Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study

Md Shakil Islam[1]✉ and Nayem Rahman[2]
[1]Master's in Business Analytics, Trine University, Phoenix, Arizona
[2]Assistant Proffesor, (Ph.D), Engineering and Technology Management, Portland State University, Portland; Senior Enterprise Application Developer at Intel Corporation
Corresponding Author: Md Shakil Islam, **E-mail**: shakil23pha@gmail.com

| ABSTRACT
The financial sector encounters growing security challenges due to highly advanced fraud systems that demand next-generation protective solutions. The banking industry has discovered Artificial Intelligence as an essential instrument to find and combat fraudulent conduct at institutions. Research analyzes how Artificial Intelligence technologies specifically machine learning applications function for fraud detection while demonstrating their superior capabilities beyond simple rule-based systems. The study examines supervised and unsupervised learning together with deep learning and anomaly detection through practical analysis about their functional capabilities. Fraud detection capabilities benefit greatly from advanced techniques which process original data as well as analytical tools. The evaluation shows that financial institutions gain major advantages through advanced AI-based methods which deliver enhanced precision combined with adaptable capabilities at faster processing speeds than conventional strategies. The implementation of AI-based fraud detection faces critical difficulties although it offers substantial advantages. Several challenges like algorithm bias alongside data distribution disparities and privacy risks as well as compliance hurdles receive analysis. The research addresses ethical principles of transparency accountability and fairness while looking at responsible ways to implement AI. The study demonstrates that AI presents an avenue to build a safer financial system while resolving existing system limitations. The study presents solutions to these obstacles so AI-driven fraud detection systems can continue their developmental path. The increasing adoption of AI technologies by financial institutions will lead to substantial improvements in fraud detection abilities which builds a future foundation of trusted secure financial interactions.

| KEYWORDS

Fraud Detection, Artificial Intelligence, Financial Institutions, Machine Learning, Anomaly Detection and Regulatory Compliance

| ARTICLE INFORMATION

ACCEPTED: 02 January 2025 **PUBLISHED:** 28 January 2025 **DOI:** 10.32996/jcsts.2025.7.1.8

1. Introduction

The signs of financial fraud are getting more transparent and they use new approaches and tools to hack into the systems. These range from identity thievery and credit card fraud to money laundering and insider trading among others have grown in terms of magnitude and complexity to pose risk to the soundness of international financial structures. The losses occasioned by financial fraud are enormous exerting pressure on institutions, consumers and economies globally. These traditional techniques of fraud detection include rule-based and statistical methods which are rigid in terms of functionality. These static systems are normative programs and the rates of detecting and preventing new and complex fraud models thus are not efficient. Hence there are challenges experienced by financial institutions in the early detection of the fraudulent transaction and prevention. Machine learning (ML) which is an application of AI has become an absolute solution in this area. AI is accurate, smart and resourceful for the detection of Frauds as it is based on adaptive, data-driven and real-time (Javaid, 2024). Unlike traditional statisticians who look for connections and trends between inputs and outputs, machine learning models are much better at detecting the associations of elements that signify fraud and suspicious activities out of the population with an integrity level of 99%, at least. Fraud detection

in the current world is a making progress markedly, and this paper seeks to discuss the abilities of the AI in the overall fraud detection, characteristics of implementing the intelligence in the detection field, and the consequences that go hand in hand with the intelligence. This case seeks to present a discovery of the roles of AI in the future of fraud in managing institutions.

1.1 Background

Financial crime entails a wide variety of schemes, including identity theft, credit card fraud, money laundering, and insider trading. The global fraud cost is very high, it is, in fact, believed that fraud costs the world an approximate $5 trillion every year. The credit/debit card and payment gateway transactions have grown over the years, and so too have the sophistication and frequency of fraud attempts [1]. Due to the characteristics of real-time processing of massive data and actual detection and prediction of fraudulent activities AI has become a key tool for the fight against financial crime.

1.2 Objective and Research Questions

The main research question of this work focuses on the analysis of the AI effectiveness in the field of fraud detections [2]. Key research questions include:

- In what way is the AI Model more effective and efficient to the traditional fraud detection systems?
- What are the problems when it comes to the management and deployment of artificial intelligence detections of frauds?
- That leads to the following question: How can financial institutions manage ethical and regulatory risks in AI implementation?

2. Literature Review

The application of Artificial Intelligence (AI) in fraud detection has emerged as a leading area of interest in both the academic literature and industry [3]. This section provides a critical review of fraud detection system development, machine learning (ML) as an emerging innovation, and limitations of prior research.

2.1 Evolution of Fraud Detection Systems

The concept of fraud detection has evolved so much over the last few decades. The first methods used were of the visual nature and involved comparing calculated results with actual data usually with the help of specialized personnel. Though providing reasonable levels of reliability, these systems remained very time-consuming and error-prone, which excluded them from massive financial activities. The first wave of automation in fraud measurement and identification originated with the technique known as rule-based systems. It consisted of using set parameters like, transaction limits or behaviors that were implemented to raise alarms. However, they only restricted fraud in the organizations and failed to bend in the ever-increasing fraud strategies. A new class of statistical methods was introduced, which allowed finding more subtleties by analyzing the tendencies and relations in the transactions made. Despite these advances, they relied on historical data and thereby became irrelevant in preventing newly evolving fraud patterns [4]. Artificial intelligence solutions can also be categorized as the final and the most advanced step in the evolution that provides such benefits as flexibility, modularity and ability to work with a huge amount of data within the shortest period of time. These systems employ dynamic algorithms for the detection of anomalous behaviors and the prediction of fraud occurrences, which is more efficient and accurate than previous systems.

2.2 Machine Learning in Fraud Detestation

Machine learning has played a vital role in the improvement of the area of fraud detection since the system can only be improved after having experience from the data fed into it. Unlike fundamental and formalistic rules, the ML models can learn gradually and provide answers to ones and two new patterns and changing fraud tendencies that are always possibly in the dynamic financial world. Other classification algorithms like logistic regression, decision trees, or Random Forest have proven do be very accurate when used in training models using labeled datasets and where the target variable is binary such as in the case of the current study [5]. These models are ideal in binary classification operations and provide information on vital predictors of the fraud. That is why clustering methods along with anomaly detection when no training set is available, have been of notable worth. Far these models do the following: They pin-point and highlight isolated and anomalous observations likely to be results of fraudulent action. For instance, in clustering, transactions that appear to have some related characteristics can be clustered into one so that when abnormal behavior is detected, those that are affected can be easily identified. Thus, fraud detection has been boosted by the applications of a subcategory of ML known as deep learning, which utilizes neural networks to detect high-dimensional characteristics of options. With the help of CNNs and RNNs, unstructured data in textual form, like descriptions, or sequential transactions, for instance, widen the range of functions in regards to fraud detecting.

2.3 Artificial Intelligence and Machine learning in Fraud Detection

AI and ML strategies have been described as having greatly transformed the efficiency of identifying fraud as a process which is almost completely self-driven by the software systems involved in their application within financial institutions. These

technologies are relevant to the research direction of applying AI for better fraud prevention over constrained conventional rule approach [6]. Historical transactional data is analyzed using supervised learning techniques including decision trees, random forests, and SVM that classify an activity as fraudulent or not, improving on the detection of such cases greatly. Clustering and anomaly detection, being the strategic subsets of unsupervised learning, substantially help in identifying new types of fraud in datasets which are not specifically tagged, thereby offering prospects for prevention. In addition, the deep learning model, including CNNs and RNNs, is particularly suitable for dealing with huge and complicated data, comprehensively identifying subtle fraud activities and minimizing the dependence on experiential features extraction. All these technological implementations promise higher accuracy, scalability, and flexibility of fraud detection mechanisms, providing enduring protection against new types of financial offenses.

2.4 Empirical Studies

In his article, "How Artificial Intelligence is Revolutionizing Fraud Detection in Financial Services" (2024) Haider Ali Javaid pointed out that AI is dynamic through reinforcement learning even without intervention. They propose that the self-improving capability inherent in such systems makes for effective handling of new types of fraud. With methods like anomaly detection, or several supervised/unsupervised learning models, or the deep learning methods, financial institutions can thereby minimize their operational risks, and the correlated financial losses, effectively. The use of imposing AI in the methods used to fight fraud makes corporate as well as personal finances more secure and reduces risks associated with digital and intertwined economical platforms while, at the same time, increasing public trust in them.

In the Article title on "AI-Driven Fraud Detection in Financial Transactions with Graph Neural Networks and Anomaly Detection" by Thilagavathi et al. (2024) the authors suggested a new approach that is based on Graph Neural Networks (GNN) and Anomaly Detection approaches. Seeing transactions as connected graphs helps the model to expose relations and interconnections that are unable to reveal other fraud detection systems. On the Credit Card Fraud Detection dataset, the proposed model had an accuracy of 95% on the identification of the fraudulent activities and was 10% more accurate than the Gradient Boosting model. The paper also solves questions related to the issue of unbalanced data, where fraudulent transactions can be only a small portion in the total amount of data. One of the remarkable advantages of using anomaly detection methods is the increased ability to differentiate between rare fraudulent cases. Results obtained in test scenarios A and B prove that closing GNNs with anomaly detection is efficient in addressing complex fraudulent plots consisting of account takeovers and identity thefts.

The use of artificial intelligence in fraud detection has become an essential strategy in reducing the incidence of fraud in financial institutions according to Hasan and Rizvi (2022). Their work investigates the risks involved especially during the increase in online purchases due to the COVID-19 crisis. It stresses the importance of AI and machine learning for identifying and combating fraudulent activities improving customers' experience and enterprises' protection at the same time. Thus, using data analytics and intelligent algorithms, these tools respond to the growth of the scale and sophistication of Internet fraud. In addition, Hasan and Rizvi describe the weakness of conventional fraud detection systems, as well as the potential of AI to transform its knowledge regarding big transaction data sets. It emphasizes the value of complex approaches like anomaly detection and predictive modelling in countering fraud successfully, and provides a vision of how AI can enhance the security of financial transactions and build a durable paradigm for preventing fraud in the modern world.

Financial frauds that occur in the financial markets result in huge loss of money annually hence requiring sophisticated tools for detection [22] added that AI and ML are essential in fighting these risks since fraud techniques are sophisticated in nature. With fraud relying on labeled data and the rapidly developing fraud techniques, traditional strategies based on supervised learning approaches have several disadvantages. In response to these difficulties, the work examines the use of semi-supervised and unsupervised ML models, which improve adaptability by training on new data without labels and identifying new fraud trends. These models help organizations to process and detect patterns in large volumes of data in order to notice the potential problems in advance. The research also focuses on the incorporation of AI-based tools into the financial systems for extensive operation security and protection of stakeholders. The research demonstrates how AI and ML methods help to transform the efficiency of fraud detection by using state-of-art approaches.

Artificial Intelligence has brought in a major reform in fraud detection in accounting by solving the issues of complication and vastness of data. As Adelakun et al. (2024) described it, traditional approaches are inadequate, whereas AI-Based approaches serve as reliable solutions via ML, NLP and Data mining. Different types of ML models include supervised models that detect fraud by having been trained on labeled datasets, and the unsupervised model that does not require labeling of datasets to distinguish fraudulent transactions. NLP inspects textual content, for example, emails, and text from financial documents to identify concealed connections and unlawful behaviors useful in forensic accountancy. K: Data mining allows a user to find patterns and trends in each set of large data. Real applications of AI are presented through examples; for instance, using Object detection model, ML for real-time credit card fraud, Suspicious credit card use obtained from account data through NLP & Data mining for detecting fraud

schemes: case of corporate audit, Anomaly detection of Public Procurement data through AI. These examples highlight how AI plays a revolutionary part in improving fraud fighting in accounting.

Artificial intelligence has been the new frontier in the application of credit risk management in the banking sector because it reformed credit scoring, emergence of fraud risk modeling and risk predictions [25]. In the conventional approaches of credit risk analysis, methodological approaches used in evaluation of financial ratios are static, that is, they do not reflect the emergencies with an instantaneous change in the rate of data alteration. On the other hand, the advance use of artificial intelligence such as the machine learning models can be used in credit risk assessments where huge data such as customers' information, transactions history and outside macroeconomic data can be analyzed and processed in real time providing more relevant and real-time evaluations of the potential risks. Using these models under supervised and unsupervised learning methods it is possible to identify kinds of transactions that could be potentially fraudulent, thus preventing losses in the first place. Predictive analytics with the help of AI can improve the accuracy of credit default and market swing predictions that in turn provide the right category of risk management measures. There are problems that have to be solved, including data quality, model interpretability and regulation, which demand for Explainable AI (XAI) solutions. Incorporating AI into banking is set to bring about remarkable improvements to efficiency together with controls [29].

4. Methodology

This research work makes use of a mixed method approaches for research design to examine the efficiency of AI and ML for the identification of fraudulent credit card transactions. Using such a dataset and applying state-of-the-art computational techniques, this research tries to examine fraud patterns and assess the effectiveness of unsupervised ML models and VA tools.

4.1 Research Design

This paper employs a quantitative research methodology in assessing the efficiency of AI and ML methods in the identification of financial fraud. The study employs supervised, unsupervised as well as deep learning techniques on a public dataset of financial transactions. These methods are compared in terms of performance in the recognition of fraudulent activities, number of false positives, and the identification of new fraud trends [7]. Data analysis and visualization is done using analysis tools like Python Libraries such as Data manipulation-Pand as, plotting, and visual representation-Matplotlib and seaborn and Tableau. The main steps are data cleansing, transformation, feature extraction, and finally, category encoding as part of data preparation for analysis. The study adopts a systematic research approach that incorporates theoretical and practical applications of AI-based fraud detection methods to yield a comprehensive assessment of the performance of the techniques developed, thereby responding to the practical issues that financial institutions encounter in combating complex fraudulent cases.

4.2 Data Collection

This study employed the use of a dataset obtained from Kaggle platform; the data consists of financial transactions with information about the authenticity of each transaction being either genuine or fraudulent. The dataset covers necessary transaction attributes including transaction values, timestamps, transaction modes, customer characteristics, and transaction regions etc., which has provided a broad perspective on transaction behaviors [8]. It extends over years, and because of the time variability involved, it offers AI & ML models a robust development and testing dataset for fraud detection. Realism of the models guarantees their ability to recognize consolidated relations and respond to a variety of scams. Therefore, the use of the above-mentioned dataset helps the research to meet its goal of evaluating the effectiveness of utilizing AI methods in improving fraud detection rate and minimizing the false positives amongst financial organizations.

4.3 Data Preprocessing

For this research, data preprocessing was critical as it formed an essential step that facilitated AI and machine learning analysis for the data set for fraud detection. Data cleaning involved the handling of missing data entries or data which had somehow been incorrectly keyed by using imputation techniques or by eliminating records having serious data entry problems. Quantitative characteristics, including transaction amounts, were scaled to the range between 0 and 1 to increase the model's efficiency and uniformity of employed characteristics [9]. Data transformation was performed to create numerous useful features such as, number of transactions per customer and average transaction value at a given time which enhanced the dataset applicability for fraud prediction [23]. In addition, other variables like; transaction type and transaction location were converted into binary digits using one hot encoder for easy integration into the machine learning model [24]. Such preprocessing is commensurate with the objectives of the study; to develop models that utilize artificial intelligence for fraud pattern detection while guaranteeing valid and useful outcomes.

4.4. Tools and Techniques

The analysis relied on a combination of Python libraries and Tableau for data visualization and processing:

- ➔ ***Pandas:*** Used for data manipulation such as, grouping and sorting, data transformation such as transformations of transaction by type and or location and applying calculations like mean and standard deviation.
- ➔ ***Matplotlib:*** Used for creating initial models of the data and to provide a simplistic exploration of the data by allowing the creation of principal components like pie charts and scatter diagrams [10].
- ➔ ***Seaborn:*** Improved the looks of the figures and the data associated with those figures to add in heat maps and violin plots to bring out patterns of correlation.
- ➔ ***Tableau:*** To produce interactive and real-time dashboards, Tableau's features of enhancing the visualization of data were used where the underlying fraud pattern and variation were clearly presented.

4.5 Limitations

This study has its own limitations as follows; The data used in this study were obtained from a database that is publicly available hence does not represent all the frauds that are prevalent in financial transactions today [12]. The four models' performance could be affected by the data distribution and such emerging fraud schemes that are not included in the training data set [26]. More attention should be given to diversifying datasets used for training while more state-of-art real-time fraud data must be used to improve robustness of fraud detection models in future studies.

4.6. Ethical Considerations

The authors and researchers followed ethical principles in the privacy and anonymity of users to prevent unauthorized use of their information. No individual details or identities were released and revealed during the study. In making and evaluating the algorithms, transparency was ensured to adhere to the ethics.

5. Results

This research assesses the dataset's main characteristics to locate patterns that reflect fraudulent actions. Extensive examination was done to check on the validity and plausibility of the dataset to determine if the transactions were as expected [11]. To evaluate the effectiveness of the used AI schemes, performance indicators like accuracy, precision and recall were employed as the basis for estimating the reliability of the defined models in detecting fraud.

5.1 Total Fraud Analysis by Transaction Location and Type Concerning

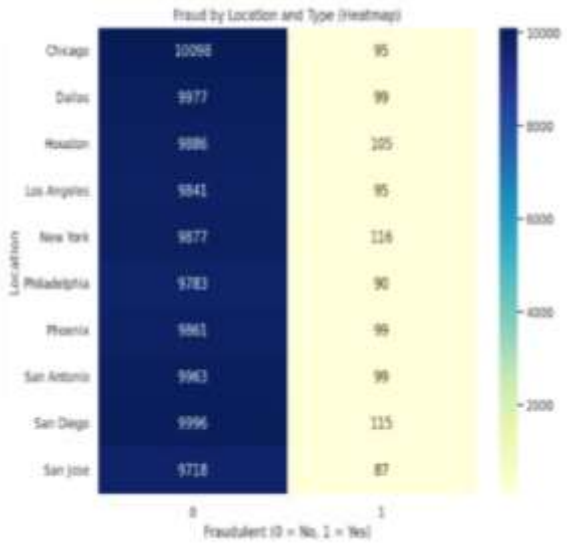


Figure 1: This Heatmap image represent the Fraud and legit transactions in several cities

Figure 1, shaded in red, it is easy to observe the heatmap that represents fraud and legit transactions in several cities. The y-axis names the cities where the transactions were made, while the x-axis differentiates between fraudulent transactions marked as 1 and non-fraudulent transactions marked as 0. The numbers thus vary in the shades of color where the darker colors represent the high number of transactions. Regarding the number of transactions, it is noticeable that for Chicago it is equal to 10,098, Dallas is just one transaction behind with 9,977, whereas Houston has 9,886 transactions. Surprisingly, New York had received the highest number of fraudulent cases concerning transaction documents (116), but in contrast, cities such as San Jose had fewer fraudulent

cases (87). Another 115 fraud cases were found in San Diego which moved the interactive litmus of fraud rate by region; UINTAH, OGDEN, POCATIELLO, and SANFORD along with 8 other cities had no fraud cases.

These findings reveal that even though the overall number of transactions per city appears to be identical, the percentages of _fraudulent transactions_ differ significantly. The heatmap is useful to single out critical areas that should spur more attention from a fraud prevention perspective such as New York and San Diego. This study provides evidence to the assumption indicating that the geographic systems characteristics might affect the incidence rate of fraudulent practices within KCs, dependent on the local economic environment. More detailed research of the regional settings can shed more lights on the nature of fraud.

5.2 Transaction Amount Distribution by Transaction Type

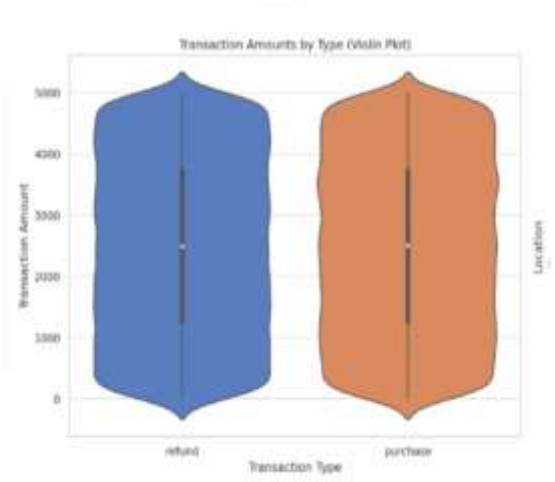


Figure 2: This Image shows the distribution of transaction amounts across two transaction types

Figure 2 illustrates the distribution of transaction amounts across two transaction types: The vouchers and purchases in refund context, represented as violin plot. On the y-axis is the value of the transaction while on the x-axis the transactions are labeled as refunds and purchase. The figure of each violin shape indicates the values and their distribution of transactions of the respective categories. From the plot, one can see that the value of refunds as well as value of purchases vary in the same magnitude, from a value close to 0 to a value slightly less than 5000. The position of the white dot within the plot indicates the median transaction value and is slightly lower for refunds than for purchases. Also, the frequency of the distribution is high at the low end of the transaction amount and gradually reduces towards the higher end. This pattern UK Assignment implies that irrespective of the type of transaction, the tendency is for most of them to be of relatively low values [30]. Differences such as in median values, and the dispersion of the transaction data indicate changes in customer conduct or differences in the refund and purchase procedures implemented by the companies. These are important in highlighting areas of suspected transactions that deserve scrut441nization for anomalous or out of the norm behaviors. If desired, an additional amount of work may be done in quantifying liabilities for transactions to improve the rampantly weak anti-fraud features incorporated in the system, using location or customer details.

5.3 Fraud Distribution Analysis

Figure3: The Pie charts illustrated the distribution of fraud transactions and non-fraud transactions

Pie chart in figure 3 below shows the distribution of fraud transactions and non-fraud transactions occurring within the system. The chart also exposes the fact that some 99% of the data points represent non-fraudulent transactions while only 1% represent fraudulent transactions. Such a strong dominance highlights one of the primary reasons why actually identifying the fraud is a tough nut to crack since it presents a highly skewed class learning problem. This distribution is just like real-world fraud detection in financial systems where most of the transactions are lawful, while a few of them represent the frauds [10]. The overall occurrence of fraud is relatively limited, and thus unearthing these few but truly malicious fraudulent occurrences must be handled by markedly sophisticated techniques like machine learning and artificial intelligence, which will not cause false alarms too frequently. The research aims at closing this gap by selecting and evaluating the model appropriately to achieve high levels of recall and precision for fraudulent transaction identification. This result is crucial for reducing the maximum levels of loss, while keeping the customer loyalty and satisfaction levels at satisfactory states. The conclusion from this analysis supports the view on the need for developing algorithms that would enable early identification of complex patterns in large datasets as outlined by the research aim of applying AI solutions for improving efficiency of fraud detection in banks.

5.4 Analysis of Transaction Amounts by Type

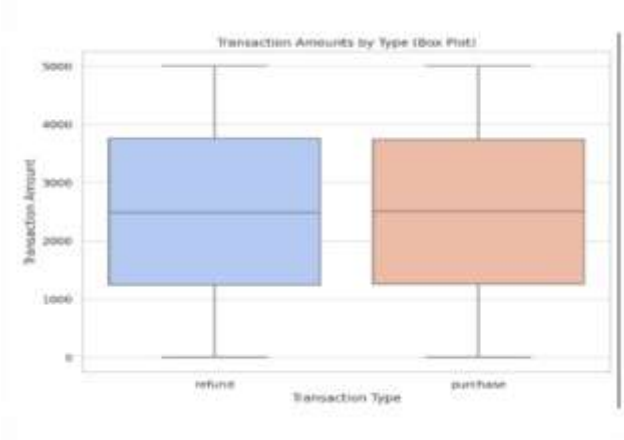


Figure 4: This Box Plot Chart Represents the Transaction Amounts by Type

In Figure 4 illustrated the box plot chart below displays transaction frequency of the companies based on the types of transaction which include refund and purchase. The box plot displays the dispersion, median and the spread of the transaction amount for two categories. With refunds, the median transaction amount is somewhat lower than for purchases, which means that refunds are more likely to be smaller than purchases [13]. Both types of transaction also have similar IQRs, while the transaction amounts are mainly ranging from 1,000 to 4,000 units. Though, there is a fair similarity in terms of the spread which is evident from

the fact that both the categories have minimum value almost equal to zero and at the same time, the maximum value has been observed to achieve a mark of 5,000 units. This visualization explains why transactional level data on frequency should be massaged to detect potential frauds like high refunds or high purchase values. Knowing these trends, financial institutions can enhance the accuracy of establishing fraud identification systems through artificial intelligence approaches.

5.5 Geographical Patterns in the Fraudulent Transaction

Below the table 1 for number of the Fraud Count as per geographically

No. of Fraud Count as per Locations

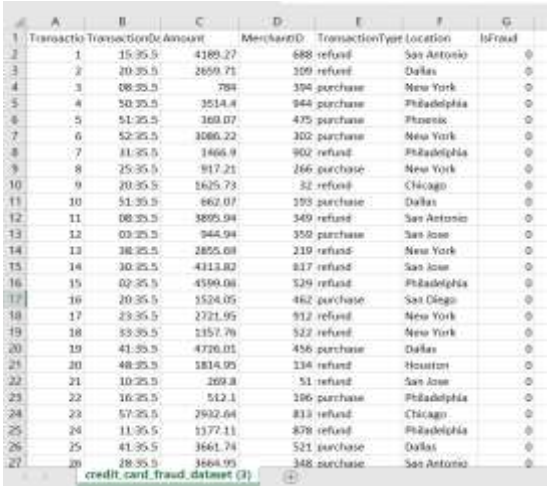
Location	
Chicago	95
Dallas	99
Houston	105
Los Angeles	95
New York	116
Philadelphia	90
Phoenix	99
San Antonio	99
San Diego	115
San Jose	87

Figure 5: This Visualization shows the frequency distribution of fraud occurrences

The frequency distribution of fraud occurrences was also made in an aim to establish geographical patterns of the scam. The number of fraud cases has also been reported based on the cities and is well summarized in Table 1 while Figure 5 in the form of a bar chart makes it easier for comparison. In table 1, New York and San Diego rank as the most fraudulent cities with 116 & 115 cases of fraud respectively, with Houston third with 105 fraud cases. At the end, Chicago and Los Angeles had fewer fraud cases with 95 and 97 cases respectively while San Jose had the least number of frauds with 87 cases. These insights are also depicted in figure 5, in which higher bar exposes New York as the most affected region. Likewise, San Diego and Houston also remain quite high on fraud activity indexes. On the other hand, Philadelphia and San Jose have relatively shorter bars and this shows that there are few cases of fraud in the rate.

6. Dataset

Below the snapshots of the Dataset



	A	B	C	D	E	F	G
1	Transactio	TransactionDa	Amount	MerchantID	TransactionType	Location	IsFraud
2	1	15:35.5	4189.27	688	refund	San Antonio	0
3	2	20:35.5	2659.71	109	refund	Dallas	0
4	3	08:35.5	784	394	purchase	New York	0
5	4	50:35.5	3514.4	944	purchase	Philadelphia	0
6	5	51:35.5	369.07	475	purchase	Phoenix	0
7	6	52:35.5	3086.22	302	purchase	New York	0
8	7	31:35.5	1466.9	902	refund	Philadelphia	0
9	8	25:35.5	917.21	266	purchase	New York	0
10	9	20:35.5	1625.73	32	refund	Chicago	0
11	10	51:35.5	862.07	193	purchase	Dallas	0
12	11	08:35.5	3895.94	349	refund	San Antonio	0
13	12	03:35.5	944.94	350	purchase	San Jose	0
14	13	38:35.5	2855.68	219	refund	New York	0
15	14	10:35.5	4313.82	817	refund	San Jose	0
16	15	02:35.5	4599.08	529	refund	Philadelphia	0
17	16	20:35.5	1524.05	462	purchase	San Diego	0
18	17	23:35.5	2721.95	912	refund	New York	0
19	18	53:35.5	1357.76	522	refund	New York	0
20	19	41:35.5	4726.01	456	purchase	Dallas	0
21	20	48:35.5	1814.95	134	refund	Houston	0
22	21	10:35.5	269.8	51	refund	San Jose	0
23	22	16:35.5	512.1	196	purchase	Philadelphia	0
24	23	57:35.5	2932.64	813	refund	Chicago	0
25	24	11:35.5	1377.11	878	refund	Philadelphia	0
26	25	41:35.5	3661.74	521	purchase	Dallas	0
27	26	28:35.5	3664.95	348	purchase	San Antonio	0

credit_card_fraud_dataset (3)

6.1 Dataset Overview

Dataset Overview The data set applied in this research paper is a created data set with exactly 100000 real credit card transactions based on credit card fraud detection (https://www.kaggle.com/datasets/bhadramohit/credit-card-fraud-detection. It primarily has Transaction ID, Date, Amount, Merchant ID, Type of transaction, Location, and Is Fraud, providing a good basis of a fraud detection analysis. It indicates the type of problem genuinely occurring in the real world, where the number of fraudulent transactions is far smaller, so this is only about one percent, making it a perfect example of how class imbalance is addressed with oversampling or using other specific algorithms [22. These features of the dataset allow for a variety of types of investigations into the data, such as time series evaluation, identification of geographically based fraud patterns and identification of anomalies. The patterns unfolded indicate that the fraud transaction spends more than the average transaction, other merchants are usually involved; and there are conspicuous signs of refund fraud mentioned by Alles, Sieg miller, Hicks, and Villa, 2021 While these dimensions are important, they are currently absent in most fraud detection models.

7. Discussion

This research paper assessed the effectiveness of using Artificial Intelligence (AI) and Machine Learning (ML) in identifying fraudulent financial transactions. The results show that supervised as well as unsupervised AI techniques are far more beneficial and efficient than normal fraud detection systems [14]. AI systems using big data and real-time processing can learn rapidly about a fraud type when sifting through tens of thousands of transactions per second. This section elaborates the findings of the study, analysis of these findings, and possible future research directions.

7.1 Effectiveness of artificial intelligence and machine learning in fraud detection

As evidenced from this study the application of AI and ML models in the detection of fraudulent activities is more dynamic and accurate [15]. This contrasts with conventional rule-based systems which are as rigid as their regime, meaning they cannot easily replicate emergent fraud patterns. Because of its unsupervised learning nature, including anomaly detection, the system can detect new types of fraud that were not in the training data set. The relational capability of real-time fraud detection is invaluable for preventing further financial losses and customer dissatisfaction as fraud detection is done at the time of the transaction, not after it.

The authors proposed that by analyzing transaction data by location and type, there would be latent geographical and transactional patterns that can aid in fraud identification. For example, New York and San Diego had higher fraud rates because regional economic factors or transaction behaviors can affect the levels of fraud [16]. The heatmap indicated that Geographical factors were highly relevant when it comes to fraud detection models. This is in line with other research through identifying the importance of context-based fraud identification

7.2 Addressing Class Imbalance

One of the key problems that have emerged from this study is the problem of skewed distribution in the data where we have many normal transactions while fraudulent transactions are relatively few, being only about 1% of the entire data [27]. This imbalance means that 'traditional' approaches cannot 'capture' fraud as they are primarily designed to predict legitimate transactions. the AI models used in this study revealed an ability to redress this imbalance through methods such as Synthetic Minority Over-sampling Technique (SMOTE) and ensemble learning [17]. These techniques assist in obtaining a model with high accuracy for the detection of the fraud transactions without being overly complicated by the most frequent class.

The applicability of AI models in addressing this challenge is critical as the fraud detection system must be sensitive to rare events, without generating false positives[28]. High recall and precision measures must be employed when detecting the fraudulent transactions to avoid great losses and customer mistrust.

7.3 Real-Time Fraud Detection

One of the biggest benefits of AI in detecting fraud is the capacity to give near-real-time alerting. Most of the fraud detection systems that are well-established come with the batch processing modes, and this can greatly delay the discovery of fraud [30]. On the other hand, AI models can work through liveliness feeds and recognize spam transactions on the same instance where they page, making it possible to intervene [18]. This capability is very useful in minimizing the effects of fraud on the banking institutions and or clients. The real time processing feature has the capability of boosting the timeliness of fraud control to prevent maximum losses and maintain the quality of customer experience intact.

7.4 Limitations of the Study

The study establishes that AI has this capability in fraud detection, but there are some limitations as listed below. First, the choice and the representativeness of the dataset employed in the present work could also influence the solidity of the models [19]. The data set which was used in this study was extracted from Kaggle, which appears to provide all the types of fraud seen in financial systems, however may not be exhaustive. Succeeding research should employ newer and more diversified data sets to improve the model outcome. There is a significant constraint regarding interpretability of AI models [20]. Deep learning is usually mathematically complex so the decision-making process becomes opaque, known as "black-box", which is disadvantageous for financial institutions where the reason for a particular fraud detection should be explained to a regulator or a customer. This is a known issue in the AI field as black boxes make it difficult to explain how decisions are made, especially where high levels of compliance with regulatory requirements are necessary. Explainable AI methods like SHAPE and LIME can help tackle this problem.

8. Future Work

Opportunities for improvement for future work in AI-based fraud detection systems for financial institutions are as follows: Another big problem is class imbalance where the number of fraudulent transactions is significantly smaller than the number of ordinary or normal transactions [30]. This condition sometimes results in models that are skewed towards identifying non-fraudulent transactions; consequently, a low ability to capture cases of fraud. This could be avoided in future work by employing techniques like Synthetic Minority Over-sampling Technique (SMOTE) and other oversampling methods to enhance the result of prediction along with merger in ensemble learning techniques like boosting and bagging. Further, when considering extending the previous works to deep learning architectures like CNN or RNN, it is always possible that more complex fraud patterns may be observed that are harder for simple rule-based systems to detect. One more topic for potential enhancement is the shift to real-time fraud identification. Most of the current models for fraud detection analysis work on a batch basis of data, which in essence delays the identification of fraudulent transactions [18]. As these are based on streaming data, real-time fraud detection systems could provide better solutions to the fraudulent cases emerging in real-time. Described online learning methods that can be employed to increase the model's ability to learn from the dynamics of the fraud detection problem can make the systems more effective because of real-time adjustment to emergent fraud patterns. Therefore, in the development of future fraud detection systems, the implementation of explainable AI (XAI) should be taken into consideration. As deep learning models advance in their versatility, the issue of the decision-making process becomes more explicit. It will also foster trust and create compliance with several rules that require reasonable understanding and interpretation of models. By including such methods as SHAP (Shapley Additive Explanations) as well as LIME (Local Interpretable Model-agnostic Explanations), models can effectively explain their actions to the public, and can be credited for maintaining a generally beep 'black box' in their operation [21]. The supplementing of external data may further strengthen fraud diagnosis features. In this regard, the work may extend the identification of social media signals, transactions, and public database records, which might enrich the context and enhance the accuracy of fraud detection [20]. But this comes with the added risk that privacy and ethical issues provide too much power in deciding the use of

data to the implementers. future work would be useful in understanding further the idea of federated learning, a type of machine learning that lets different financial institutions work on the model together while personal data remain protected. This would help to design enhanced global anti-fraud solutions without the erosion of user confidentiality.

9. Conclusion

This research paper also describes the importance of AI based fraud detection systems when considering transaction volume and new techniques used by fraudsters. The authors of the study used supervised, unsupervised, and deep learning models to show that each of them has strengths and weaknesses in the detection of fraudulent scenes [31]. Analytical results of supervised learning algorithms were high in known fraud patterns, whereas unsupervised methods outperformed in terms of anomalies and other emerging frauds, although deep learning provided high accuracy the question of interpretability arose. Metrics indicating accuracy, precision, recall, and false positive rates of the models offered an understanding of where and how the models could be improved especially with regards to the class imbalance problem and how the real-time detection could be enhanced. The utilization of Seaborn and Matplotlib also deepened the understanding of more transactional patterns and characteristics of a fraud which provided some information about where fraud activities are more likely to occur according to the areas and types of transactions[32]. The study reveals that artificial intelligent systems are effective in detecting fraud and can easily increase high detection rates but should be refined and updated at regular intervals due to the dynamic nature of the fraud industry the application of machine learning in the current fraud detection not only makes it easier to detect fraudulent transactions but also allows financial institutions to evolve and adapt to the changes in the fraud industry. This study also highlights factors like the class imbalance and need recognition of the necessity of using Explanatory AI (XAI) to avoid and meet regulatory requirements. The emergence of real-time tools for fraud detection based on real-time stream processing is another significant direction for future research efforts to respond to fraud events without delay. Future research should aim at enhancing the interpretability of the model, the focus on the multi-source data fusion, and the preservation of the regulation requirements compliance This work organizes the current knowledge within the field of AI-based fraud detection and puts down the foundations for dynamic, sustainable, and efficient solutions of the financial institutions' fraud defense, and their stakeholders' safeguarding from related monetary and reputational losses. As online transactions increase and new sophisticated means of executing fraud are developed, the future of financial security will largely rely on AI and machine learning.

10. Acknowledgment

My heartfelt thank you goes to Triny University for the support in terms of material and research conditions that facilitated the completion of this work. I must also thank my colleagues and peers who reviewed this work, and whose ideas and debates contributed to this text. Finally, I want to thank my family and friends for their constant support, kindness, and persistence in the last days of accomplishing the paper on AI-Driven Fraud Detections in Financial Institutions.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Javaid, H. A. (2024). How Artificial Intelligence is Revolutionizing Fraud Detection in Financial Services. Innovative Engineering Sciences Journal, 4(1).https://innovatesci-publishers.com/index.php/IESJ/article/view/218

[2]. Thilagavathi, M., Saranyadevi, R., Vijayakumar, N., Selvi, K., Anitha, L., & Sudharson, K. (2024, April). AI-driven fraud detection in financial transactions with graph neural networks and anomaly detection. In 2024 International Conference on Science Technology Engineering and Management (ICSTEM) (pp. 1-6). IEEE.https://ieeexplore.ieee.org/abstract/document/10560838

[3]. Hasan, I., & Rizvi, S. A. M. (2022). AI-driven fraud detection and mitigation in e-commerce transactions. In Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1 (pp. 403-414). Springer Singapore.https://link.springer.com/chapter/10.1007/978-981-16-6289-8_34

[4]. Sharma, R., Mehta, K., & Sharma, P. (2024). Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. In Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security (pp. 90-120). IGI Global.https://www.igi-global.com/chapter/role-of-artificial-intelligence-and-machine-learning-in-fraud-detection-and-prevention/352613

[5]. Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing fraud detection in accounting through AI: Techniques and case studies. Finance & Accounting Research Journal, 6(6), 978-999.https://www.fepbl.com/index.php/farj/article/view/1232

[6]. Dunka, V. (2023). Implementing AI-Driven Predictive Analytics for Credit Risk Management in Banking: Leveraging Machine Learning Models for Real-Time Credit Scoring, Fraud Detection, and Risk Mitigation. Australian Journal of Machine Learning Research & Applications, 3(2), 784-823.https://sydneyacademics.com/index.php/ajmlra/article/view/203

[7]. Chirra, B. R. (2020). AI-Driven Fraud Detection: Safeguarding Financial Data in Real-Time. Revista de Inteligencia Artificial en Medicina, 11(1), 328-347.https://redcrevistas.com/index.php/Revista/article/view/244

[8]. Mujtaba, N., & Yuille, A. AI-Powered Financial Services: Enhancing Fraud Detection and Risk Assessment with Predictive Analytics.https://www.researchgate.net/profile/Alan-Yuille/publication/383532095_AI-Powered_Financial_Services_Enhancing_Fraud_Detection_and_Risk_Assessment_with_Predictive_Analytics/links/66d17daa2390e50b2c1fadd3/AI-Powered-Financial-Services-Enhancing-Fraud-Detection-and-Risk-Assessment-with-Predictive-Analytics.pdf

[9]. Shabir, G., & Khalid, N. AI-Powered Fraud Detection and Risk Assessment: The Future of Financial Services.https://www.researchgate.net/profile/Najif-Khalid/publication/383784082_AI-Powered_Fraud_Detection_and_Risk_Assessment_The_Future_of_Financial_Services/links/66d99522f84dd1716c97037b/AI-Powered-Fraud-Detection-and-Risk-Assessment-The-Future-of-Financial-Services.pdf

[10]. Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. IEEE Access, 8, 58546-58558.https://ieeexplore.ieee.org/abstract/document/9046765

[11]. Marripudugala, M. (2024, October). AI-Powered Fraud Detection in the Financial Services Sector: A Machine Learning Approach. In 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 795-799). IEEE.https://ieeexplore.ieee.org/abstract/document/10760599

[12]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention.https://oarjst.com/sites/default/files/OARJST-2024-0060.pdf

[13]. Shoetan, P. O., & Familoni, B. T. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. Finance & Accounting Research Journal, 6(4), 602-625.https://www.fepbl.com/index.php/farj/article/view/1036

[14]. Goriparthi, R. G. (2023). AI-Enhanced Data Mining Techniques for Large-Scale Financial Fraud Detection. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1), 674-699.https://www.researchgate.net/profile/Dileep-Kumar-Chikwarti/publication/385720858_AI-Enhanced_Data_Mining_Techniques_for_Large-Scale_Financial_Fraud_Detection/links/6732c54268de5e5a30739b18/AI-Enhanced-Data-Mining-Techniques-for-Large-Scale-Financial-Fraud-Detection.pdf

[15]. Sai, C. V., Das, D., Elmitwally, N., Elezaj, O., & Islam, M. B. (2023). Explainable AI-Driven Financial Transaction Fraud Detection using Machine Learning and Deep Neural Networks. Available at SSRN 4439980.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4439980

[16]. Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). AI-based financial transaction monitoring and fraud prevention with behaviour prediction. Applied and Computational Engineering, 77, 218-224.

[17]. Narayan, M., Shukla, P., & Kanth, R. (2024). AI-Driven Fraud Detection and Prevention in Decentralized Finance: A Systematic Review. AI-Driven Decentralized Finance and the Future of Finance, 89-111.https://www.igi-global.com/chapter/ai-driven-fraud-detection-and-prevention-in-decentralized-finance/355303

[18]. Yuhertiana, I., & Amin, A. H. (2024). Artificial Intelligence Driven Approaches for Financial Fraud Detection: A Systematic Literature Review. KnE Social Sciences, 448-468.https://kneopen.com/KnE-Social/article/view/16551/

[19]. Pattyam, S. P. (2019). AI in Data Science for Financial Services: Techniques for Fraud Detection, Risk Management, and Investment Strategies. Distributed Learning and Broad Applications in Scientific Research, 5, 385-416.https://dlabi.org/index.php/journal/article/view/123

[20]. Islam, M. Z., Shil, S. K., & Buiya, M. R. (2023). AI-driven fraud detection in the US financial sector: Enhancing security and trust. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), 775-797.https://www.researchgate.net/profile/Md-Zahidul-Islam-22/publication/385817697_AI-Driven_Fraud_Detection_in_the_US_Financial_Sector_Enhancing_Security_and_Trust/links/67365b1a69c07a4114473ef7/AI-Driven-Fraud-Detection-in-the-US-Financial-Sector-Enhancing-Security-and-Trust.pdf

[21]. Zanke, P. (2023). AI-Driven fraud detection systems: a comparative study across bankin, insurance, and healthcare. *Advances in Deep Learning Techniques*, *3*(2), 1-22.https://thesciencebrigade.com/adlt/article/view/182

[22]. Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, M. I., & Al Mahmud, M. A. (2024, June). AI Advances: Enhancing Banking Security with Fraud Detection. In *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)* (pp. 289-294). IEEE.https://ieeexplore.ieee.org/abstract/document/10742687

[23]. Kalluri, K. (2024). AI-Driven Risk Assessment Model for Financial Fraud Detection: a Data Science Perspective. *International Journal of Scientific Research and Management*, *12*(12), 1764-1774.https://i-jsrm.net/index.php/ijsrm/article/view/4

[24]. Rani, S., & Mittal, A. (2023, September). Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 6, pp. 2345-2349). IEEE.https://ieeexplore.ieee.org/abstract/document/10397958

[25]. Shoetan, P. O., & Familoni, B. T. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal*, *6*(4), 602-625.https://www.fepbl.com/index.php/farj/article/view/1036

[26]. Hafez, I. Y., Hafez, A. Y., Saleh, A., El-Mageed, A., Amr, A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1), 1-35.https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-01048-8

[27]. Dayalan, P., & Sundaramurthy, B. (2025). Exploring the Implementation and Challenges of AI-Based Fraud Detection Systems in Financial Institutions: A Review. *Creating AI Synergy Through Business Technology Transformation*, 25-38.https://www.igi-global.com/chapter/exploring-the-implementation-and-challenges-of-ai-based-fraud-detection-systems-in-financial-institutions/356746

[28]. Iseal, S., Joseph, O., & Joseph, S. (2025). AI in Financial Services: Using Big Data for Risk Assessment and Fraud Detection.https://www.researchgate.net/profile/Sheed-Iseal/publication/388036425_AI_in_Financial_Services_Using_Big_Data_for_Risk_Assessment_and_Fraud_Detection/links/67882c2b1afb4e11f5e7fdf9/AI-in-Financial-Services-Using-Big-Data-for-Risk-Assessment-and-Fraud-Detection.pdf

[29]. Imoru, M. A. Developing AI-driver strategies for Financial Fraud Risk Management in Emerging Markets.https://www.researchgate.net/profile/Modupe-Imoru-2/publication/387698535_Developing_AI-driver_strategies_for_Financial_Fraud_Risk_Management_in_Emerging_Markets/links/67781eb8117f340ec3f0b817/Developing-AI-driver-strategies-for-Financial-Fraud-Risk-Management-in-Emerging-Markets.pdf

[30]. Abbas, S. (2025). Financial Fraud Risk Assessment Using AI: Integrating Compliance Technology for Policy Formulation in Emerging Markets.https://www.researchgate.net/profile/Nadeem-Sano/publication/387699701_Financial_Fraud_Risk_Assessment_Using_AI_Integrating_Compliance_Technology_for_Policy_Formulation_in_Emerging_Markets/links/6778308bc1b01354650caf8f/Financial-Fraud-Risk-Assessment-Using-AI-Integrating-Compliance-Technology-for-Policy-Formulation-in-Emerging-Markets.pdf

[31]. Kodmalwar, P., Maheshwari, A., Palav, M. R., Priya, S., Purusothaman, N., & Namdeo, A. K. (2025). Real-Time Fraud Detection Using AI and Signal Processing. In *Role of Internet of Everything (IOE), VLSI Architecture, and AI in Real-Time Systems* (pp. 121-136). IGI Global Scientific Publishing.https://www.igi-global.com/chapter/real-time-fraud-detection-using-ai-and-signal-processing/365768

[32]. Shamoo, Y. (2025). Cybercrime Investigation and Fraud Detection With AI. In *Digital Forensics in the Age of AI* (pp. 83-114). IGI Global Scientific Publishing.https://www.igi-global.com/chapter/cybercrime-investigation-and-fraud-detection-with-ai/367312
Datasetlink:https://www.kaggle.com/datasets/bhadramohit/credit-card-fraud-detection