The application of artificial intelligence techniques in credit card fraud detection: a quantitative study

Yusuf Yusuf Dayyabu[1*], *Dhamayanthi* Arumugam[1], and *Suresh* Balasingam[1]

[1]Asia Pacific University, Jalan Teknologi 5, Taman Teknologi Malaysia, 57000 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia

Abstract. Credit card fraud is a major problem that has caused several challenges for practitioners in theaccounting and finance industry due to a large number of daily transactions as well as the difficulties encountered in identifying fraudulent transactions. The purpose of this study is to investigate the application of artificial intelligence techniques as a fraud detection mechanismthat can effectively and efficiently detect credit card fraud and identify fraudulent financial transactions. The data was acquired from 100 respondents across the accounting and finance industry and analysed using SPSS. Researcher analysed the data using regression analysis, Pearson correlation coefficient, and reliability analysis. Findings revealed that the three artificial intelligence techniques machine learning, data mining, and fuzzy logic have a significant positive relationship with credit card fraud detection. However, fuzzy logic was discovered tobe the least utilized by experts due to its low accuracy/precision in comparison with machine learning and data mining. Based on these findings, our study concludes that the application ofartificial intelligence techniques provides experts with better accuracy and efficiency in detecting fraudulent transactions. Therefore, it is recommended that fraud examiners, auditors, accountants, bankers, and organizations should implement and apply artificial intelligence techniques in order to spot anomalies faster and identify fraudulent financial transactions effectively and efficiently.
Keywords: Identity Theft, Credit Card Fraud Detection, Artificial Intelligence, MachineLearning, Data Mining, Fuzzy Logic.

1 Introduction

There has been a tremendous surge in fraudulent schemes related to all aspects of the business world since the continuous advancement of the world wide web and the introduction of modern-day technologies (Association of Certified Fraud Examiners [ACFE], 2020). Some ofthe most common fraudulent schemes and financial crimes that have caused significant damage in several industries to include financial statement fraud, e-commerce fraud, insurance fraud, money laundering, asset misappropriation, and credit card fraud (PricewaterhouseCooper [PWC], 2020). The use of credit cards as a mode of payment is

* Corresponding author: dhamayanthi@staffemail.apu.edu.my

becoming very common among enterprises in both small and large industries, given the effortless nature of credit cards and theability to utilize them both online and offline (Susan, 2016). However, credit card transactionsare not completely safe from the occurrence of fraud.

According to Asha and Kumar (2021), credit card fraud occurs in industries such as the automobile industry, e-commerce industry, appliances industry, and financial institutions, among others. These industries are exposed to different types of credit card fraud, which mostly arises because a fraudster intends to deliberately deprive another of property or gain an unfair advantage over an individual (Albrecht, 2015). The Global Economic Crime and Fraud Survey report 2020 showed that an estimated $11 billion was lost to credit card fraud in the United States last year and in the previous year (2019). The total amount of losses from payment card fraud was reported to be around $28.65 billion worldwide (El-Naby et al., 2021).

Bragg (2019) defines credit card fraud as the unauthorised use of any system or illicit action involving the use of a physical card or card information without the cardholder's knowledge. Fraudulent activities involving credit cards are rapidly growing with the significant increase inthe number of credit card transactions. Credit cards can be categorized into offline fraud that detects cards that are stolen by using their details, and online fraud which can be detected through mobile phones, the internet, the web, and shopping (Maharjan and Chudal, 2020). In an offline mode, credit cards are physically presented when completing a transaction. Fraudsters can take advantage of this mode of purchase by stealing the credit card in order to carry out fraudulent transactions. While in the online credit card mode of transaction, only a few key details about the card, such as the card number, expiration date, and card verificationvalue (CVV) are necessary to complete the transaction. Typically, such purchases are made over the phone or on the Internet. Fraudsters only have to know the card details to conduct fraud in these types of transactions. Aside from this categorization, there are other types of fraud transactions, such as the conventional way of stealing account credentials, and internet fraud, which includes site cloning, card cloning, and questionable merchant sites (Bansal & Garg, 2021).

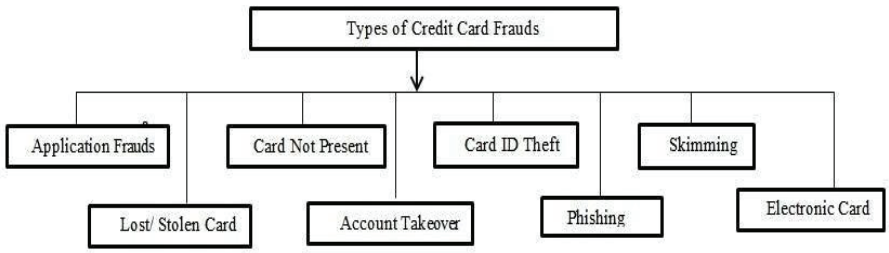


Fig. 1. Types of Credit Card FraudSource: Bansal & Garg (2021).

Most of the time, the actual cardholder is unaware that his or her card information has been seen or stolen by someone else. Fraudulent credit card transactions coexist with legitimate transactions and form similar patterns, making it very difficult to distinguish between fraudulent and non-fraudulent transactions (Yee et al., 2018). Therefore, the adoption/application of artificial intelligence techniques is essential for credit card fraud detection. For instance, credit card firms such as MasterCard, Visa, and American Express have successfully used AI to detect fraudulent patterns and prevent credit card fraud (Sorournejad et al., 2016). However, the knowledge and understanding of artificial intelligenceas a credit card fraud detection tool is still relatively limited given the several techniques and algorithms associated with such disruptive technology (Yee et al., 2020). The concept of artificial intelligence gives machines a huge edge by allowing them to learn from previous fraud patterns/trends and subject experts such as forensic accountants (Naqvi, 2020). Such features give disruptive technology the ability to process large amounts of data efficiently and effectively, resulting in sophisticated algorithms that become part of its

learning process (Moody, 2021).

Furthermore, AI is mostly discovered in a variety of domains, including machine learning, natural language processing, deep learning, cognitive computing, the internet of things, as wellas automation and robotics that operate with algorithms (Carvajal et al., 2018). The different characteristics and capabilities of artificial intelligence make it relatively easy to expand into numerous industries, such as manufacturing, retail (e-commerce), and healthcare. Moreover, identity theft such as credit card fraud can be minimized with the use of artificial intelligence to verify and authenticate the user's identity (Larson, 2019). The use of verification and processing systems with machine learning or deep learning would be an effective method to detect anomalies in card transactions (Asha and Kumar, 2021). AI provides a solution to detecting fraudulent credit card transactions by flagging any suspicious patterns, allowing thefraud examiner or organization to identify the anomaly quickly and prevent future fraud occurrences (Issa et al., 2016). As a result, the global rise in fraudsters necessitates immediateaction to reduce the danger of financial loss, reputational damage, and bankruptcy. In this research, the researcher have identified artificial intelligence techniques/variables, namely machine learning, data mining, and fuzzy logic, which are some of the most utilized credit card fraud detection tools. Essentially, this study discusses the significance of applying Artificial Intelligence (AI) to credit card fraud detection, since it is the most contemporary and effectivetool for detecting and preventing fraudulent activities across different industries.

2 Literature Review

2.1 Credit Card Fraud Detection

The application of artificial intelligence techniques to fight cybercrime and detect credit card fraud was further discussed by Chukwuneke et al. (2018). Their study emphasised the findings of previous studies by implying that different methods of artificial intelligence canbe used to detect credit card fraud. The authors used intelligent agents to detect credit card fraud during transactions. Based on this approach, they discovered that such an intelligent agentcould achieve a high rate of fraud transactions while having a low false alarm rate, making fraud detection more efficient. Their intelligent agent approach focuses on detecting fraud while a transaction is in progress, taking into consideration the customers' pattern, and any variation from that pattern is considered a fraudulent transaction. Similarly, Amanze et al., (2018) present multi-agent techniques for fraud analysis and credit card fraud detection. This method compares different intelligent agents using a mathematical model for credit card identification. The authors tested the agents' resistance to credit card fraud over time and at various rates of consumer fraud notifications. Finally, the research proposes a security solution that will increase communication channel trust by utilising hybrid technology that combines adaptive data mining and intelligent agents to validate credit card transactions. The result of the model showed that multi-agent credit card fraud detection systems have a 94% performance rate, which is comparable to that of other fraud detection software.

Furthermore, Niu et al. (2019) conducted a comparison study of credit card fraud detection using supervised and unsupervised methods. The study utilized six supervised classification models, including Support Vector Machines (SVM), Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), K-Nearest Neighbors (KNN), and Extreme Gradient Boosting (XGB), and four unsupervised anomaly detection models, including One-Class SVM (OCSVM), Auto-Encoder (AE), Restricted Boltzmann Machine (RBM), and Generative Adversarial Networks (GAN The results demonstrate that supervised models

outperform unstructured models by a small margin. Due insufficient annotation and data imbalance concerns in real-world applications, our research suggests that unsupervised approaches for credit card fraud transaction detection are still effective. Several researchers have also indicatedthat various artificial intelligence tools can be applied to build a credit card fraud detection model that would assist financial institutions and fraud examiners to determine the frequency of credit card fraud and classify both fraudulent and non-fraudulent transactions accurately andeffectively (Paruchuri, 2017), (Li et al., 2018), (Yazici, 2020). Therefore, in order to analyse and measure the effectiveness of these artificial intelligence-based tools, experts' perspectiveson the use of these tools are required.

2.2 Artificial Intelligence

Artificial intelligence is extensively utilised and plays a critical role in credit card fraud detection, according to research by Mahmud et al., (2017). The research analyses and contrasts several prominent classifier systems for identifying credit card fraud. The authors concentratedon the metrics that were used to evaluate and rank the algorithms' classification performance, using the UCSD-FICO Data Mining Contest 2009 dataset for performance evaluation tests. According to the findings of the experiment, the attained classification accuracy rate is 98.25%,but the fraud detection success rate is less than 50%. Moreover, meta and tree classifiers outperform the other groups of classifiers. Finally, the overall fraud detection success rate should be considered when evaluating the effectiveness of classifiers in a fraud detection system. Save et al., (2017) suggested a system for detecting fraud in credit card transactions bycombining Luhn's and Hunt's algorithms into a decision tree. The system was built to check whether a transaction is genuine or not. The results revealed that the suggested model could validate a credit card by indicating whether a transaction was real or fraudulent with a very lowfalse alarm rate. Therefore, their findings were consistent with comparative studies in the sensethat the proposed system's correctness and efficacy are secure.

Moreover, Sisodia et al., (2018) mentioned that fraud detection systems have acquired great importance for financial institutions, prompting the exploration of the class imbalance problem that is prevalent in fraud-occurring transactions. They used the resampling techniques of "SMOTE, SMOTE ENN, SMOTE TL, SAFE SMOTE and ROS" to handle this imbalance problem. Their findings showed that in the set of oversampling approaches analysed, the artificial intelligence-based model constructed using the SMOTE ENN method detects credit card fraud better than other classifiers, while TL performs better in the set of under-sampling strategies considered. Choi and Lee (2018) also discussed the application of artificial intelligence techniques such as machine learning and deep learning to detect financial fraud and proposed a process using artificial neural networks for accurate fraud detection based on their merits and limitations. Their findings revealed that, at various ratios, machine learning- based methods outperform neural networks in terms of detection effectiveness, although the feature selection procedure must be done based on the input data. In addition, a machine learning-based procedure must confirm the best mix of clustering and classification techniques(de Sá et al., 2018).

However, studies by Yazici et al., (2020) highlighted that the enormous number of credit card transactions that occur in a short period of time,it is difficult to adapt a fraud detection system to real-time situations. Moreover, a study conducted by Nkomo and Breetzke et al., (2020) assessed the credit card fraud detection technologies utilised by banks, as well as the challenges associated with applying them. To minimise the flaws of current credit card fraud detection systems, the study advises using artificial intelligence, geolocation, and data mining in credit card fraud detection methods.

Thus, credit card fraud detection technologies could leverage artificial intelligence, data

mining, and geolocation to analyse and discover trends in client spending in order to detect fraudulent transactions. This shows that the use of artificial intelligence in credit card fraud detection is relatively underutilized by experts and financial institutions despite the highlightedbenefits and features of the disruptive technology.

2.3 Machine Learning

Based on their studies, Yee et al., (2018) investigated how machine learning and data mining techniques might be used to detect credit card fraud, and found that by learning data patterns, the combination of machine learning and data mining approaches could distinguish between valid and illegitimate transactions. This means that, in comparison to a rule-based system, machine learning systems are more adaptable to continual changes and upgrades through algorithm and data preparation, giving them a more effective and efficient fraud detection approach (Das et al., 2021). To detect credit card transaction fraud, Huang (2019) focused on the basic function of feature selection in a supervised model utilising machine learning methods such as neural net, boosted tree, and random forest. The results demonstrate that the random forest model achieved the best performance, detecting roughly half of all fraud attempts using only the top 3% of data classified as suspicious by the fraud algorithm score.

According to Varmedja et al., (2019), several machine learning algorithms can be used for thedetection and classification of transactions as fraudulent or genuine. In their study, the authorsused machine learning algorithms such as logistic regression, random forest, naïve Bayes, and multilayer perception to train and test the data. Their results showed each algorithm can be used for credit card fraud detection and other irregularities with high accuracy. Furthermore, Awoyemi et al., (2017) tested the efficacy of multiple machine learning techniques on a creditcard fraud dataset that was severely skewed. The accuracy, sensitivity, specificity, precision, Matthew's correlation coefficient, and balanced classification rate were used to assess the techniques' performance. The results demonstrate that naïve Bayes, k-nearest neighbour, and logistic regression classifiers have optimal accuracy of 97.92%, 97.69%, and 54.86%, respectively. In addition, the results revealed that k-nearest neighbour outperforms both naïveBayes and logistic regression approaches.

Studies by Kumar et al., (2019) created a fraud detection model that used random forest algorithms (RFA) for detecting fraud in credit card transactions. Their findings suggest that therandom forest algorithm is a supervised machine learning approach that uses a decision tree to classify credit card transactions and then uses a confusion matrix to measure performance. According to research by Kumar and 1qbal (2019), Mastercard fraud detection can be carried out with a series of analysis performed using machine learning algorithms in credit card frauddetection. They suggested that there is still a growing need to use efficient systems that performwell in every situation. Hence, experts and financial institutions must determine the most suitable and efficient AI technique that would assist them in credit card fraud detection. Therefore, the researcher has formulated the following hypothesis:

H1: There is a positive relationship between Machine learning and Credit Card Fraud Detection.

2.4 Data Mining

Yee et al., (2020, p. 24) mentioned that "a large number of studies have exploited the strength of data mining and machine learning to prevent credit card fraud". Several new approaches based on artificial intelligence and data mining have emerged to detect a variety of fraudulent credit card transactions (Kumar and Pavaskar, 2012). Deng et al., (2021) created a data mining-based model for transaction fraud detection using random forest and manual detection as the data mining techniques. The findings of the credit card fraud dataset demonstrated that this

model's technique outperforms benchmark models like logistic regression and support vector machines with an accuracy rate of 96.8% and an AUC ROC score of 92.5%. Similarly, Maharjan and Chudal (2020) attested that the emerging data mining techniques assist in detecting and identifying fraudulent behaviour associated with credit card transactions. Their study compared different data mining techniques to determine the best technique for credit card fraud detection based on the highest accuracy. Their experiment showed that SVM has the highest accuracy of 99.3%, while other models were all above 95% accuracy, making them very precise at detecting fraudulent users' activities on credit cards.

Furthermore, Dutta et al., (2017) also conducted a review on the most commonly encounteredcrimes in credit card applications. Their study suggested that, when existing non-data mining ways of preventing identity theft such as credit card fraud are used, there is a likelihood of challenges arising. Therefore, to address these difficulties, a novel data mining layer of defencewas developed. The authors used two data mining algorithms, Communal Detection (CD) andSpike Detection (SD), to produce innovative layers for identifying fraud in various applications. Their results indicated that the system could produce results while requiring a significant amount of time. Moreover, even after a frequent update of the algorithms, there is no true evaluation because the fraudsters do not have time to adjust their behaviour in responseto the techniques being deployed in real-time, which shows that a proper demonstration of theconcept of flexibility is impossible (Mehndiratta and Gupta, 2019).

In a study by Vardhani et al., (2018), a novel data mining algorithm called Condensed NearestNeighbor (CNN) algorithms was used to detect credit card fraud transactions and classificationof fraudulent and illegitimate transactions in the dataset with high precision. The study used data reduction concepts intending to create a condensed set by preserving the samples that are most vital in decision making. Their findings showed that the use of this data mining algorithmminimized training data, improved processing time, and decreased the recognition rate. Therefore, it is important to further explore the efficiency and benefits of data miningalgorithms in order to improve the rate of credit card fraud detection in the financial industry.

Modi and Dayma (2017) studied numerous strategies for detecting fraudulent transactions andconducted a comparison study among them. Any one of these strategies, or a combination of them, can be used to detect fraudulent credit card transactions. Thus, with the addition of newattributes to the model, it may be possible to train it more accurately. The authors also mentioned that financial institutions and credit card companies utilise a variety of data mining tools to detect fraudulent behaviour. Any of these methods can be used to determine a client's regular usage pattern based on their previous behaviour. Therefore, a comparison should be conducted by examining the various credit card fraud detection systems that have been offered over time. Mishra and Kumari et al., (2019, p.1) also mentioned that "several modern data mining techniques have been deployed for the detection of fraud in the domain of credit cards, such as Hidden Markov model, fuzzy logic, K-nearest neighbor, genetic algorithm, Bayesian network, artificial immune system, neural network, decision tree, support vector machine, hybridized method, and ensemble classification". These techniques were used for detecting credit card fraud by researchers, with most of this research contributing significantly towards the efforts of financial institutions and credit card companies to mitigate the risk of fraud and detect any subsequent fraudulent activities (Carneiro et al., 2017).

In addition, studies by John et al., (2016) and Rambola et al., (2018) both analysed the use of data mining techniques and algorithms to detect fraudulent activities like credit card fraud in the financial industry. In their research, they looked at how to detect bank fraud using data- mining techniques including classification, clustering, forecasting, and association to evaluatecustomer data and find patterns that could result in fraud occurring. They both revealed that data mining algorithms are effective and accurate at detecting fraud in the

banking sector, showing high precision, sensitivity, and accuracy rates. Therefore, this resulted in the formulation of the researchers' second hypotheses described below, based on the review of studies:

H2: There is a positive relationship between Data Mining and Credit Card Fraud Detection.

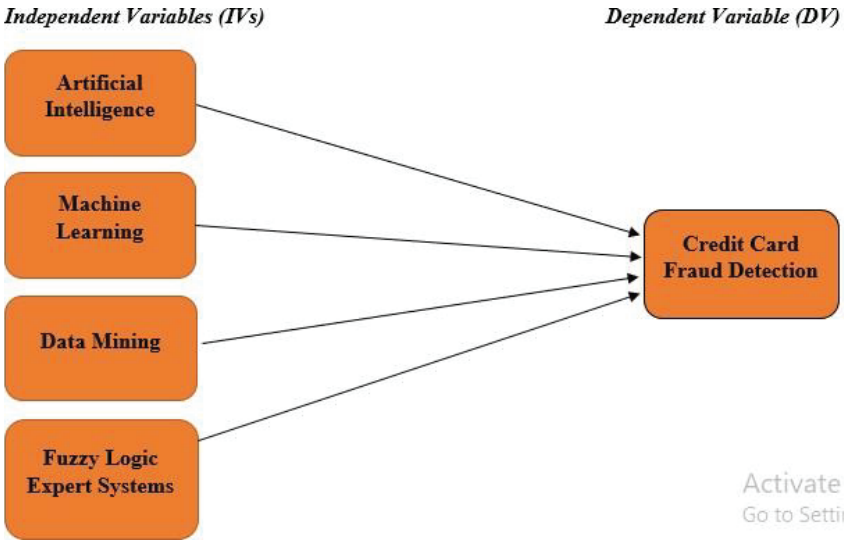
2.5 Fuzzy Logic

A study by Razooqi et al., (2016) used a fuzzy database to detect credit card fraud by monitoring users' behaviour and spending patterns. They aimed to build a model using fuzzy logic systems and artificial neural networks to compare the AI techniques that would correctly and accurately identify legitimate or fraudulent transactions. Their results indicated that both methods are effective in credit card fraud detection. However, the ANN method is better in comparison to fuzzy logic, based on the accuracy rate of both models. The study revealed that ANN is 33% more accurate than fuzzy logic at detecting credit card fraud in the financial industry. In a similar vein, Saeed (2019) used real-world data collected from Sudanese financial institutions to develop unique intelligent type-2 Fuzzy Logic Systems (FLSs) that candetect debit card fraud. The results of the research suggest a system that reveals a high level ofaccuracy in the automatic detection of fraud in the financial industry. Behera and Panigrahi (2017b) proposed a two-stage fuzzy expert system for the detection of credit card fraud, whichwas implemented in MATLAB. A pattern-matching mechanism was used to process the incoming transactions to get things started. This component is made up of two modules: a fuzzyclustering module and an address-matching module. Each of these modules assigns a score tothe transaction based on the amount by which it deviates from the norm. Based on a comparisonof the fuzzy logic expert system's performance with other fraud detection systems, their findings verified the effectiveness of the fuzzy logic expert system in detecting credit card fraud.

In addition, Askari and Hussain (2020) introduced an e-transactional fraud detection system based on intuitionistic fuzzy logic and the C4.5 decision tree. In an online transaction dataset,the researchers looked at both derived and normal features. In comparison to previous studies,their findings revealed that the fuzzy logic-based system had a high and efficient detection rate.Therefore, it is clear that fuzzy logic-based systems, albeit not the most effective fraud detection methods, are still rated highly among experts as one of the most suitable and cost- effective artificial intelligence-based fraud detection mechanisms in the financial industry. Asa result, we have developed the following hypothesis.

H3: There is a positive relationship between Fuzzy Logic Based Systems and Credit Card FraudDetection.

3 Research Framework



4 Methodology/Materials

This study is supported by quantitative primary data. In terms of sampling methods, this study employed a convenient sampling approach. According to Sekaran and Bougie, sample sizes larger than 30 and lesser than 500 are appropriate for the majority of other investigations (2010). To assure the accuracy of the final results, 100 respondents were chosen for this study. The data collected from the forensic accounting, banking & finance, and auditing industry via LinkedIn and other social networking platforms. The analysis carried out using SPSS software and present the extracted results.

5 Results, Findings and Discussion

5.1 Reliability Statistics of each Variable

Table 1. Reliability Statistics of each Variable. (Source: Primary Data).

Variable	No of Items	Cronbach's Alpha	Justification
Credit Card Fraud Detection	5	0.879	"Good internal consistency"
Artificial Intelligence	5	0.855	"Good internal consistency"
Machine Learning	5	0.872	"Good internal consistency"
Data Mining	5	0.876	"Good internal consistency"
Fuzzy Logic	5	0.918	"Excellent Internal Consistency"

Table 1 illustrates that the Cronbach's Alpha of the dependent variable credit card fraud detection and the independent variables artificial intelligence, machine learning, data mining, and fuzzy logic are 0.879, 0.855, 0.872, 0.876, and 0.918 respectively. "This indicates that allthe variables are within the Cronbach's Alpha required range and adhere to the doctrine of Cronbach" (George and Mallery, 2010). Therefore, since the reliability test of all the variables

is good and excellent, we can conclude that the variables are reliable, acceptable, and have a significant continuous consistency.

5.2 Pearson Correlation Coefficients of all variables

Table 2. Pearson Correlation Coefficients of all variables. Source: Primary Data.

Variables	N	Pearson Correlation,r	p-value	Significance	Relationship
Artificial Intelligence	100	0.815	"0.000"	"Significant"	Strong and Positive
Machine Learning	100	0.697	"0.000"	"Significant"	Moderate and Positive
Data Mining	100	0.723	"0.000"	"Significant"	Moderate and Positive
Fuzzy logic	100	0.416	"0.000"	"Significant"	Weak and Positive

Table 2 shows the results of the Pearson correlation analysis and summaries the coefficients between credit card fraud detection and each independent variable. The significance of the coefficients is demonstrated, and the strength of the relationship is mentioned. The output illustrates that the relationship between credit card fraud detection andthe independent variable "artificial intelligence" is fairly strong and positive because the coefficients are above 0.80. This indicates that data points of the variable fall closer to the line. Moreover, the independent variables "Machine Learning" and "Data Mining" have a moderateand positive relationship with credit card fraud detection since the coefficients are within the range of 0.60 to 0.80. Lastly, the relationship between credit card fraud detection and fuzzy logic is fairly weak and positive as explained by Ratner (2009).

5.3 Regression Analysis

Table 3. Multiple linear regression

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.845[a]	.714	.702	.34385	.714	59.406	4	95	.000

a. Predictors: (Constant), Fuzzy Logic, Data Mining, Machine Learning, Artificial Intelligence

b. Dependent Variable: Credit Card Fraud Detection

Source: Primary Data

The model summary displayed in Table 5.2.1 above shows the R square. "The R is the multiplecorrelation coefficient values derived from the difference between real and estimate value of the DV" (Pallant, 2013). This means the R-value is a measure to estimate the likelihood of thedependent variable. The range of the R must be within -1 to +1, where a value nearer to -1 shows a negative relationship and +1 shows a positive relationship. In Table 5.2.1, the R-valueof 0.845 indicates a high degree of correlation and a positive relationship between the variables.The result also shows that the R-squared is 71.4%, which shows that our model supports all thevariability of the data around the average (mean). In other words, 71.4% of the total variation in credit card fraud detection can be justified by the independent variables, which shows that the model fits our data quite well. As a result, we can conclude that an increase in the usage ofartificial intelligence, machine learning, data mining, and

fuzzy logic will bring an instant increase in credit card fraud detection.

5.4 Analysis of Variance (ANOVA) between Variables

Table 4. Analysis of Variance (ANOVA) between Artificial Intelligence and Credit card fraud.

ANOVAa						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	28.095	4	7.024	59.406	.000[b]
	Residual	11.232	95	.118		
	Total	39.327	99			
a Dependent Variable: Credit Card Fraud Detection						
b Predictors: (Constant), Artificial Intelligence						

Source: Primary Data

Table 4 displays the ANOVA between credit card fraud detection and artificial intelligence. The output reveals the p-value of 0.000 to be lower than the 0.05 significant level. This indicates that the positive relationship between credit card fraud detection and artificial intelligence is highly significant and at the 5% significance level, which means that machine learning has a positive influence on credit card fraud detection. Therefore, "the null hypothesis will be rejected at the 95% confidence interval, and the alternative hypothesis is accepted."

Table 5. Analysis of Variance (ANOVA) between Machine Learning and Credit card fraud.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	19.122	1	19.122	92.751	.000[b]
	Residual	20.204	98	.206		
	Total	39.327	99			
a. Dependent Variable: Credit Card Fraud Detection						
b. Predictors: (Constant), Machine Learning						

Source: Primary Data

Table 5 shows the analysis of variance between credit card fraud detection and machine learning. The output illustrates the p-value of 0.000 to be less than the 0.05 significant level. This demonstrates that the positive relationship between credit card fraud detection and machine learning is highly significant and at the 5% significance level, which means that machine learning has a positive influence on credit card fraud detection. Thus, "the null hypothesis will be rejected at the 95% confidence interval, and the alternative hypothesis is accepted."

Table 6. Analysis of Variance (ANOVA) between Data Mining and Credit card fraud.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	20.565	1	20.565	107.415	.000[b]
	Residual	18.762	98	.191		
	Total	39.327	99			
a. Dependent Variable: Credit Card Fraud Detection						
b. Predictors: (Constant), Data Mining						

Source: Primary Data

Table 6 shows the analysis of variance between credit card fraud detection and data mining. The table demostrates that the p-value of 0.000 is less than the 0.05 significant level. This indicates that the positive relationship between credit card fraud detection and data mining is highly significant at the 5% significance level, which means that data mining has a positive influence on credit card fraud detection. Thus, we may infer that "the null hypothesis will be rejected at the 95% confidence interval, and the alternative hypothesis is accepted".

Table 7. Analysis of Variance (ANOVA) between Fuzzy Logic and Credit card fraud.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.804	1	6.804	20.502	.000[b]
	Residual	32.523	98	.332		
	Total	39.327	99			
a. Dependent Variable: Credit Card Fraud Detection						
b. Predictors: (Constant), Fuzzy Logic						

Source: Primary Data

Table 7 displays the analysis of variance between credit card fraud detection and fuzzy logic. The output illustrates the p-value of 0.000 to be less than the 0.05 significant level. This indicates that the positive relationship between credit card fraud detection and fuzzy logic is highly significant at the 5% significance level, which means that fuzzy logic has a positive influence on credit card fraud detection. Thus, "the null hypothesis will be rejected at the 95% confidence interval, and the alternative hypothesis will be accepted".

6 Limitation of the Study

Sample Size & Geographical Region: One limitation of this study is the sample size of respondents which is limited to only 100 participants. The outcome of this study will be more accurate if the sample size of the respondents is increased, and the results will be more reliable. Thus, future researchers should explore expanding the sample size of respondents since test statistics usually require a large sample size to generate a greater accuracy of results for the study. Also, the geography of the respondents used in this study was restricted to a single region (Malaysia), as opposed to having a global perspective of the expert's opinion. This means thatthe findings of this study might not be sufficient to properly gain an understanding of the expert's knowledge on artificial intelligence and credit card fraud detection. In this regard, future researchers should consider collecting data from target respondents in developed countries like the United States of America, given that it also has a problem of identity theft and are more advanced in utilizing artificial intelligence to detect fraudulent financial transactions.

Independent Variable Constraint: In this study, the independent variables are confined to three: "machine learning, data mining, and fuzzy logic-based systems". These independent factors are insufficient to fully assess the advantage of artificial intelligence in the detection ofcredit card fraud. This is because artificial intelligence is a broad concept with different layersand algorithms which means in order to fully understand the application of AI in credit card fraud detection, future researchers should investigate the different classification algorithms like "Neural Networks, Naïve Bayes, Random Forest, SVM and Decision tree" which are all commonly used for financial fraud detection.

This would ensure that the research is narrowed down to AI algorithms instead of artificial intelligence as a whole, which gives the expert a better understanding of the statements in the questionnaire survey. Thus, future researchers should consider selecting independent

variablesthat the target respondents are familiar with, to widen the scope of knowledge and provide a different perspective to the findings in this study.

Data Collection Method: Similar to the limitation highlighted previously, the structure and statements in our questionnaire survey might have certain flaws that prevent it from capturingthe right response from the respondents. The questionnaires used in this study might be missingcertain questions that would address certain areas omitted in this study and make it easier for the target respondents to comprehend the questions. For example, a number of the phrases areoverly broad and vague, which may have influenced the feedback received. As a result, it wouldbe more appropriate to modify the statements in the survey in order to investigate the researchtopic and obtain a more comprehensive or relevant result. Moreover, it is evident that the resultsof this study would be more reliable if the researcher conducted interviews as a form of data collection rather than questionnaires. Nevertheless, the results are still accurate because the structure of our questionnaire was closed-ended. Consequently, given that the researcher has little extensive experience in primary data collection, the statements in the questionnaire couldbe structured better in a future study.

Time Constraint: This research was conducted in a short period of time (six months), which is not nearly enough time to extensively investigate the application of artificial intelligence incredit card fraud detection, given the vast amount of research that needs to be done in this areato obtain the appropriate result. Thus, future research should schedule enough time to researcha topic of the magnitude in order to properly analyze the data collected and complete the objective of the research is reliable and credible.

7 Conclusion

This research was performed to investigate the application of artificial intelligence in credit card fraud detection. This study aimed to investigate the application of artificial intelligence techniques as a fraud detection mechanism that can effectively and efficiently detect credit card fraud and identify fraudulent financial transactions. Previous studies have highlighted the vastpotential of artificial intelligence as a fraud detection mechanism that accurately spots anomalies in transactions performed by customers and notifies the organization or experts of any suspected red flags, which prevents further financial loss. The findings of our research revealed that the three artificial intelligence techniques machine learning, data mining, and fuzzy logic used to detect fraudulent transactions were revealed to have a significant positive relationship with credit card fraud detection. This indicates that the application of artificial intelligence provides experts with better accuracy and efficiency in detecting fraudulent transactions. As a result, fraud examiners, auditors, accounting and finance experts, and several organizations continue to implement and apply artificial intelligence as a fraud detection tool in order to spot anomalies and identify fraudulent transactions effectively and efficiently.

Although several organizations and experts are more comfortable with their traditional approach to credit card fraud detection, this study reveals that experts are beginning to adopt this new model of fraud detection to enhance their operation, improve accuracy, and carry outtheir duties on time. Hence, the independent variables, machine learning, data mining, and fuzzy logic appear to have a significant relationship with credit card fraud detection, and all the variables have a positive relationship as well as a high accuracy in detecting fraudulent financial transactions. The findings in this research will be beneficial to practitioners across theaccounting and finance industry, forensic accountants, and regulatory bodies as well as create awareness regarding the continuous advancement of technologies and digital transactions, which has led to several challenges that can no longer be effectively handled with a traditional approach. As a result, this research will provide some knowledge to practitioners on the importance of applying artificial intelligence techniques as a fraud

detection mechanism in order to properly detect credit card fraud and prevent fraudulent financial transactions in the future.

8 Recommendation

Credit card fraud is a growing concern that has caused several issues for practitioners and victims due to the difficulties they encounter in detecting fraudulent acts. Based on this study, we have highlighted several limitations and improvements that could be made in future research to enhance the scope of the study and provide practitioners, organizations, and fraud examiners with additional knowledge. The recommendations in this study have been made based on the limitations and conclusion of the research. One of the recommendations is to extend the time frame of the research to a period longer than six months. As stated earlier, a topic of this magnitude requires a flexible schedule and a time frame of no less than one year to adequately investigate the application of artificial intelligence in credit card fraud detection and accurately analyse the data collected to reflect the best possible outcome. Another recommendation is to increase the sample size to more than 100 and target respondents in countries with more advanced artificial intelligence technologies. The author also recommendsthat given the high rate of identity fraud in Malaysia, fraud examiners, auditors, and organizations in the country should consider applying artificial intelligence technologies in their fraud detection and prevention policies in order to have an edge over the fraudsters and effectively detect anomalies in financial transactions.

In addition, organizations must implement artificial intelligence training and awareness programs so that employees and managers can spot unusual transactions and other red flags asthey occur. This would allow an organisation to keep track of the fraudsters in real-time and deploy the necessary measures to combat the fraudster's techniques using artificial intelligence.Likewise, organizations should encourage employees to engage in cyber security training programs both to educate themselves and develop the necessary skills to utilise artificial intelligence-based fraud detection tools. Furthermore, victims should be aware of the threat ofidentity theft and remain conscious of their responsibilities to protect their personal information to prevent criminals from getting a hold of their credit card information to perform fraudulent transactions. Finally, for future research on a topic like this, we recommend conducting interviews to provide a more accurate and reliable conclusion or outcome. Further research canalso be conducted on specific artificial intelligence algorithms such as Neural Networks and Naïve Bayes to see how each algorithm performs in terms of accuracy and efficiency in detecting fraudulent transactions (credit card fraud). Subsequently, the research could suggestvarious ways in which experts can incorporate these techniques.

References

1. I. Agur, S.M. Peria, C. Rochon, International Monetary Fund Special Issue on COVID-19, 1–13 (2020)
2. Pumsirirat, L. Yan, International Journal of Advanced Computer Science and Applications **9**, 01 (2018)
3. M.J. Alam, M.I. Kamrul, S.M. Zia Ur Rashid, S.Z. Rashid, Engineering and Technology (ICISET), 451-454 (2018) DOI: 10.1109/ICISET.2018.8745647
4. S.W. Albrecht, C.O. Albrecht, C.C. Albrecht, M.F. Zimbelman, *Fraud Examination (6th ed.)* (Cengage Learning, 2018)
5. B.C. Amanze, H.C. Inyiama, M.O. Onyesolu, International Journal of Computer

Sciences and Engineering **6(6)**, 1333-1343 (2018)

6. R.B. Asha, S.KR. Kumar, Credit card fraud detection using artificial neural network. Global Transitions Proceedings **2(1)**, 35–41 (2021) DOI: https://doi.org/10.1016/j.gltp.2021.01.006
7. S.M.S. Askari, M.A. Hussain, Journal of Information Security and Applications **52**, 102469 (2020) DOI: https://doi.org/10.1016/j.jisa.2020.102469
8. Association of Certified Fraud Examiners [ACFE]. Report to the Nations (2020) DOI: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf
9. J.O. Awoyemi, A.O. Adetunmbi, S.A. Oluwadare, Credit card fraud detection using machine learning techniques: A comparative analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI). Published (2017) DOI: https://doi.org/10.1109/iccni.2017.8123782
10. B. Wiese, C. Omlin, Credit Card Transactions, Fraud Detection, and Machine Learning: Modelling Time with LSTM Recurrent Neural Networks. Innovations in Neural Information Paradigms and Applications (2009) DOI: 10.1007/978-3-642-04003-0_10
11. L.M. Bahsin, Wulfenia Journal **23(2)** (2016)
12. R. Banerjee, G. Bourla, S. Chen, M. Kashyap, S. Purohit, Comparative Analysis of Machine Learning Algorithms through Credit Card Fraud Detection. 2018 IEEE MIT Undergraduate Research Technology Conference (URTC). Published (2018) DOI: https://doi.org/10.1109/urtc45901.2018.9244782
13. T.K. Behera, S. Panigrahi, Advances in Intelligent Systems and Computing, 835–843 (2017) DOI: https://doi.org/10.1007/978-981-10-3874-7_79
14. S.M. Bragg, Fraud Examination: Second Edition: Prevention, Detection, and Investigation. AccountingTools, Inc. (2019)
15. C. Chukwuneke, “Credit card fraud detection system using intelligent agents and enhanced security features,” 06 2018.
16. Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining-based system for credit-card fraud detection in e-tail. Decision Support Systems, 95, 91–101. https://doi.org/10.1016/j.dss.2017.01.002
17. Carvajal, G., Maucec, M., & Cullick, S. (2018). Components of Artificial Intelligence and Data Analytics. Intelligent Digital Oil and Gas Fields, 101–148. https://doi.org/10.1016/b978- 0-12-804642-5.00004-9
18. Castelli, M., Manzoni, L., & Popovic, A. (2016). An Artificial Intelligence System to Predict Quality of Service in Banking Organizations. Computational Intelligence and Neuroscience, 2016.
19. Chong & Steve, K, H. (2016). Cybercrime Precursors: Towards a Model of Offender Resources. Australian National University, Thesis. https://openresearch-repository.anu.edu.au/handle/1885/107344
20. Columbus, L. (2020, May 19). How E-Commerce’s Explosive Growth Is Attracting Fraud. Forbes. https://www.forbes.com/sites/louiscolumbus/2020/05/18/how-e-commerces- explosive-growth-is-attracting-fraud/?sh=6e4084cf6c4b
21. Cressey, D. (1953). Other People’s Money: A Study in the Social Psychology of Embezzlement, Free press, Glencoe, IL.
22. D. Dighe, S. Patil, and S. Kokate, “Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study,” 08 2018, pp. 1–6.

23. Das, P. K., Tripathy, H. K., & Yusof, M. S. A. (2021). Privacy and Security Issues in Big Data: An Analytical View on Business Intelligence (Services and Business Process Reengineering) (1st ed. 2021 ed.). Springer.
24. de Sá, A. G., Pereira, A. C., & Pappa, G. L. (2018). A customized classification algorithm for credit card fraud detection. Engineering Applications of Artificial Intelligence, 72, 21– 29. https://doi.org/10.1016/j.engappai.2018.03.011
25. Deng, W. Huang, Z. Zhang J. and Xu, J. (2021). A Data Mining Based System For Transaction Fraud Detection. IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), 2021, pp. 542-545, doi: 10.1109/ICCECE51280.2021.9342376.
26. Denis, D. J. (2018). SPSS Data Analysis for Univariate, Bivariate, and Multivariate Statistics (1st ed.). Wiley.
27. disruptive technology. (n.d.). Oxford Reference. Retrieved September 1, 2021, from https://www.oxfordreference.com/view/10.1093/oi/authority.20110810104753313
28. Dutta, S. Gupta, A. K. & Narayan, N. (2017). Identity Crime Detection Using Data Mining. 3rd International Conference on Computational Intelligence and Networks (CINE), pp. 1-5, doi: 10.1109/CINE.2017.18.
29. El Naby, A. A., El-Din Hemdan, E., & El-Sayed, A. (2021). Deep Learning Approach for Credit Card Fraud Detection. 2021 International Conference on Electronic Engineering (ICEEM). Published. https://doi.org/10.1109/iceem52022.2021.9480639
30. Fernando, (2020).
31. https://repositorio.yachaytech.edu.ec/bitstream/123456789/120/1/ECMC0015.pdf
32. Goyal, R. & Manjhvar, A, K., (2020). Review on Credit Card Fraud Detection using Data Mining Classification Techniques & Machine Learning Algorithms.. IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.7, Issue 1, Page No pp.972-975: https://ssrn.com/abstract=3677692
33. Huang, J. (2020). Credit Card Transaction Fraud Using Machine Learning Algorithms.
34. Semantic Scholar, DOI:10.2991/icesed-19.2020.14
35. ICAEW. (2018, September). Artificial intelligence and the future of accountancy. Global Accountancy Advance. https://www.icaew.com/-
36. /media/corporate/files/technical/technology/thought-leadership/artificial-intelligence-report.ashx
37. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1–20. https://doi.org/10.2308/jeta-10511
38. Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018). Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism. IEEE Internet of Things Journal, 1–1. doi:10.1109/jiot.2018.2816007
39. John, S., Anele, C., Kennedy, O. O., Olajide, F., & Kennedy, C. G. (2016). Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm. 2016 International Conference on Computational Science and Computational Intelligence (CSCI). Published. https://doi.org/10.1109/csci.2016.0224
40. Kültür, Y., & ÇAğlayan, M. U. (2016). Hybrid approaches for detecting credit card fraud.
41. Expert Systems, 34(2), e12191. https://doi.org/10.1111/exsy.12191

42. Kumar, M. S., Soundarya, V., Kavitha, S., Keerthika, E., & Aswini, E. (2019). Credit Card Fraud Detection Using Random Forest Algorithm. 2019 3rd International Conference on Computing and Communications Technologies (ICCCT). Published. https://doi.org/10.1109/iccct2.2019.8824930
43. Kumar, P., & Iqbal, F. (2019). Credit Card Fraud Identification Using Machine Learning Approaches. 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT). Published. https://doi.org/10.1109/iciict1.2019.8741490
44. Larson, G. (2019). How to use AI to fight identity fraud. [Online]. TechBeacon. Available at: https://techbeacon.com/security/how-use-ai-fight-identity-fraud [Accessed 21 Sep 2019].
45. Lee, N. (2021, February 1). Credit card fraud will increase due to the Covid pandemic, experts warn. CNBC. https://www.cnbc.com/2021/01/27/credit-card-fraud-is-on-the-rise-due- to-covid-pandemic.html
46. Li, Z., Liu, G., Wang, S., Xuan, S., & Jiang, C. (2018). Credit Card Fraud Detection via Kernel- Based Supervised Hashing. 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). Published. https://doi.org/10.1109/smartworld.2018.00217
47. "Maharjan, A., & Chudal, P. (2020) Comparative Analysis of Algorithms for
48. Credit Card Fraud Detection. KEC Conference. http://kec.edu.np/wp-content/uploads/2020/01/Paper_36.pdf"
49. Mahmud, M. S., Meesad, P., & Sodsee, S. (2016). An evaluation of computational intelligence in credit card fraud detection. 2016 International Computer Science and Engineering Conference (ICSEC). Published. https://doi.org/10.1109/icsec.2016.7859947
50. Mehndiratta, S. & Gupta, K. (2019). Credit Card Fraud Detection Techniques: A Review. International Journal of Computer Science and Mobile Computing, Vol. 8, Issue. 8, pg.43
51. 49. https://ijcsmc.com/docs/papers/August2019/V8I8201911.pdf
52. Mishra, S. P., & Kumari, P. (2019). Analysis of Techniques for Credit Card Fraud Detection: A Data Mining Perspective. Advances in Intelligent Systems and Computing, 89–98. https://doi.org/10.1007/978-981-13-9330-3_9
53. Mittal S., Tyagi S. (2020) Computational Techniques for Real-Time Credit Card Fraud Detection. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham. https://doi.org/10.1007/978-3-030-22277-2_26
54. Modi, K., & Dayma, R. (2017). Review on fraud detection methods in credit card transactions. 2017 International Conference on Intelligent Computing and Control (I2C2). doi:10.1109/i2c2.2017.8321781
55. Moody, M. (2019, November 12). How Artificial Intelligence Uncovered Evidence of Fraud. ACFE Insights. https://www.acfeinsights.com/acfe-insights/2018/12/14/how-artificial- intelligence-uncovered-evidence-of-fraud
56. Naqvi, A. (2020). Artificial Intelligence for Audit, Forensic Accounting, and Valuation: A Strategic Perspective (1st ed.). Wiley.
57. Ngai, E., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). The application of data

mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

58. Niu, X., Wang, L., & Yang, X. (2019). A Comparison Study of Credit Card Fraud Detection: Supervised versus Unsupervised. ArXiv, abs/1904.10604.
59. Nkomo, B. K., & Breetzke, T. (2020). A conceptual model for the use of artificial intelligence for credit card fraud detection in banks. 2020 Conference on Information Communications Technology and Society (ICTAS). doi:10.1109/ictas47918.2020.23398
60. Paruchuri, H. (2017). Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review. ABC Journal of Advanced Research, 6(2), 113-120. https://doi.org/10.18034/abcjar.v6i2.547
61. PricewaterhouseCoopers. (2020). PwC's Global Economic Crime and Fraud Survey 2020.
62. PwC. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
63. Prusti, D., & Rath, S. K. (2019). Web service-based credit card fraud detection by applying machine learning techniques. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). Published. https://doi.org/10.1109/tencon.2019.8929372
64. Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. Expert Systems with Applications, 35(4), 1721–1732. https://doi.org/10.1016/j.eswa.2007.08.093
65. Rambola, R., Varshney, P., & Vishwakarma, P. (2018). Data Mining Techniques for Fraud Detection in Banking Sector. 2018 4th International Conference on Computing Communication and Automation (ICCCA). Published. https://doi.org/10.1109/ccaa.2018.8777535
66. Rasha, K. & Andrew H. (2012). "The New Fraud Triangle'': Journal of Emerging Trends In Economics And Management Sciences, Vol.3 (3): Retrieved From Google.Com on September 3, 2014
67. Razooqi, T., Khurana, P., Raahemifar, K., & Abhari, A. (2016). Credit card fraud detection using fuzzy logic and neural network. SpringSim. DOI:10.22360/springsim.2016.cns.009
68. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018). Deep learning detecting fraud in credit card transactions. 2018 Systems and Information Engineering Design Symposium (SIEDS). Published. https://doi.org/10.1109/sieds.2018.8374722
69. Ruankaew, T. (2016). Beyond the fraud diamond. International Journal of Business Management and Economic Research (IJBMER), vol. 7 issue 1, pp. 474-476.
70. Saeed, S, K. (2019). A Fraud-Detection Fuzzy Logic Based System For The Sudanese Financial Sector. Vol 20, No 1.
71. http://journal.sustech.edu/index.php/JECS/article/view/398
72. Saunders, M. N. K., Lewis. P. Thornhill. A. (2016). Research Methods For Business Students.
73. PEARSON.
74. Save, P., Tiwarekar, P., N., K., & Mahyavanshi, N. (2017). A Novel Idea for Credit Card Fraud Detection using Decision Tree. International Journal of Computer Applications, 161(13), 6–9. https://doi.org/10.5120/ijca2017913413
75. Sekaran, U. & Bougie, R. (2016) Research Methods for Business: A Skill-Building

Approach.

76. 7th Edition, Wiley.
77. Shakya, R,. (2018). Application of Machine Learning Techniques in Credit Card Fraud Detection. UNLV Theses, Dissertations, Professional Papers, and Capstones. 3454. http://dx.doi.org/10.34917/14279175
78. Sisodia, D. S., Reddy, N. K., & Bhandari, S. (2017). Performance evaluation of class balancing techniques for credit card fraud detection. 2017 IEEE International Conference on Power, Control, Signals, and Instrumentation Engineering (ICPCSI). doi:10.1109/icpcsi.2017.8392219
79. Sorournejad, S., Zojaji, Z., Atani, R.E., & Monadjemi, A. (2016). A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective. ArXiv, abs/1611.06439.
80. Sorunke & Abayomi, O. (2016). Personal ethics and fraudster motivation: The missing link in fraud triangle and fraud diamond theories. International Journal of Academic Research in Business and Social Sciences, vol. 6 issue 2.
81. Sujana, E., Yasa, I., & Wahyuni, M.A. (2019). Testing of Fraud Diamond Theory Based on Local Wisdom on Fraud Behavior. DOI:10.2991/teams-18.2019.3
82. Syeda, M., Yan-Qing Zhang & Yi Pan. (2002). Parallel granular neural networks for fast credit card fraud detection. 2002 IEEE World Congress on Computational Intelligence. pp. 572-577 vol.1, doi: 10.1109/FUZZ.2002.1005055.
83. Syeda, M., Yan-Qing Zhang, & Yi Pan. (2002). Parallel granular neural networks for fast credit card fraud detection. 2002 IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems. FUZZ-IEEE'02. Proceedings (Cat. No.02CH37291). doi:10.1109/fuzz.2002.1005055
84. Taha, A. A., & Malebary, S. J. (2020). An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine. IEEE Access, 8, 25579–25587. https://doi.org/10.1109/access.2020.2971354
85. Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-time Credit Card Fraud Detection Using Machine Learning. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). Published. https://doi.org/10.1109/confluence.2019.8776942
86. Tran, P. H., Tran, K. P., Huong, T. T., Heuchenne, C., HienTran, P., & Le, T. M. H. (2018). Real Time Data-Driven Approaches for Credit Card Fraud Detection. Proceedings of the 2018 International Conference on E-Business and Applications - ICEBA 2018. Published. https://doi.org/10.1145/3194188.3194196
87. Tripathi, K. K., & Pavaskar, M. A. (2012). Survey on Credit Card Fraud Detection Methods. International Journal of Emerging Technology and Advanced Engineering, 2(11). doi=10.1.1.414.3256
88. Vardhani, P. R., Priyadarshini, Y. I., & Narasimhulu, Y. (2018). CNN Data Mining Algorithm for Detecting Credit Card Fraud. SpringerBriefs in Applied Sciences and Technology, 85–93. doi:10.1007/978-981-13-0059-2_10
89. Wolfe, D. & Hermanson, D, R. (2004).The fraud diamond: Considering four elements of fraud. The CPA Journal, vol. 74 issue 12, pp. 38-42.
90. Yazici, Y. (2020). Approaches To Fraud Detection On Credit Card Transactions Using Artificial Intelligence Methods. Department of Computer Engineering. https://aircconline.com/csit/papers/vol10/csit101018.pdf
91. Yee, O. S., Sagadevan, S., & Malim, N. H. A. H. (2018). Credit card fraud detection

using machine learning as data mining technique. Journal of Telecommunication, Electronic and Computer Engineering, 10(1–4), 23–27.

92. Zareapoor, M., & Shamsolmoali, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. Procedia Computer Science, 48, 679–685. https://doi.org/10.1016/j.procs.2015.04.201
93. Zareapoor, M., Seeja.K.R, S., & Afshar Alam, M. (2012). Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria. International Journal of Computer Applications, 52(3), 35–42. https://doi.org/10.5120/8184-15