American Journal of Technology Advancement 2997-9382, Vol 02, No. 12, 2025

*Article*

# Explainable AI-Driven Behavioral Analytics for Detecting Emerging Financial Crime Patterns in Digital Banking Systems

Mohammad Ali
*MASTER of SCIENCE IN BUSINESS ANALYTICS, TRINE UNIVERSITY*
Mohammadali6833@gmail.com

Md Shahadat Hossain
*MASTER of SCIENCE IN BUSINESS ANALYTICS, TRINE UNIVERSITY*
shahadat130122@gmail.com

Professor Parvin Sultana Haider
*Principle (in-charge) Dhaka College, National University of Bangladesh*
*Professor in Economics*

**Abstract:** With the rise in digital banking and online payment systems, financial crimes have become more complex and sophisticated, necessitating the adoption of intelligent and transparent fraud detection methods. The study aims to explore how Explainable Artificial Intelligence (XAI) through Behavioral Analytics can be leveraged for the detection of emerging patterns in financial crime within digital banking systems. The study uses an exploratory research approach with the secondary research methodology. R Studio is used to conduct exploratory analysis of the chosen dataset to understand transaction patterns, risk factors, device patterns, and payment processes related to fraudulent transactions. We conducted a secondary research analysis of existing scholarly work on AI, behavioral analytics, machine learning fraud detection, and explainable AI. The outcomes of visualization analysis are important patterns in relation to fraud distribution, abnormal transaction behavior, behavioral risk indicators, and device based fraud patterns. The results prove the effectiveness of the detection of financial crimes based on several behavioral characteristics and not one. The study demonstrates that the combination of explainable AI and behavioral analytics can enhance the transparency, accountability, and understanding of AI fraud detection decisions. The findings of this study will be useful in the development of responsible AI solutions to enhance digital banking security and aid in the identification of new or changing financial crime schemes.

**Keywords:** Digital Banking, Online Payment, Financial crimes, Behavioral Analytics, Fraudulent Transaction, Explainable Artificial Intelligence, R Studio, AI, Dataset, Exploratory Study.

## I. Introduction

### *A. Background of the Study*

The widespread use of digital banking systems and online payment platforms has revolutionized the financial world, making transactions quick, convenient, and automated. This shift to the digital world has also heightened the risk of sophisticated financial crimes that involve fraudulent transactions, account takeover attacks and unusual payment activity. The traditional rule based fraud detection systems are weak in capturing new fraud schemes, as they rely on predefined rules and lack of behavioral knowledge [1]. One of the solutions that has shown promise is the use of Artificial Intelligence (AI) and machine learning techniques, which can detect hidden trends in the data of transactions and flag them for investigation.Artificial Intelligence (AI) and machine learning techniques have proven to be effective by analysing massive amounts of transaction data and identifying hidden trends that are associated with fraudulent activities. Behavioral analytics is another valuable tool in fraud detection, analyzing customer transaction patterns, device actions, login behaviors and customer financial trends. AI-based models, however, have a drawback in terms of transparency and interpretability due to their growing complexity, especially when dealing with decision-making processes of high impact in the financial sector. To address this challenge, Explanatory Artificial Intelligence (XAI) has emerged as a solution that enables financial institutions to grasp the underlying logic behind AI-driven predictions and boosts confidence in AI-powered fraud detection tools [1]. Recent studies emphasize the need to incorporate explainability into financial crime detection models to ensure accurate and transparent identification of financial crime.

### *B. Problem Statement*

With the advancement of increasingly sophisticated attack techniques and the increasing prevalence of online financial services, the landscape of digital banking fraud has become more complex. While AI-powered fraud detection tools offer robust tools for detecting suspicious transactions, many of the advanced machine learning models operate as black-box systems, making it hard for financial institutions and security analysts to understand how these models reach their conclusions [2]. Lack of transparency makes it difficult to determine the rationale behind particular transactions that are considered fraudulent, and reduces confidence in automated decision making processes. In addition, traditional fraud detection methods are typically based on predictive accuracy and do not consider behavioral factors that drive financial crime dynamics. Thus, the development and implementation of an explainable AI-driven approach that integrates behavioral analytics with fraud detection tools to detect risk signals, gain transparency and facilitate responsible banking decisions is necessary in digital banking environments. The existing research highlights that XAI tools can improve the financial AI's accountability and interpretability [2].

### *C. Aim of the Research*

This study aims to evaluate the potential of explainable AI for detecting emerging financial crime trends in digital banking systems by leveraging exploratory data analysis (EDA) methods for analysing transaction behaviors, risk indicators and suspicious activity.

### *D. Research Objectives*

The objectives of this research are:

1. To conduct a critical evaluation of behavioral patterns related to the fraudulent activities in digital transactions.
2. To acknowledge essential indicators of financial crime present in digital banking transaction data.
3. To conduct exploratory technique on the chosen dataset using R Studio for determining fraud-related patterns.
4. To investigate the use of explainable AI in optimizing the transparency and understanding of AI-based fraud detection.
5. To study real-time patterns of financial crime associated with transaction behavior, device usage, and risk factors.

### *E. Significance of the Study*

The study is important in the context of financial crime detection in digital banking systems, as the researchers seek to understand the impact of explainable AI and behavioral analytics. By analysing transaction patterns, user behavior, and risk-related indicators, the research provides insights into the factors associated with fraudulent activities. The study is useful for financial institutions to create clearer and more accurate methods to fight fraud using AI. Also, it enhances trust and accountability in AI decision-making processes, enabling stakeholders to grasp the rationale behind AI predictions. The results can help researchers and bankers to solve new fraud threats with responsible and explainable AI solutions.

## II. Literature Review

### *A. Artificial Intelligence Applications in Digital Banking Fraud Detection*

As digital banking services are becoming more widespread, there has been a significant need for intelligent systems that can accurately detect fraudulent financial activities. AI is an increasingly valuable tool in the fight against financial crimes, as it can sift through massive amounts of data and uncover patterns that traditional methods might miss. Choi and Lee [3] state that AI techniques offer valuable benefits in financial fraud detection by enhancing the ability of banking systems to analyse complex financial behaviors and detect suspicious activities. The research also notes, however, that an implementation of AI needs to be carefully considered because inaccurate predictions can have an impact on customer trust and financial decision making. This means while AI aids in the detection process, it is also essential that the data used is high quality and the right models are employed.

Given the ability of machine learning and deep learning to detect unusual transaction patterns, they are extensively used in digital banking fraud detection. As mentioned by Hernandez Aros et al. [4] the artificial intelligence-based fraud detection models can assist in enhancing financial security by learning from the past transactional data, and detecting anomalies from normal user behavior. The findings show how AI models can identify complex fraud patterns better than traditional rule-based models. The study concludes, however, that many of the AI strategies are primarily concerned with achieving a high predictive accuracy level and giving little explanation as to why a specific transaction is deemed fraudulent. This restriction poses problems for financial institutions that need crystal clear decision making.

AI in fraud detection is crucial for tackling the ever-changing landscape of cyber financial fraud, especially in the modern banking environment. Ali, et al. [5] found that artificial intelligence techniques can be very effective in detecting fraudulent transactions through behavioral and transactional patterns. The authors do stress, however, that fraud detection systems need to be continually developed as fraudsters find ways to circumvent existing security measures. AI applications used in digital banking should therefore not only be geared towards making the detection more accurate but also include explainability and understanding of behavior to aid in the reliable prevention of financial crime.

### *B. Behavioral Analytics for Identifying Financial Crime Patterns*

Financial crime detection in recent years has made behavioral analytics an important area of research due to the fact that fraudulent operations are not necessarily linked to the value of transactions but rather, to the changes in the behavior of customers. Behavioral analytics can detect unusual activity, like spending patterns, login activity, and device usage, that can be a sign of fraud based on transaction frequency. Chen et al. [6] state that behavioral analysis helps in identifying fraud by analyzing unusual user activity and offers more information on suspect financial transactions. But the research shows that behavior analysis isn't something that can be done once and for all; as customers' behavior evolves over time, static detection methods can lead to false results.

Using behavioral indicators has enhanced financial institutions' ability to identify new fraud patterns in digital banking systems. Fraud detection models that include behavioral features are

more effective to identify financial crimes that are more complex in nature, as stated by West and Bhattacharya [7] that fraud detection models based on behavioral features may consider the association between transactions and user behavior. This study proposes that analysis of customer behavior can decrease false positive cases than traditional methods. The research also uncovers the necessity of having accurate and comprehensive user information for effective behavioral analytics, presenting challenges for privacy and data management.

Behavioral analytics works to detect fraud by combining various risk indicators in a digital payment context. Carcillo et al. [8] argue that a combination of transaction behavior and using machine learning based analytical methods would be more effective in detecting fraudulent activities since financial crimes are typically multi-connected. The study describes how unusual transaction amounts, unusual locations and unusual payment patterns can be of great value in predicting fraud. However, the findings indicate that behavioral models should be carefully designed as relying too heavily on past behaviors can hinder identification of all new fraud methods.

Behavioral analytics combined with AI has opened up the possibilities to create more adaptive financial crime detection systems. According to Salami et al. [9] AI-based behavioral analysis can recognize complex fraud patterns by observing user behavior and looking for changes that might signal a threat. The research emphasizes that behavioral analytics offers a more solid base for financial crime detection, than approaches which are solely transaction based. But it also means that future systems should be more transparent because financial institutions must know about the impact of behavioral factors on fraud predictions. Thus, a balanced approach that includes both behavioral analytics and explainable AI could be the best way to detect fraud accurately and make decisions that are easy to understand.

### *C. Machine Learning Approaches for Financial Fraud Prediction*

One of the most important reasons for the growing interest in machine learning for financial fraud prediction is its ability to process vast amounts of transactional data and detect intricate patterns linked with fraud. Machine learning models are able to learn from historical financial data, whereas traditional rule-based methods can't. Machine learning methods are highly effective in the prediction of frauds, as they can discover hidden relationships between transaction attributes and frauds outcome [10]. Nevertheless, the study also points out that machine learning models are faced with challenges when dealing with imbalanced datasets, as fraudulent transactions typically constitute a smaller percentage of the overall transactions than legitimate ones. This restriction may be a problem for prediction performance and should be addressed with proper data management.

Ensemble learning models, decision tree, random forest, support vector machine (SVM), and various other machine learning models have been used in the detection of financial fraud. Since financial crimes can be complex and evolve over time, multiple learning approaches can be combined together to enhance the fraud detection performance, as mentioned by Carcillo et al. [11]. The study describes the pros and cons of supervised and unsupervised learning techniques: supervised learning techniques work well if the fraud data is available with labels, whereas unsupervised learning techniques help to detect unknown fraudulent behaviors. Research, however, suggests that adding complexity to the model may undermine the interpretability, making it hard for financial institutions to make a clear decision about fraud detection.

The ability of financial institutions to detect sophisticated fraud patterns has also been enhanced with the use of deep learning and advanced machine learning techniques. In digital payment systems, Jurgovsky et al. [12] state that sequence-based machine learning models can be used to analyze the transactions conducted in a specific time window and identify suspicious behavior that deviates from the normal pattern over time. The study shows that transaction sequence analysis offers more insight than the analysis of individual transactions. The study, however, also highlights the need for more data and computational power in advanced models, potentially limiting their applicability in financial settings.

Machine learning for fraud prediction is not just about accuracy; it's also about delivering

results that are reliable and meaningful. Conducted by Abdallah et al [10] financial fraud detection systems have to perform well in terms of predictive power and meet the operational needs, as false detection of fraud impacts financial organizations and customers. Thus, today's fraud prediction methods are increasingly turning to the concept of marrying machine learning with explainable methods to enhance transparency and facilitate proper decision making in digital banking systems.

### *D. Explainable Artificial Intelligence (XAI) in Financial Decision System*

Explainable Artificial Intelligence has become relevant in financial decision systems due to the fact that many of the advanced financial AI models are complex structures that are hard to understand by humans. In financial applications, where choices can have a direct impact on customers and organizations, comprehending the logic behind AI predictions is crucial. Based on Arrieta et al. [13], describe some ways in which explainable AI can help users understand and interpret the decisions made by their machine learning models. The study also shows that full model explainability is also difficult, as increasing transparency could make the model more complex and less accurate.

In financial fraud detection, the use of XAI aids institutions in understanding the elements that lead to fraud classifications. As cited by Bussmann et al. [14], explainable AI techniques can boost the confidence in financial machine learning systems by offering explanations regarding the choices made by the models and aiding in the verification processes. The study delves into the methods that facilitate understanding of risk factors for fraud predictions, like feature importance analysis and local explanation techniques. The research, however, implies that it is important to consider how explanations are constructed to ensure that they do not generate more confusion than clarity when making decisions.

With digital banking systems, XAI can serve as an avenue for accurate fraud prediction while maintaining responsible AI practices. According to Linardatos et al. [15], explainability methods such as SHAP and LIME contribute towards improving the understanding of complex AI models by highlighting the influence of individual features on predictions. In high-risk domains like finance, explainable models have proven to be valuable for their accountabilities and regulatory needs, the study shows. Thus, when combined with behavioral analytics, XAI can help to improve the financial crime detection system by providing insights into how transaction patterns and risk indicators are linked to fraud detection.

### *E. Ethical Challenges and Transparency Issues in AI-Based Financial Analytics*

The rise of AI in financial analysis presents a number of ethical issues, including transparency, fairness, and responsible decision making. There are concerns about the privacy of personal and financial data and the proper use of customer information by AI systems. Automated systems can impact critical decisions, necessitating clear principles on transparency, accountability and fairness in the implementation of AI, as mentioned by Jobin et al. [16]. The study indicates that there are challenges in implementing principles of ethics as actionable AI governance policies within organizations.

Another significant issue with algorithmic bias in the context of financial analysis is that the training data used for the algorithms can be biased, which can lead to unfair outcomes. As pointed out by Mehrabi et al. [17], the machine learning model could potentially take in the pre-existing biases of the data that it was trained on, yielding discriminatory predictions. In financial crime detection, biased models can sometimes result in false positive or false negative results for legitimate customers and misclassify some types of financial crime. So, the dataset and model's performance must be continually evaluated to maintain fairness.

The key to enhancing trust in AI-powered financial decision systems is transparency. For financial analytics, Arrieta et al. [13] define explainability as the ability of stakeholders to grasp how an AI system makes predictions, and to detect potential mistakes. The big trouble, however, is finding the transparency as complex models can often be more predictive but less understood by humans. This provides a compromise between model accuracy and interpretation.

Another key ethical concern with AI fraud detection is data privacy, as the system needs to process a vast amount of user activity data. Uzougbo, Ikegwu and Adewusi, [18] stated that the responsible AI systems must be able to ensure that personal information is maintained confidentially and that organizations can still benefit from the insights that can be gained by analyzing the information. The study highlights the need for privacy-preserving methods to ensure customer trust in digital financial settings.

Implementing AI in an ethical manner demands ongoing surveillance, transparent governance, and responsible handling of financial information. Jobin et al. [16] state that ethical development of AI systems should enable transparency, accountability and alignment with human values. Not only should financial institutions prioritize fraud detection accuracy, but they should also strive to make sure that AI-driven analytical systems are fair and transparent.

### *F. Emerging Digital Banking Crime Patterns and Risk Indicators*

New financial crime patterns have emerged with the growth of digital banking platforms, which demand more sophisticated financial crime detection methods. Sophisticated fraud schemes like account takeover, identity manipulation and unusual payment behaviors in digital channels are evident. Modern frauds are multifaceted and difficult to detect using the traditional methods, so multiple transaction and behavioral indicators need to be analyzed to detect financial crime [19]. The study emphasizes that a transaction pattern, user behavior, and contextual information offer valuable clues in detecting suspicious transactions.

Digital banking behavior is closely linked to digital banking fraud, and to some extent, to other unusual characteristics of transactions. The usage of abnormal amounts of transactions, unusual location, irregular user activities, etc. can help identify fraudulent behavior as mentioned by Hilal et al. [5]. The study indicates that, however, fraud detection systems have to evolve constantly, as financial crimes are becoming more and more prevalent, and fraudsters are creating new ways to evade security measures.

With the rising trend of various digital payment methods, there are added risks of device behavior, logon activity and payment authentication. Machine learning based methods can be used to assist in identifying these risks by analysing the behavioral patterns and identifying deviations from normal activity. But to be effective, these detection methods must be explainable, enabling financial institutions to grasp the relationship between fraud and the indicators.

Hence, a blend of behavioral analytics, Artificial Intelligence, and explainable decision making is needed to detect the new trends and patterns of digital banking crimes. These can enable financial institutions to go beyond fraud detection and work towards a proactive stance in combating financial crimes in the future.

### *G. Research Gap*

While there is significant prior work on AI and machine learning for financial fraud detection, there are fewer studies that have examined the intersection of behavioral analytics and explainable AI to gain insights into emerging patterns in financial crimes. Few models currently available focus on predicting fraud with high accuracy and offer minimal insights on risk factors driving decisions on fraud. Hence, this study takes the gap to fill in by analysing behavioral indicators and enhancing transparency in the field of digital banking fraud detection.

## III. Methodology

### *A. Research Design*

This research is exploratory research with secondary research methodology in order to study the pattern of financial crime in digital banking systems. The exploratory approach concentrates on applying statistical methods to analyze the chosen digital payment fraud dataset and visual analysis with the help of R Studio. This method enables detection of behavioral trends, fraudulent transactions and key risk factors linked to bad practices. In addition, secondary research is carried out which involves analyzing various scholarly articles, research papers, books and online academic

publications on the development of artificial intelligence, behavioral analytics and explainable AI for fraud detection. Both of these will give a holistic view of new financial crime trends.

### *B. Dataset Description and Data Source*

The data set for this study is Digital_Payment_Fraud_Detection_Dataset.csv that specifically targets cases pertaining to digital payment transactions and fraud behavioral indicators. It is a data set that includes transaction-level information needed to understand the patterns of financial crimes in digital banking environments. The main attributes are the amount of the transaction, type of transaction, payment method, device type, device location, account age, transaction hour, number of previous transaction failures, average transaction amount, international transaction status, IP risk score, number of logins, and fraud label [20]. These variables can help you understand how the user is using the site, the risks of the transactions, and suspicious activity that could be connected to the fraudulent transactions.

The selected dataset is useful for achieving the goal of this research as it includes features of behavior and security useful for recognizing emerging financial crime patterns. Exploratory analysis and visualization of the data are done using the R Studio. The data can be used to gain insights into the behavior of real transactions and risk factors, as well as digital banking activity patterns, to understand the differences between real and fraudulent transactions. Findings from the dataset analysis are also compared to other research studies to draw links between the practical findings and previous research.

### *C. Exploratory Data Analysis Using R Studio*

The digital payment fraud data is analyzed using Exploratory Data Analysis in the R Studio software to explore the structure, distribution and behavior present in the dataset. This analysis involves data cleansing, exploration of features, statistical summaries and discovery of links between fraud indicators. The data is analyzed for transaction patterns and represented graphically with R programming libraries like dplyr and ggplot2. It can be used to identify key similarities and differences between genuine and fraudulent transactions, such as uncharacteristic transaction volumes, user activity, and the risk level of various digital payment attributes. The exploratory analysis serves as a basis to understand financial crime patterns prior to the interpretation of the results of the research.

### *D. Visualization-Based Behavioral Analysis*

The visualization based behavioral analysis is performed to uncover significant patterns in fraudulent transactions on digital banking. The analysis of fraud distribution, transaction behavior, risk indicator and user activity patterns is done using different graphical techniques and R Studio. The visualizations are concerned with knowing the relationship between transaction value, transaction behavior, device activity, logon activity and fraud occurrence. The graphical analyses, which serve as an aid to the identification of abnormal behavioral trends, may lead to the identification of potential financial crimes. The findings from the visualization analysis are analyzed and explained by referring it to literature on the existing approaches of the artificial intelligence-based fraud detection and behavioral analytics.

### *E. Secondary Research Analysis*

Secondary research analysis involves a literature review of existing academic literature like journal articles, research papers, books and online academic publications on the subject of AI for fraud detection, behavioral analytics and explainable artificial intelligence. This analysis aims to gain insight into research contributions made in the past, highlight limitations and compare results from the data analysis to past studies. This will help in building a solid theoretical foundation and aid in the understanding of the actual results from exploratory analysis.

### *F. Ethical and Explainability Consideration*

In this study, ethical issues concerning the use of AI and financial analysis of data are taken into account. Digital banking information carries with it sensitive behavioral patterns, so responsible

data handling and privacy protection is important. The study also concentrates on explainability by analysing fraud indicators and explaining them in an understandable way instead of just the prediction outcomes. This will help to keep the AI-driven financial crimes detection strategies transparent, accountable, and meaningful to stakeholders. The adoption of explainable practices helps enhance the trust and responsible decision making in digital banking fraud analytics.

## IV. Conceptual Framework

The conceptual model of this research shows the systematic relationship between the data of digital banking transactions, behavioral analysis, explainable artificial intelligence, and financial crime detection results. The framework starts with gathering digital payment transaction data, which includes behavioral, transactional, and security attributes like transaction amount, payment method, device details, logins, IP risk score, and fraud labelling. The data is then analysed and processed by using the exploratory data analysis technique in R Studio, revealing patterns, trends, and anomalies in financial transactions. As a result of the analysis, key behavioral and risk patterns linked to fraudulent actions are identified, such as varying transactions which might be abnormal, unusual spending behavior, device-related irregularities, and authentication risks. Explainable AI techniques are used to analyze the impact of each of these indicators on fraud predictions to understand their contribution, supporting AI and machine learning based fraud analysis. Finally, the framework produces results, including the discovery of new financial crime trends, the detection of high-risk transactions, a higher rate of accurate fraud detection, and clear AI-based decision making. Ongoing feedback and improvement loops keep the fraud detection approach current with evolving digital banking fraud risks and changing fraud tactics.

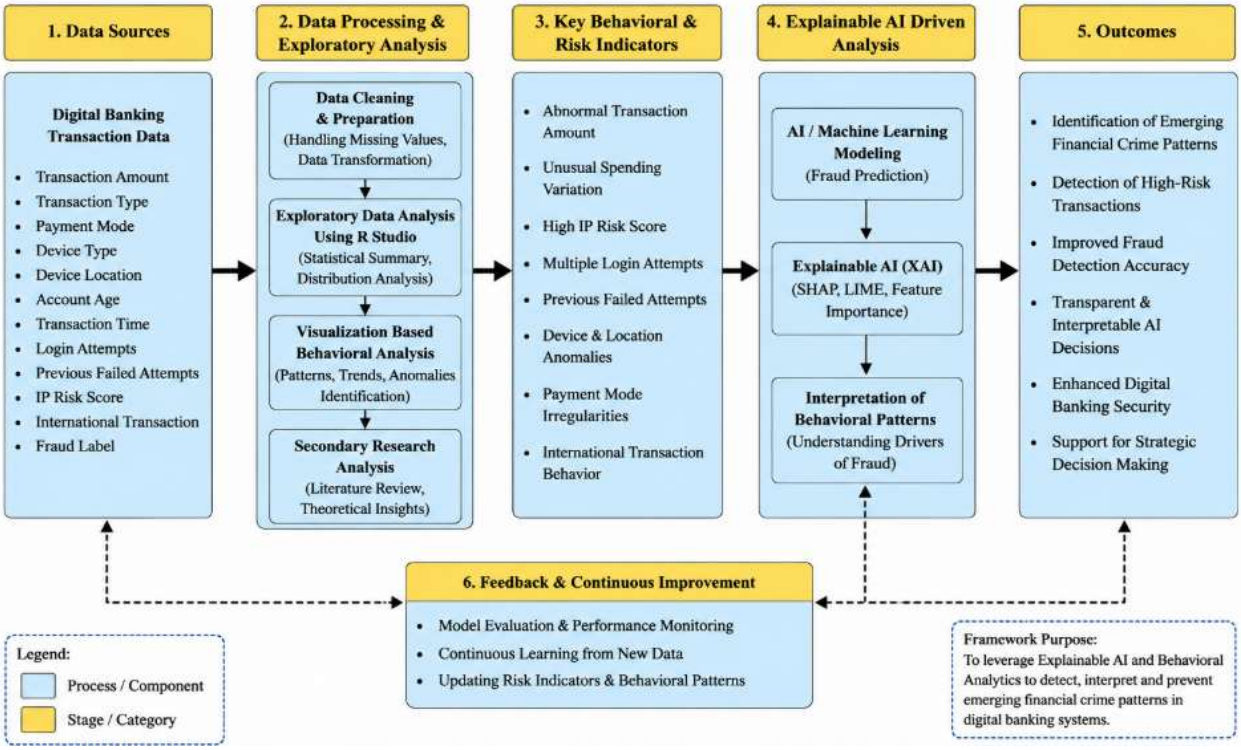


**Figure 1.** Conceptual Framework Diagram.

(Source: Created by learner)

## V. Result

### *A. Analysis of Fraudulent Transaction Distribution in Digital Payment System*

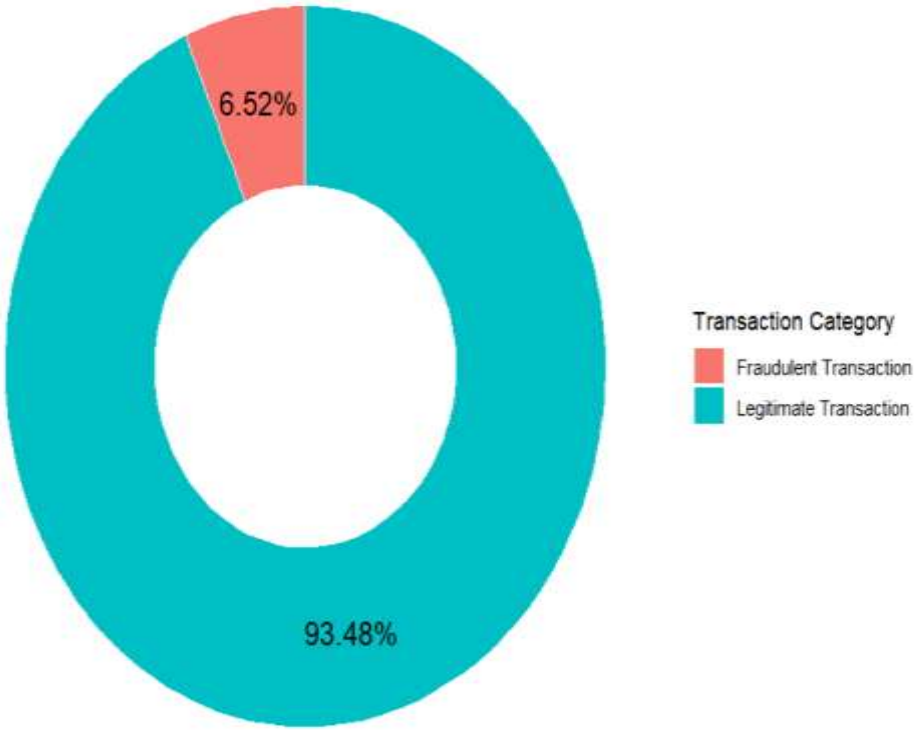


**Figure 2:** Distribution of Fraudulent and Legitimate Digital Payment Transaction.

(Source: Created by learner)

The donut chart shows the proportion of fraudulent and legitimate digital payments. As can be seen in the visualization, the majority of transactions are legitimate (93.48%), while the rest (6.52 %) are fraudulent ones. This imbalance suggests that financial crimes are not happening as regularly as with a normal transaction and making fraud detection difficult. The result highlights the importance of AI driven behavioral analytics for identifying rare but significant fraudulent activities.

***B. Behavioral Pattern Analysis Through Transaction Amount and Spending Variation***

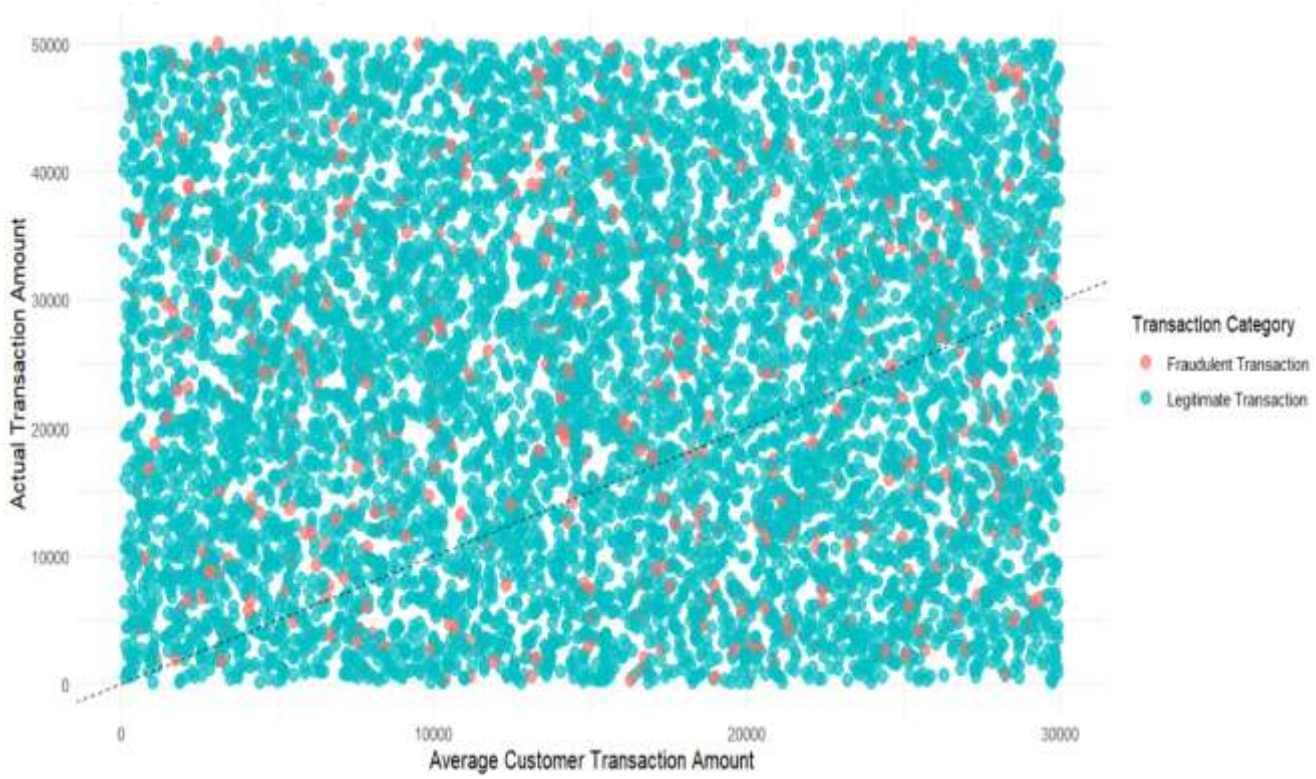


**Figure 3:** Identifying Abnormal Spending Pattern Related to Financial Fraud.

(Source: Created by learner)

The scatter plot shows the relationship between the average amount per transaction and the actual amount per transaction, and looks for any unusual customer transactions. The visualization reveals wide variations in customer financial activities with transaction values being spread across a range of spending levels. The fraudulent and legitimate transactions are distributed throughout the range of transaction values indicating that transaction amount may not be the only factor used in fraud detection. This aligns with the need for using multiple behavioral indicators for correct financial crime detection.

***C. Identification of Key Risk Indicators Associated with Financial Crime Activities***

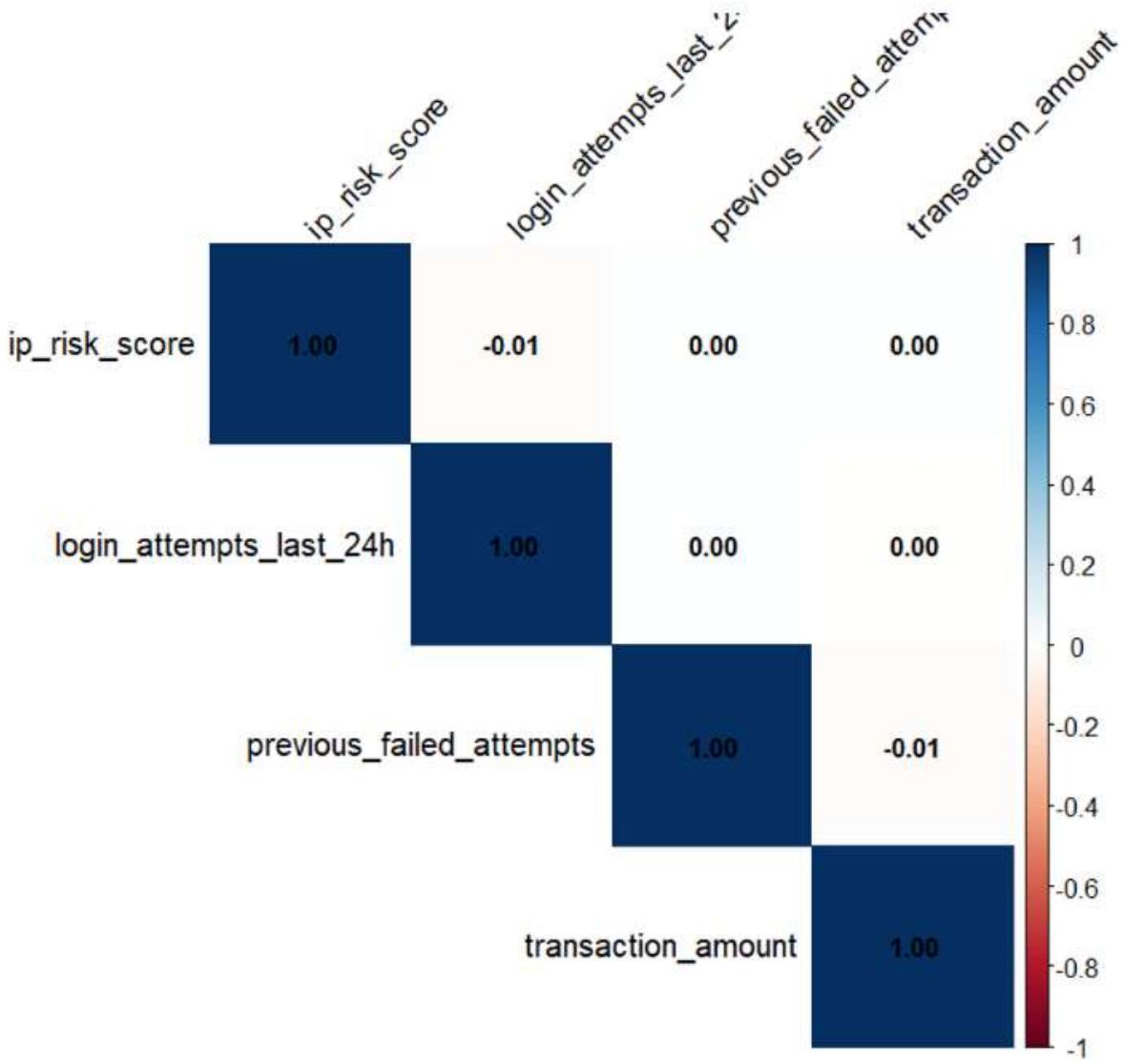


**Figure 4.** Correlational Analysis of Financial Crime Risk Indicators.

(Source: Created by learner)

The correlation heatmap refers to the relationship between these crucial behavioral and transaction risk signals such as IP Risk Score, failed login attempts, past failed logins, and transaction amount. The visualization shows that there are very weak relationships between the selected variables, which may suggest that financial crime patterns are not dependent on just one variable. Rather, fraud detection should be done by analyzing several behavioral attributes at once. This discovery is consistent with explainable AI strategies for assessing various risk factors to identify fraud transparently.

***D. Device and Payment Behavior Analysis for Detecting Emerging Fraud Patterns***

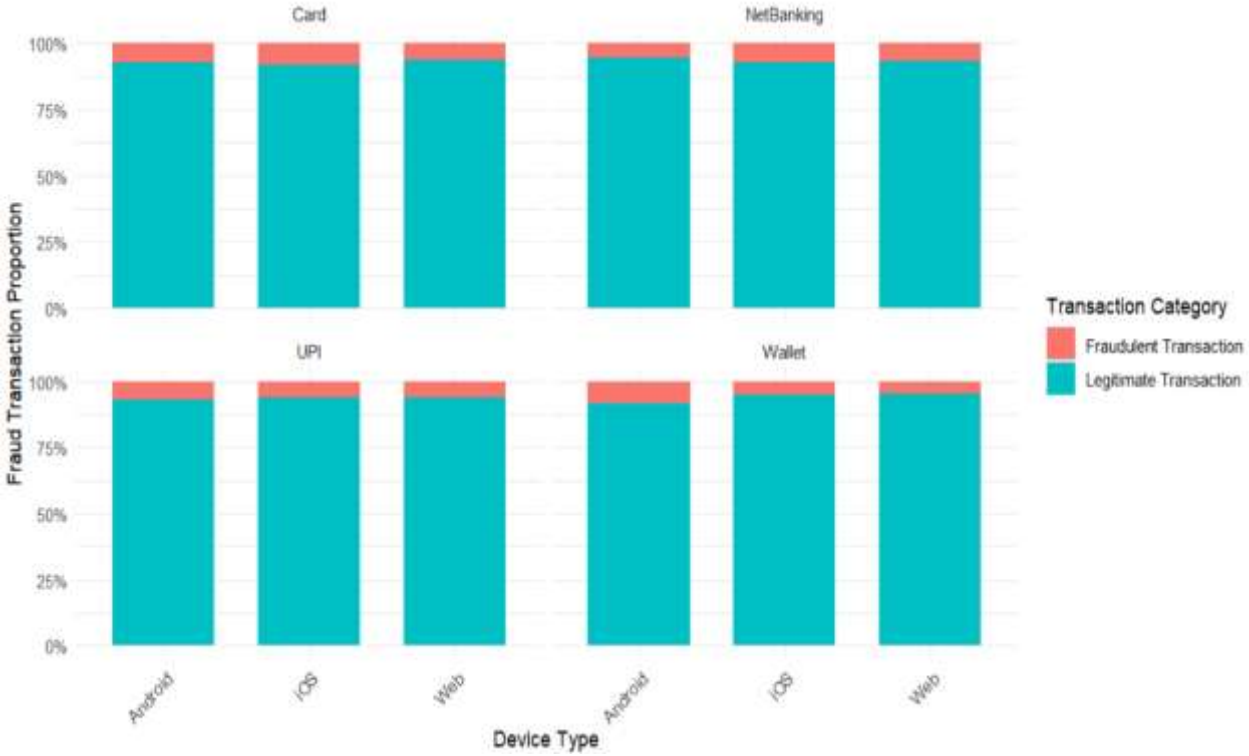


**Figure 5.** Identifying Fraud Risk Distribution across Digital Banking Channels.

(Source: Created by learner)

The stacked bar chart compares the distribution of fraud by device type and payment channel. As seen in the visualization, the percentages of fraudulent and legitimate transactions are relatively small and small respectively across all devices and payment types, with digital banking activities being dominated by legitimate transactions. But device behavior differences suggest that device behavior can be a valuable contextual clue for fraud analysis. These findings highlight the importance of considering device and payment behavior as potential indicators in AI based financial crime detection systems.

**VI. Discussion of Result/Findings**

The results of visualization analysis are valuable to help understand the patterns of financial crimes in digital payment systems. Fraud distribution analysis showed the number of fraudulent transactions as a percentage of the number of legitimate transactions is low. This is due to the fact that financial fraud happens on an infrequent basis but can cause substantial financial risk, which is a real-world challenge for financial fraud detection. The outcome reinforces the importance of intelligent detection methods that will be able to detect rare fraud without impacting on regular banking activities. The report also reveals that conventional tools, relying just on the number of transactions, could be inadequate in detecting complex financial crimes.

Results of the behavioral analysis of transaction values showed that there is a lack of ability to detect fraudulent activity solely based on differences in transaction value. The broad range of the transaction amount suggests that there can be both legitimate and fraudulent transactions at any amount. The finding underlines the significance of studying and understanding the customer behavior patterns instead of relying on the one financial variable. The correlation analysis also revealed low levels of correlation between individual risk indicators, indicating that a multi-faceted evaluation involving several behavioral risk factors like IP risk, login behavior, failed attempts, and transaction characteristics is necessary for financial crime detection. The relevance of explainable AI is further emphasized, as comprehending the role of various indicators can aid in understanding which ones are driving the fraud detection and help increase transparency.

The device and payment behavior analysis enabled further insights into the characteristics of

new digital banking fraud. The findings revealed that fraudulent activities span multiple devices and payment channels, suggesting that fraudsters can potentially take advantage of multiple digital banking environments. The discovery shows that device action, payment methods, and more can be contextual risk factors when looking at suspicious transactions. In summary, the findings are consistent with the existing literature and the critical role of AI, behavioral analytics and explainability in enhancing financial crime detection systems. The study illustrates how transaction analysis can be a useful tool for incorporating behavioral signals to enhance the ability to detect digital banking fraud patterns in an effective and transparent way.

**VII. Future Work**

The proposed study can be extended to future studies by using sophisticated machine learning and deep learning algorithms for predictive financial crime detection. The present study emphasizes exploratory analysis and visualization-based interpretation, so that further studies could combine classification models (Random Forest, XGBoost, and neural networks) to evaluate performance in the prediction of fraud. Moreover, techniques like SHAP and LIME can be used for explainable AI to uncover the impact of individual behavioral factors in fraud predictions. This would help gain more insights into the risks that affect financial automation decisions.

There is opportunity to further develop real-time fraud monitoring systems that would be constantly monitoring customer behavior and transaction activity. More extensive and varied datasets from banking contexts can be added for increased generalizability. Further research is required to address privacy concerns and ensure data security when using AI to analyze sensitive financial information. There is a need for further research to explore privacy-preserving AI methods that ensure data security and privacy while analyzing financial information. By combining behavioral analytics with explainable AI, financial institutions can enhance their ability to create responsible and transparent fraud detection systems that effectively combat the changing landscape of digital banking fraud.

**VIII. Conclusion**

The study investigated the potential of explainable AI with behavioral analytics to identify evolving financial fraud trends in digital banking. Patterns of transaction distribution, spending behavior, risk indicators, device usage and payment activity were identified as important patterns in the exploratory analysis. The results clearly illustrate that fraudulent operations can't be identified by using just one behavioral aspect and need to be analyzed against a number of behavioral aspects. The study emphasizes the need for integrating AI with behavioral analytics and explainability to enhance transparency and reliability in fraud detection. The research gives insights into the indicators of financial crime which help to develop responsible AI-based approaches to enhance digital banking's security and strengthen its fraud prevention strategies.

**REFERENCES**

[1] Y. Zhou, H. Li, Z. Xiao, J. Qiu *et al.*, "A user-centered explainable artificial intelligence approach for financial fraud detection," *Finance Research Letters*, vol. 58, Art. no. 104309, 2023, doi: 10.1016/j.frl.2023.104309.

[2] N. Rane, S. Choudhary, and J. Rane, "Explainable Artificial Intelligence (XAI) Approaches for Transparency and Accountability in Financial Decision-Making," *SSRN Electronic Journal*, 2023.

[3] D. Choi and K. Lee, "An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation," *Security and Communication Networks*, vol. 2018, no. 1, Art. no. 5483472, 2018.

[4] . Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela, J. J. Moreno Hernandez, and M. S. Rodríguez Barrero, "Financial fraud detection through the application of machine learning techniques: A literature review," *Humanities and Social Sciences Communications*, vol. 11, no. 1,

pp. 1–22, 2024.

[5] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, *et al.*, "Financial fraud detection based on machine learning: A systematic literature review," *Applied Sciences*, vol. 12, no. 19, Art. no. 9637, 2022.

[6] Z. Chen, L. D. Van Khoa, E. N. Teoh, A. Nazir, E. K. Karuppiah, and K. S. Lam, "Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review," *Knowledge and Information Systems*, vol. 57, no. 2, pp. 245–285, 2018.

[7] D. Chakraborty, A. Paul, and G. Kaur, "Microeconomics: Machine learning model with behavioral intelligence to reduce credit card fraud," *International Journal of Electronic Banking*, vol. 3, no. 4, pp. 358–378, 2022.

[8] F. Carcillo, Y. Le Borgne, O. Caelen, and G. Bontempi, "Combining unsupervised and supervised learning in fraud detection," *Information Sciences*, vol. 557, pp. 317–331, 2021.

[9] I. A. Salami, A. D. Popoola, M. O. Gbadebo, F. H. O. Kolo, and T. O. Adesokan-Imran, "AI-powered behavioral biometrics for fraud detection in digital banking: A next-generation approach to financial cybersecurity," *Asian Journal of Research in Computer Science*, vol. 18, no. 4, pp. 473–494, 2025. .

[10] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, 2020.

[11] F. Carcillo, Y. Le Borgne, O. Caelen, and G. Bontempi, "Combining supervised and unsupervised learning in fraud detection," *Information Sciences*, vol. 557, pp. 317–331, 2021.

[12] M. Jurgovsky et al., "Sequence classification for credit card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2020.

[13] A. B. Arrieta et al., "Explainable Artificial Intelligence: Concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020.

[14] N. Bussmann, P. Giudici, D. Marinelli, and J. Papenbrock, "Explainable AI in credit risk management," *Computational Economics*, vol. 57, pp. 203–216, 2021.

[15] P. Linardatos, V. Papastefanopoulos, and S. Kotsiantis, "Explainable AI: A review of machine learning interpretability methods," *Entropy*, vol. 23, no. 1, 2021.

[16] A. Jobin, I. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nature Machine Intelligence*, vol. 4, pp. 389–399, 2022.

[17] N. Mehrabi et al., "A survey on bias and fairness in machine learning," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–35, 2021.

[18] N. S. Uzougbo, C. G. Ikegwu, and A. O. Adewusi, "Legal accountability and ethical considerations of AI in financial services," *GSC Advanced Research and Reviews*, vol. 19, no. 2, pp. 130–142, 2024.

[19] E. W. T. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection," *Decision Support Systems*, vol. 50, pp. 559–569, 2020.

[20] J. Joshi, "Digital Payment Fraud Detection Dataset," Kaggle, 2025. [Online]. Available: https://www.kaggle.com/datasets/jayjoshii37/digital-payment-fraud-detection