

Exploratory Factor Analysis On AApplication in Financial Fraud Detection

Gouri Anilkumar
Student
Thiruvananthapuram, India
anilkumargouri750@gmail.com

Dr. Suresh Subramoniam
Director
CET School of Management
Thiruvananthapuram, India
sureshsubramoniam@gmail.com

Abstract—Artificial intelligence and machine learning algorithms are used in the rapidly expanding field of artificial intelligence enabled financial crime detection to spot and stop financial crimes. Financial institutions can enhance their compliance efforts and lower risk of financial crimes by adopting AI. In this exploratory study attempt has been made to identify some of the major factors that enable AI to spot and prevent potential financial crimes where traditional methods fail. The items were identified from literature, and an exploratory factor analysis was conducted. A total of 20 items were identified and a questionnaire based on these items were formulated and responses were collected online. After the analysis the 20 items were grouped under five factors and these factors were termed as technology, accuracy, integration, adaptability and speed.

Keywords- Artificial intelligence, Financial crimes, Detection, Identified.

I. INTRODUCTION

Financial institutions and governments throughout the world have been quite concerned about financial crimes. The most prevalent financial crimes that endanger the stability of financial systems are fraud, money laundering, and cybercrime. Artificial intelligence and other technologies have been developed as a result of the financial crimes epidemic to aid in detection and prevention of financial crime.

Recent years have seen a substantial increase in interest in the application of artificial intelligence (AI) in the identification of financial crimes has been demonstrated in numerous research. For instance, a Deloitte study discovered that employing AI can assist reduce false positives and identify sophisticated financial crimes that are challenging to find using traditional approaches. The advantages of AI in identifying fraud and money laundering are also highlighted in a paper by McKinsey, which includes faster detection, improved accuracy, and lower costs (McKinsey, 2020). Achim and Borelea (2020), emphasis the significance of efficient regulatory and enforcement measures in combating financial crimes. It gives a general overview of economics and financial crimes as well as tips for spotting and avoiding financial crimes with application of artificial intelligence. Alsedrah (2017), opined the use of artificial intelligence in a variety of fields, such as in finance the application of AI technologies, including machine learning, robots, and natural language processing to reduce financial frauds. Basley (2000) in his study on fraudulent financial reporting was done to determine how industry characteristics and corporate governance practices affect the

prevalence of financial fraud are crucial in preventing misleading financial reporting. Bello (2017), in his study explained its key concepts and applications of AI, impact on numerous industries including banking.

According to Benaich and Hogarth (2019), a thorough assessment on the state of AI was release, detailing its development and possible effects on numerous industries. He pointed out an important development in AI as well as its ethical and social implication. Biddle (2017) conducted thorough analysis of studies done on the effects of various fraud techniques. The study underlined the necessity for businesses to put strong fraud prevention measures in place, including good governance, internal controls, and employee training programmes for the effective implication of AI in fraud detection. Broadhurst (2019) give a summary of the present state of the application of AI to crime investigation, criminal profiling, predictive policing and drawbacks of using AI to prevent crimes, such as bias and privacy issues. Charanjit (2021) conducted a study on the topic of effective solutions for anti-money laundering and counter-terrorist financing. The study focuses on the adoption of AI and decrease the likelihood of fraudulent activity. D'Andrea and Marcelloni (2019) in their study state the application of deep autoencoder neural network to find irregularities in banking transactions. It gives a thorough analysis of the methodology and examines the possibilities of this approach in enhancing the accuracy and effectiveness of fraud detection.

Hentzen and Hoffmann (2022) examined the possibilities of AI in financial services with customers. Their study identified numerous research gaps and points to potential areas for future investigation on artificial intelligence (AI) can aid in enhancing risk management, lowering expenses, and improving customer experience in financial service sector. In a 2011 policy discussion paper on financial system abuse, financial crime and money laundering, the International Monetary Fund (IMF) examines the connections between financial crimes and money laundering. The report talks on the dangers of money laundering and how it affects financial stability, national security and economic growth. In order to combat financial crimes, the IMF suggests a multifaceted strategy that includes preventive measures, legal frameworks and international cooperation.

Wang (2010) pointed out that many data mining methods, such as neural networks, decision trees, support vector machines and association rules, that have been used to find accounting fraud. According to him, those methods have been effective in spotting false financial statements,

changing accounting ratios and fabricating transactions. Wang also examines the techniques drawback such as the requirement for massive volumes of data and the difficulty in handling unbalanced datasets. Sen et al., (2022) pointed out the potential of artificial intelligence (AI) and machine learning (ML) algorithms can be used to identify the odd trends and transactions which could help in stopping the fraud. Sherly and Nedunchezian (2020) examined an algorithm-based adaptive system for detecting credit card fraud. The system can identify frauds by examining a number of variables, including the transaction's location, kind, and value.

I. PROBLEM STATEMENT

Traditional detection techniques find it difficult to keep up with the complexity of financial crimes. There are problems to be overcome, such as the need for accurate and reliable data and the potential for preexisting biases to be reproduced and maintained by AI models. The challenges are figuring out how to effectively use AI for financial crimes detection while resolving these concerns and ensuring the moral and responsible use of the technology.

II. RESEARCH OBJECTIVES

The main objectives are:

- a) To study the application of AI in financial crime detection through literature review.
- b) To identify factors responsible for AI adoption in financial crime detection using Exploratory Factor Analysis.

III. METHODOLOGY

The study is carried out to conduct exploratory factor analysis for the purpose of identifying factors responsible for AI adoption in financial crime detection. Here the primary data is collected through a survey using a questionnaire method. The sample gathered through online survey and questionnaire are provided to working professionals from IT department in banks using Google form. A subset of individuals or units from a larger group or population that are selected for this study refers to sample. Statistical analysis will be performed on the surveyed data using IBM SPSS.

A. Reliability of the Instrument

Table 1: Reliability of the instrument

Reliability Statistics	
Cronbach's Alpha	
	.883

Based on Cronbach's Alpha, the reliability of the questionnaire is measured. According to Table 1, its value is 0.883 which is well above 0.7. Thus, the instrument developed is acceptable from the reliability point of view.

B. Sample Size

Selecting a sample size is considered to be most relevant decision to be made while conducting any study. There are several opinions and guiding rules of thumb in the literature for selecting a sample size (Gorsuch 1983; Tabachnick and Fidell 2001; Hogarty, Hines et al.2005). A total of 200 samples were drawn from the population of IT professionals working in banks. For this study purposive sampling method is used and sample size is ten times the number of items.

C. Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy/Bartlett's Test of Sphericity

Table 2: KMO Measure of Sampling Adequacy and Bartlett's Test of Sphericity

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	.855
Approx. Chi-Square	1397.777
Bartlett's Test of Sphericitydf	190
Sig.	.000

Based on Kaiser-Meyer-Olkin (KMO) sampling adequacy can be measured (Kaiser 1970). KMO value above 0.70 suggest that the data is adequate for conducting Exploratory Factor Analysis (Netemeyer, Bearden et al. 2003). In this study, the KMO value of 0.855 as seen in the Table 2 indicates that the data is adequate. Another measure, Bartlett's test of Sphericity (Bartlett 1950), it provides a chi-square value that must be significant (Bartlett 1950). According to the Table 2, which means that the data is adequate enough for Exploratory Factor Analysis (Hair, Anderson et al.1995a; Tabachnick and Fidell 2001).

D. Factor Extraction Method

Here principal component analysis is used to obtain initial factor solution. This is the most commonly used factor extraction method. PCA is used when there is no prior theoretical basis or model exists (Gorsuch 1983). It is pointed out the reason for the wide use of PCA since it is the default method in many statistical software (Thompson 2004). Moreover, (Pett, Lackey et al. 2003) it is recommended for using PCA in establishing preliminary solutions in exploratory factor analysis (Pett, Lackey et al. 2003).

Table 3: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.467	32.334	32.334	6.467	32.33	32.334
2	1.667	8.337	40.671	1.667	8.337	40.671
3	1.458	7.289	47.959	1.458	7.289	47.959
4	1.231	6.157	54.116	1.231	6.157	54.116
5	1.065	5.327	59.443	1.065	5.327	59.443
6	.987	4.935	64.378			
7	.888	4.442	68.820			
8	.755	3.773	72.592			
9	.678	3.391	75.984			
10	.659	3.293	79.277			
11	.608	3.039	82.316			
12	.542	2.709	85.026			
13	.507	2.535	87.560			
14	.454	2.271	89.831			
15	.417	2.086	91.917			
16	.384	1.921	93.838			
17	.356	1.782	95.620			
18	.319	1.593	97.213			
19	.296	1.481	98.694			
20	.261	1.306	100.000			

Extraction Method: Principal Component Analysis.

According to Kaiser's method (Kaiser 1960). Eigenvalues greater than one should be retained for further interpretation. Number of components or factors are identified with the eigenvalues of more than one. Table 3, shows that there are five component having eigenvalue greater than one. Thus, the stated set of 20 variables represents 5 components. The identified 5 component is shown in Table 5 is based on these items rest of them got deleted. There are 5 component jointly explain 59.44% of the variance.

E. Rotated Component Matrix

The idea of rotation is to reduce the number of factors on which the items under investigation have high loadings. If the value is lower than the required value of 0.5 or the set limit for one of the components, then that items cannot be considered for the further analysis. From Table 4, there are five components named as technology, accuracy,

integration, adaptability and speed. Technology comprises of new payment system, updation of technology, new patterns development. Accuracy comprises of specialization in AI, precise detection with AI tool, benefit of banks from accurate results. Integration comprises of data mart integration, behavioural data, integration of non-financial transaction in data mart. Adaptability comprises of especially skilled resources for adaptation of AI, compared to traditional method AI is better and challenges in adaptation of AI. Speed comprises of dependence on AI technique used, depends on regulatory, customer experience and performance of AI system.

Table 4: Rotated Component Matrix

Items	Components				
	1	2	3	4	5
Qn_16	.696				
Qn_8	.684				
Qn_7	.676				
Qn_4	.560				
Qn_5	.542				
Qn_2	.528				
Qn_12		.847			
Qn_9		.670			
Qn_13		.625			
Qn_11		.683			
Qn_20			.711		
Qn_14			.686		
Qn_10			.406		
Qn_15			.520		
Qn_18				.710	
Qn_1				.675	
Qn_17				.653	
Qn_19				.717	
Qn_3					.812
Qn_6					.666

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

F. Identified factors

The Table 4, shows the classification of items into different component as per the factor loadings. Here the factors

identified is up shown in Table 5 are named as technology, accuracy, integration, adaptability and speed.

Table 5: Identified Factors

SI.NO	Factors	Items
1	Technology	-New payment system -Updation of Technology -New patterns development
2	Accuracy	-Specialization in AI -Precise detection with AI -Benefit to banks with accurate results
3	Integration	-Data mart integration - Behavioural data -Integration of non-financial transaction in data mart
4	Adaptability	-Specially skilled resources for adaptation of AI -Compared to traditional method AI is better -Challenges in AI adaptation
5	Speed	-AI technique used -Depends on regulatory -Customer Experience -Performance of AI system.

G. Component Correlation Matrix

As per Table 6, component correlation matrix shows low inter component correlation values of -.285 except in one case where it is .450, all components are important. These 5 components represent 5 factors which are significant.

Table 6: Component Correlation Matrix

Component	1	2	3	4	5
1	.273	.171	.470	.383	.126
2	-.240	.273	-.176	-.042	-.285
3	-.450	-.152	.208	.219	-.247
4	-.119	.130	-.174	.323	.241
5	-.212	.150	.101	-.278	.124

Extraction Method: Principal Component Analysis

Rotation Method: Oblimin with kaiser Normalisation

IV. CONCLUSION

Table 4 leads to the conclusion that of five factors were identified from the exploratory factor analysis (technology, accuracy, integration, adaptability, and speed). This study shows a strong relationship between application of AI in banks, as banks deal with substantial transaction volumes and complex networks of interactions. The adaptation of AI is both superior to traditional methods, due to its ability to analyse vast amount of data, spot patterns, and discover abnormalities that could be signs of potentially fraudulent activity, artificial intelligence Hence, artificial intelligence (AI) has become increasingly used in financial fraud detection.

REFERENCES

- [1]. Achim, M. V., & Borelea, S. N. (2020). Economic and financial crime: Detection, prevention, and strategy. Springer International Publishing, volume 20.
- [2]. Alsedrah, M. (2017). Artificial intelligence. International Journal of Advanced Research in Computer Science, 8(5), 150-156.
- [3]. Al-Suwaidi, A. K., Nobanee, H., & Jabeen, F. (2018). The causes of cybercrime: An empirical study. Journal of Financial Crime, 25(2), 346-358.
- [4]. Bartlett, M.S. (1950). "Tests of significance in factor analysis. British Journal of Psychology 3(2): 77-85.
- [5]. Beasley, M.S., Carcello, J.V., Hermanson, D.R., & Neal, T.L. (2000). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. Accounting Horizons, 14(4), 441-454
- [6]. Bello, I. (2017). Beginners guide to Artificial Intelligence 'AI'. Becoming Human.
- [7]. Benaich, N., & Hogarth, I. (2019). The state of AI report. MMC Ventures.100-114.
- [8]. Biddle, S.J., Bengoechea García, E., Pedisic, Z., Bennie, J., Vergeer, I., Wiesner, G. (2017). Effect of various fraud practices: A systematic review of reviews.10(1),195-210.
- [9]. Boland, A., Cherry, M. G., & Dickson, R. (2017). Doing a systematic review: A student's guide (2nd ed.). Sage Publications Ltd.
- [10]. Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., Wang, J. (2019). Artificial Intelligence and Crime. Social Science Research Network.
- [11]. Charanjit Singh, W. L. (2021, Volume 24). Can artificial intelligence,RegTech and CharityTech provideeffective solutions for anti-moneylaundering and counter-terrorfinancing initiatives incharitable fundraising. Journal of money laundering Controle, 464-482.
- [12]. D'Andrea, E., Lazzerini, B., & Marcelloni, F. (2019). Anomaly detection in financial transactions using deep autoencoder neural networks. IEEE Access, 7, 111697-111707.
- [13]. Gorsuch, R. (1983). Factor Analysis., Hillsdale, NJ: Erlbaum.
- [14]. Gottschalk, P. (2010). Financial crime: A global problem. Journal of Money Laundering Control, 13(3), 185-195.
- [15]. Hair, J., R. Anderson, et al. (1995a). Multivariate data analysis. New Jersey, Prentice-Hall Inc.
- [16].Harrast, S. A., & Mason-Olsen, C. (2007). The effectiveness of audit committees in preventing management fraud. Journal of Forensic Accounting, 8(1), 1-24.
- [17]. Hentzen, J. K., Hoffmann, A., Dolan, R., & Pala, E. (2022). Artificial intelligence in customer-facing financial services:agenda for future research. the International Journal of BankMarketing ; Bradford , Vol. 40, Iss. 6, (2022): 1299-1336.
- [18]. Hogarty, K., C. Hines, et al. (2005). The Quality of Factor Solutions in Exploratory Factor Analysis: The Influence of Sample Size, Communalilty, and Overdetermination." Education and Psychological Measurement. 65(2): 202-226.
- [19]. International Monetary Fund. (2001). Financial system abuse, financial crime, and money laundering. IMF Policy Discussion Paper, 01(2).
- [20]. Kaiser, H. (1960). "The application of electronic computers to factor analysis." Educational and Psychological Measurement 20: 141-151.
- [21]. Kaiser, H. F. (1970). "A Second-Generation Little Jiffy." Psychometrika 35(4): 401-415.
- [22]. Netemeyer, R. G., O. Bearden, et al (2003). Scaling Procedures: Issues and Applications. London, Sage
- [23]. Pett, M. A. N. R. Lackey, et al. (2003). Making Sense of Factor Analysis: The use of factor analysis for instrument development in health care research. California, Sage Publications Inc.
- [24]. Sen, R., Heim, G., & Zhu, Q. (2022). AI and ML in cybersecurity: Application, Challenges and opportunities for MIS. Communication of the Association for Information Systems, (2022), pp. 179-209,51(1).
- [25]. Sherly, K. K., & Nedunchezian, R. (2010). Credit card fraud detection system using genetic algorithm. Expert System with Application, 37(1), pp.130-136.
- [25]. Tabachnick, B. G. and L. S. Fidell (2001). Using multivariate statistics. Needham Heights, MA, Allyn & Bacon.
- [26]. Thompson, B. (2004). Exploratory and confirmatory factor analysis: understanding concepts and applications. Washington, DC, American Psychological Association.
- [27]. Wang, S. (2010). A comprehensive survey of data mining-based accounting-fraud detection research. International Conference on Intelligent Computation Technology and Automation.

APPENDIX

Sl.NO	Items	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	Financial crimes are going up with the evolvement of new payment systems and applications.					
2.	Financial Crime Detection requires continuous technology upgradation and data modelling to equip the current methods with an rise in financial crimes.					
3.	Using AI and Machine Learning can help financial institutions to monitor and build patterns for suspicious transactions and other illegal frauds.					
4.	Relevance of having separate team of people with specialization in AI and ML play a major role in generating accurate result of financial crime detection .					
5.	Banking industry is most likely to benefit with accurate detection of financial crime with application of AI					
6.	AI based tools would help in precisely detecting Fiancial crimes in your organisation,if it is not implemented so far					
7.	Having a Data Mart or Data Lake with data from all touch points is the key challenge in using the AI /ML based application					
8.	Having access to behavioural data would help in enhancing financial crime detection using AI.					
9.	Non-financial transaction in data mart would help AI in better financial crime detection.					
10.	Using AI-enabled financial crime detection might escalate the cost for					

	compliance for financial institution.					
11.	Using AI-enabled financial crime detection has reduced the role of human analysts in financial sector.					
12.	AI implementation is sufficient enough to detect the new pattern of Financial Crimes.					
13.	The rule-based AML/Transaction monitoring systems are efficient to detect new types of Financial Crimes.					
14.	Need for specially skilled resources to manage the implementation of AI/ML in Financial Crimes					
15.	AI adaptation is much better than traditional methods of financial crime detection					
16.	Lack of resources with expertise and know-how is the biggest challenges in adaptation of AI in financial crime detection.					
17.	Speed of AI-enabled financial crime detection system could depend on the specific AI techniques used.					
18.	The speed generating an AI-enabled financial crime detection system could depend on the regulatory and policy environment in which it operates.					
19.	AI-enabled financial crime detection enhances customer experience in the financial sector.					
20.	The performance of the AI system could depend on the quality, scalability of the underlying technology infrastructure based on which the speed is identified.					