third party or hackers, preparators, or insiders (workers) via the leaking of unencrypted information and are classified as transactions or behaviors. There are various forms of credit card fraud, which we shall explain as follows: Hackers take over a bank account and any related accounts of the original consumer in account takeover fraud. Application fraud: when a criminal utilizes a cardholder's personal information to impersonate them to the bank that issued the card. When the application is granted, the fraudster alters his contact information and address. If a customer's card hasn't been disabled, the thief may spend the money. Card Not Present (CNP): techniques employed in the new world of online payments, mobile apps that enable card-less payments like Google Pay and Apple Pay, etc. Friendly fraud: The cardholder requests a chargeback and dispute since he did not make the purchase. Skimming Cards: at an ATM by attaching a device to read and gather information after you turn it, or at a point of sale (POS) by a staff person using a small device reader. Getting the real card number and encoding it on a blank card, magnetic strip, game, or membership card creates counterfeit cards. Phishing involves attacking bogus websites to steal

personal information, login passwords, and credit card numbers. Loyalty card fraud, especially with branded products or credit card points, is also called reward fraud [12].

2.2 Credit Card Fraud Prevention

Fraud prevention is cheaper and more effective than detection. Fraud investigations, especially those involving vast transactional data, cost money and effort. Application Process: Card issuers often verify application data from numerous sources. The user desired dual authentication by contact center, SMS, or mobile apps during the new card activation procedure. Replacement Cards: The bank issuer replaces the card at the client's or bank's request, activating it. When cards expire or need to be replaced, this occurs too (damage, loss, suspicious transaction, etc.)

Bank card issuers monitor high-risk transactions using advanced technologies to prevent fraud. Fraud control may verify a card that seems to have been altered, ripped, or encountered by retailers by physically recognizing it.

2.3 Credit Card Fraud Detection Process

The transactions are verified at the terminal point to determine whether they are valid or not for certain prerequisites like the card number, bank issuance, sufficient balance, and valid Personal Identification Number (PIN), after which they are filtered to determine whether they are accepted or rejected. Meanwhile, a predictive model is receiving this information and raising red flags in the event of suspicious transactions (Fig. 1).

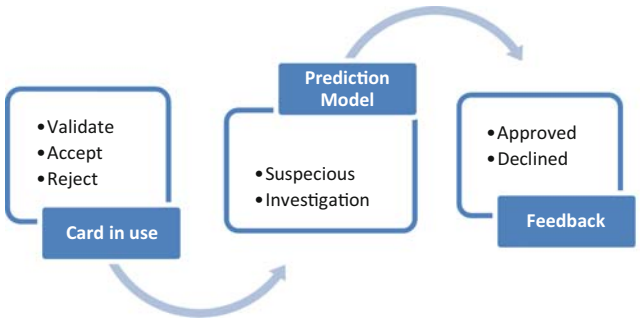

Fig. 1. The fraud detection process.

Credit card fraud has skyrocketed due to growing credit card transactions. Credit card fraud occurs when a credit card is used to defraud a transaction. Statistics and data mining are used to identify fraud. Most credit card fraud detection solutions use AI, meta learning, and pattern matching. Effective fraud detection systems quickly discriminate between fraudulent and genuine transactions [13].

Reviewing the data involved in credit card fraud detection is essential to understanding its challenges. Fraudulent data is substantially less than non-fraudulent data. Data quality and quantity are also issues. Early-stage startups lack user history. Credit agency

ratings may be a temporary solution. Credit card businesses and financial institutions utilize several regulations, instruments, processes, and practices to prevent identity theft and fraudulent transactions. This is credit card fraud detection. Over the past decade, fraud detection has become digitized and automated using statistical tools, AI, and machine learning to manage alerts and analyze big data due to the large number of transactions and criminals' advanced technology to circumvent traditional methods like CVV verification, expiry date, and location tracking. Hence, machine learning algorithms identify fraudulent transactions [14]. Banks and companies fight fraud on two fronts: detection and prevention [1]. "Fraud prevention" refers to any measures taken to prevent fraud. Fraud protection includes pre-activating credit cards to prevent surface mail theft. Internet credit card security prevents fraud. Debit card pin codes prevent ATM withdrawals by requiring the thief to know and hold the card [1]. According to the E-commerce Fraud Index, the rate of retail fraud increased from 0.06% in 2016 to 0.23% in 2017. Credit card fraud is thought to account for 10% of all frauds, which has led to enormous financial losses that alarm businesses [15].

2.4 Models and Techniques Used in Credit Card Fraud Detection

There are different machine learning algorithms used to detect credit card frauds classified as supervised learning and unsupervised learning as shown in Fig. 2, however we are used in this research regression analysis and artificial neural network.

Rational Regression: A method that may be used to both classification and regression problems, albeit it is most often employed for classification. Using dependent variables, logistic regression is used to forecast categorical variables Consider two classes where the class to which a new piece of data belongs must be determined. After that, the algorithms calculate probability values between (0) and (1).

Artificial Neural Networks: A complicated interplay between outputs and inputs is used by this kind of machine learning algorithm to find current trends.

Statistical methods for detecting credit card fraud Use a base line distribution to reflect normative behavior, use a basis distribution; next, seek for data that deviates most from it. Using text analysis and digit analysis [16].

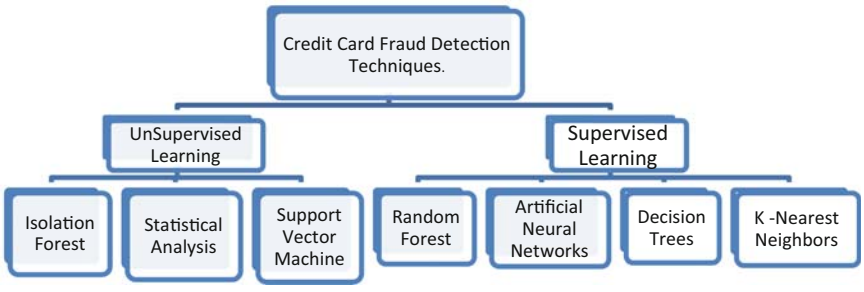

Fig. 2. Fraud detection techniques.

3 Literature Review

Use of machine learning and artificial intelligence approaches for credit card fraud detection has been the subject of several research. Gupta et al. [17] developed a technique to examine how biased machine learning models produced by unequal data affect firms' capacity to adapt and endure technological change. When machine learning techniques and oversampling were employed to detect credit card fraud, accuracy rose.

Credit card fraud detection is becoming important. Online transactions and complicated financial networks need reliable fraud prevention technologies. Most credit card companies use machine learning algorithms and data analytics to spot suspicious conduct. These powerful tools help them detect fraudulent transactions and protect customers from potential losses [18]. Financial security requires credit card theft detection. To identify and fight fraud, a variety of methods and tools are used. Machine learning, pattern recognition, and human review are used to ensure correctness. Banks, merchants, and other financial institutions spend heavily in credit card fraud detection solutions to protect their customers [19].

There is still a lot of work to be done in fraud detection and prevention, despite the advancements achieved. Since credit card fraud is an issue that is always changing, it is crucial for businesses and banks to stay up to date on the most recent fraud detection techniques. Organizations must make sure they are investing in the appropriate technology and stay up to date on any new advancements in the area of fraud prevention in order to achieve this. Additionally, it's critical to remind clients of the best ways to safeguard their credit cards and personal data [3]. Despite progress, fraud detection and prevention need more effort. Businesses and banks must keep current on fraud detection methods since credit card theft is continually evolving. To do this, organizations must invest in the right technology and remain abreast of fraud prevention advances. It's also important to advise customers on credit card and personal data security [3]. Companies are also considering blockchain and facial recognition to reduce credit card fraud. These technologies may improve credit card processing security for businesses. Machine learning and AI algorithms can detect fraud in real time for businesses. With the latest technologies, businesses can protect customer data [20].

Detecting credit card theft is crucial in the age of online purchasing. The number of fraudulent transactions increases along with the online payment processing sector. To identify and prevent fraud, it's critical to have the appropriate tools and strategies in place. Any efficient fraud detection system now relies on cutting-edge technology like machine learning algorithms, predictive analytics, and artificial intelligence. Credit card fraud costs the US $15 billion annually. To avoid fraud, credit card companies analyze spending patterns and watch for odd activities. Customers may also use spending limits and account monitoring. Online credit card users should also be mindful of current scams and identity theft [21]. Credit card fraud detection is operational. Customer data may help banks and businesses spot fraud patterns. This prevents credit card fraud and theft losses. It prevents identity theft, which may cause financial and legal issues.

Fraud detection has become important in the credit card business because it protects customers from fraud and illegal activity. Advanced algorithms can monitor and identify aberrant actions or patterns, enabling real-time fraud detection. Credit card companies

utilize machine learning algorithms to detect transaction abnormalities. These systems can detect hidden data trends and possible fraud [22].

3.1 Research Hypothesis

The main Hypothesis in this study is: There is significant relation between transaction type, transaction amount, card old balance origin, card new balance origin, old balance destination, new balance destination and transactions time, and fraud transactions.

4 Research Methodology

4.1 Data

The credit card transaction data is considered confidential information in the banks, network cards and not easy even impossible to get such datasets. However, a unique dataset about credit card transaction, contains 9999 credit card transactions collected around the world, is available in Kaggle.com [23], these data set includes transaction time, amount in local currency, initial balance before the transaction, customer balance after the transaction, initial recipient before the transaction, recipient balance after the transaction, type of transaction, transaction frauds or not. Table 1 defines the variables used in this study.

Table 1. Variables, its Acronyms, and Description.

Variable	Acronyms	Description
Transaction type	Type	CASH-IN, CASH-OUT, DEBIT, PAYMENT and TRANSFER
Transaction Amount	AMT	Amount of the transaction in local currency
Old balance Origin	OBO	Credit Card initial balance before the transaction
New balance Origin	NBO	Credit Card balance after the transaction
Old balance Destination	OBD	Credit Card initial balance recipient before the transaction. Note that there is not information for customers that start with Merchants
New balance Destination	NBD	Credit Card new balance recipient after the transaction. Note that there is not information for customers that start with Merchants
Transaction Time	Time	Maps a unit of time in the real world. In this case 1 step is 1 h of time
Fraud Transaction	FT	The transactions made by the fraudulent agents = 1 Genuine Transaction made by real customer = 0

4.2 Empirical Model

Regression analysis and artificial neural networks are used in this research to assess the influence of several drivers on credit card fraud.

As indicated in the research model below, where the dependent variable is fraud transactions and the independent variables are including transaction type, amount, origin of the old balance, origin of the new balance, origin of the old balance destination, origin of the new balance, and transaction time.

The empirical specification is expressed as follows:

$$FT = \alpha + \beta 1Type + \beta 2AMT + \beta 3OBO + \beta 4NBO + \beta 5OBD + \beta 6NBD + \beta 7Time + e \quad (1)$$

where Type, AMT, OBO, NBO, OBD, NBD, Time, and FT are defined in Table 1. e is the error term.

The regression analysis is used to identify independent variables that impact and influence the dependent variable, while neural networks adapt to clarify changes in normal transaction conduct and identify importance of the independent variables.

5 Results and Discussion

The results show that most of the Credit Cards transactions type was payments while the lowest transactions type was debit. Figure 3 illustrate the Credit Cards Transactions by Type.

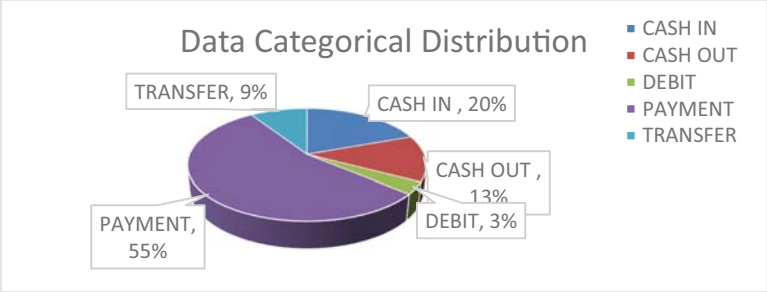

Fig. 3. The Credit Cards Transactions by Type.

5.1 Regression Analysis, Results and Discussion

The regression analysis was used to test the hypothesis of the study. According to the findings, the variables of old balance origin, new balance origin, and new balance destination all have statistically significant effects on the fraud transaction, but old balance destination and transaction time do not. The variables transaction type and amount also

Table 2. Estimations of the regression results.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	−.003	.002		−1.321	.186
Type	.006	.001	.102	8.292	.000***
AMT	8.245E−9	.000	.027	2.170	.030**
OBO	1.197E−7	.000	3.109	22.391	.000***
NBO	−1.201E−7	.000	−3.188	−22.732	.000***
OBD	1.014E−9	.000	.033	1.097	.273
NBD	−1.528E−9	.000	−.056	−1.833	.067*
Time	.000	.000	−.005	−.532	.595

Dependent Variable: Fraud Transaction.
* Indicate statistical significance at the 10% level.
** Indicate statistical significance at the 5% level.
*** Indicate statistical significance at the 1% level.

have statistically significant effects on the fraud transaction. Table 2 show the Regression results.

Table 2 shows that transaction type significantly affects fraud transactions. Transaction type affects fraud transactions statistically. Card-not-present transactions are more likely to be fraudulent than card-present ones. Because there's no face-to-face connection, online transactions likewise carry a higher fraud risk, Transaction type is critical for analyzing and forecasting fraud. To establish whether transaction type affects fraud, investigate the prevalence of particular types of fraud within those transactions. Online transactions may increase credit card fraud. Transaction type affects fraud rates. Because certain transactions are more susceptible to fraud. So, organizations must understand the different transactional types that might be used for fraud.

Table 2 shows that transaction value statistically affects fraud. This is because fraudsters pursue higher-value transactions and transaction size is a statistically significant factor in fraud transactions. Banks and other financial institutions also like to closely monitor transactions with higher monetary amounts. Transaction amounts might indicate fraud risk.

Table 2 shows that the origin of the transaction's old balance affects fraud transactions statistically. Yet, detecting real fraud is difficult. Combining data improves fraud detection, the analysis demonstrates that the new balance destination and old balance origin are highly correlated. Origins with old balances are more linked than destinations with new balances. The data suggest that the source of the prior balance is a better predictor of fraud transactions. Fraud estimate relies on the old transaction balance. Look at the past balance of transactions investigated in that region to identify fraud-prone locations.

Table 2 shows that the origin of the transaction's new balance statistically affects fraud transactions. The origin of the new balance determines fraud risk. The source of the new balance makes it easier to notice suspicious outliers or weird behavior that may be fraud. The new balance's source might reveal a customer's activity and possible transactions. High-new balance transactions are more likely to be fraudulent, Predictive models may identify fraud tendencies using such data. Machine learning can enhance model accuracy.

Table 2 shows that the statistically small Old Balance Destination has no effect on fraud transactions. Since few frauds originate from the same source. Even if balance and destination data may not indicate fraud risk, we cannot draw any judgments from them. To investigate fraudulent transactions from particular regions, more data must be collected and analyzed. Complex algorithms can also detect and prevent future fraud. As fraud is rare, there is no time series or trend. The available information do not support the idea that destination affects fraud detection. Lack of proof disproves a connection, and see problems. This data collection is usually unbalanced. Fraud detection relies more on transaction volume. With transaction data, fraud detection algorithms may be enhanced. This research suggests using transaction volume while detecting fraud.

Table 2 shows that fraud transactions are unaffected by transaction time, which is statistically insignificant. Fraud has no temporal effect since money is always the same. To reduce fraud risk, consider all customer lifetime stages. Examine the consumer's credit history, product knowledge, and geography for odd behavior. To reduce fraud, customers should be verified using many methods. Scammers commit crimes 24/7. Time sensitivity manipulation might enable fraud. If the fraudster is an insider, they may be able to circumvent timely measures. Even at unusual hours, the fraudster may be able to complete a fraudulent transaction. Fraudsters don't care about time and only want money, to detect suspicious activity, several data analysis layers and diverse methods and technologies must be employed, we can create fraud-detecting models using data trends, the correlation research showed a strong negative correlation between the variables, illustrating this inverse relationship. The investigation found that most data points had a substantial negative link, supporting the correlation analysis. Moreover, changing the new balance origin lowers the new balance destination and vice versa. When the new balance's starting point is higher, the destination point will be lower. This shows that fraudsters make the illicit purchase and then move the funds to avoid disputes or disallowed transactions.

5.2 Artificial Neural Networks

Artificial Neural Networks were used in this study to identify the independent variables importance. Table 3 show the importance of the variable's effects in credit card fraud transaction detection.

Table 3 findings demonstrate that the learning procedure grouped the transaction factors into layers, with the old balance destination typically receiving the highest weight as the transactions got underway. As a result, a layer was given to the new balance origin, followed by layers for the new balance origin, old balance origin, amount, amount, type, and time of transactions. Different layers may modify their inputs in different ways. After visiting the layers many times, indications could pass through them, but this will alter according on machine learning inputs and data supplied to the system.

Table 3. Artificial Neural Networks results.

Variable	Importance	Normalized Importance
Type	.115	50.5%
AMT	.133	58.3%
OBO	.150	65.8%
NBO	.194	84.9%
OBD	.228	100.0%
NBD	.157	69.0%
Time	.022	9.7%

More and more, fraud in credit card transactions is being detected using artificial neural networks. It's essential to evaluate the significance of independent variables for this purpose, which include the kind, quantity, and time of the transactions as well as the old and new balances of the destination account. The network is better equipped to identify fraudulent behavior by considering the numerous parameters.

With tremendous success, artificial neural networks have been employed to identify credit card fraud. It is feasible to spot patterns of fraud by examining independent variables such the old balance, the new balance, the destination amount, and the types of transactions. This may be used to stop fraudulent transactions before they happen, minimizing losses for both clients and financial institutions.

6 Conclusion, Business Implications and Future Work

Due of the financial losses and harm to credit ratings it causes, credit card fraud is a serious issue for both financial institutions and private citizens. When a criminal obtains access to another person's credit card information and uses it for illicit purchases, it results in fraudulent transactions. Numerous tactics may be used to commit credit card fraud, including using stolen or fake cards and making unlawful internet transactions. The danger of credit card fraud has expanded along with the popularity of online transactions, making fraud detection a crucial aspect of credit card security. This study discusses the process and techniques of detecting fraudulent credit card transactions and uses regression analysis and artificial neural networks to analyze a unique dataset of credit card transactions gathered from all around the globe. We also checked the methodologies used in fraud detection by comparing various methods and tools, then summarized the findings and offered some suggestions for future work.

This study concludes that credit card fraud detection is becoming more and more crucial in this age of digital transactions to protect the economy and provide people financial security. To keep the confidence of their consumers and the integrity of the credit card system, financial institutions and companies must be attentive in identifying and blocking fraudulent behavior.

One of the most important limitations of this research is the availability of data that is not only secret but also does not include vital information about the transactions made using and transactions of credit cards.

In future studies, the researchers recommend that other models and techniques be re-examined using the current data set to compare and contrast as well as measure accuracy and precision.

References

1. Bolton, R., Hand, D.: Statistical fraud detection: a review. Stat. Sci. **17**(3), 235–255 (2002)
2. Tidal Commerce: Tidal Commerce Learn (2022). http://www.tidalcommerce.com/learn/signs-of-credit-card-fruad
3. Delamaire, L., Abdou, H., Pointon, J.: Credit card fraud and detection techniques: a review. Banks and Bank Syst. **4**(2), 57–68 (2009)
4. Asmar, M., Ahmad, Z.: Market microstructure: the components of black-box. Int. J. Econ. Financ. **3**(1), 152–159 (2011)
5. Asmar, M., Trimbath, S.: Regulatory reform and trade settlement failures in USA equity markets: does regulatory reform matter? Quant. Financ. Econ. **6**(4), 537–552 (2022)
6. Asmar, M.: Effects of bank-specific factors on the net interest margin of working banks in Palestine. J. Econ. Manage. **33**, 5–24 (2018)
7. Schuessler, K.F., Cressey, D.R.: Personality characteristics of criminals. Am. J. Sociol. **55**(5), 476–484 (1950)
8. Wolfe, D.T., Hermanson, D.R.: The fraud diamond: considering the four elements of fraud (2004)
9. Abdullahi, R.U., Mansor, N.: Fraud triangle theory and fraud diamond theory: understanding the convergent and divergent for future research. Int. J. Acad. Res. Account. Financ. Manage. Sci. **5**, 54–64 (2015). https://doi.org/10.6007/IJARAFMS/v5-i4/1823
10. Association of Certified Fraud Examiners (2022). ACFE. http://www.acfe.com
11. European Central Bank: Seventh report on card fraud. European Central Bank, Frankfurt, Germany (2021)
12. Gupta, S., Malsa, N., Gupta, M.V.: Credit card fraud detection and prevention—a survey. Int. J. Innov. Res. Sci. Technol. **4**, 1–7 (2017)
13. Shiv Kumar Verma, A.K. Credit Crad Fraud Detection System. Credit Crad Fraud Detection System. Galgotias University-Conference Paper (2022)
14. Inscribe: Inscrine.com (2022). https://www.inscribe.ai/fraud-detection/credit-fraud-detection
15. Madhurya, M.J., Gururaj, H.L., Soundarya, B.C., Vidyashree, K.P., Rajendra, A.B.: Exploratory analysis of credit card fraud detection using machine learning techniques. Global Transitions Proceedings **3**(1), 31–37 (2022). https://doi.org/10.1016/j.gltp.2022.04.006
16. Fayyomi, A.M., Eleyan, D., Eleyan, A.: A survey paper on credit card fraud detection techniques. Int. J. Sci. Technol. Res. **10**(09) (2021)
17. Gupta, P., Varshney, A., Khan, M.R., Ahmed, R., Shuaib, M., Alam, S.: Unbalanced credit card fraud detection data: a machine learning-oriented comparative study of balancing techniques. Procedia Comput. Sci. **218**, 2575–2584 (2023). https://doi.org/10.1016/j.procs.2023.01.231
18. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., Imine, A.: Credit card fraud detection in the era of disruptive technologies: a systematic review. J. King Saud Univ. Comput. Inf. Sci. **35**(1), 145–174 (2023). https://doi.org/10.1016/j.jksuci.2022.11.008
19. Ryman-Tubb, N.F., Krause, P., Garn, W.: How artificial intelligence and machine learning research impacts payment card fraud detection: a survey and industry benchmark. Eng. Appl. Artif. Intell. **76**, 130–157 (2018). https://doi.org/10.1016/j.engappai.2018.07.008

20. Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., Shah, M.: A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. Ann. Data Sci. (2022). https://doi.org/10.1007/s40745-022-00433-5
21. Bin Sulaiman, R., Schetinin, V., Sant, P.: Review of machine learning approach on credit card fraud detection. Hum.-Centric Intell. Syst. **2**(1), 55–68 (2022). https://doi.org/10.1007/s44230-022-00004-0
22. Zhang, X., Han, Y., Wei, Xu., Wang, Q.: HOBA: a novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Inf. Sci. **557**, 302–316 (2021). https://doi.org/10.1016/j.ins.2019.05.023
23. Kaggle: Kaggle.com (2022). https://www.kaggle.com/search?q=fraud+detection