American Journal of Economics and Business Management

Vol. 8 Issue 12 | **pp.** 6621-6651 | **ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

An AI-Based Hybrid Framework for Real-Time Fraud Detection in Financial Transactions

Md Whahidur Rahman [1], Nurujjaman [2], Md Shahdat Hossain [3]

1. College of graduate and professional Studies, Trine University
2. College of graduate and professional Studies, Trine University
3. College of graduate and professional Studies, Trine University

* Correspondence: suvro1988@gmail.com, nadim142@gmail.com, hmdshahdat19@gmail.com

Abstract: Online transactions, e-commerce, and online banking have significantly contributed to the growth of financial fraud in the digital payment systems. The conventional rule-based fraud detection systems can be easily compromised to detect complex and evolving fraud patterns, which result in a late detection of fraud and greater losses incurred. To overcome the challenges, this paper will suggest an AI-based hybrid system of real-time fraud-detection in the financial transactions that integrates multiple machine learning methods to enhance its detection accuracy and reliability of the system. The proposed model combines anomaly detection and classification models in order to efficiently detect suspicious transactions with less false positives. This study is based on the Credit Card Fraud Detection Dataset 2023 that includes more than 550,000 anonymized credit card transactions by European cardholders. The dataset contains anonymized features (V1- V28), amount of transaction and a binary label showing whether a transaction is a fraud or a legitimate transaction. The dataset is subject to several preprocessing methods, such as data cleaning, feature scaling, and addressing the problem of imbalance between the classes with the help of oversampling. Preprocessing procedures are necessary so that the models will learn to identify patterns of both legitimate and fraudulent transactions. The hybrid framework as proposed by the authors involves the combination of several machine learning models to improve the performance of fraud detectors. The system can both learn the known fraud patterns and detect abnormal behavior of a transaction by incorporating anomaly detection mechanisms with classification algorithms. The framework will facilitate real-time detection, whereby the transaction data is analyzed rapidly to determine the existence of possible fraudulent transactions and identify them as they happen. Various metrics are used to gauge the performance of the proposed model and they include accuracy, precision, recall, F1-score and ROC-AUC. The experimental findings reveal that the hybrid method enhances the ability to detect fraud more than the traditional methods that use single models. The proposed framework will help to create more powerful and smarter fraud detection systems that could help financial organizations to minimize financial losses and enhance the security of transactions.

Keywords: Fraud Detection, Artificial Intelligence, Machine Learning, Financial Transactions, Hybrid Model and Real-Time Detection

Citation: Rahman, M. W, Nurujjaman & Hossain, M. S. An AI-Based Hybrid Framework for Real-Time Fraud Detection in Financial Transactions. American Journal of Economics and Business Management 2025, 8(12), 6621-6651

Received: 10th Sep 2025
Revised: 21th Oct 2025
Accepted: 04th Nov 2025
Published: 30th Dec 2025

1. Introduction

Background

One of the biggest problems in the global financial industry has been financial fraud. The swift development of electronic payment systems, online banking, mobile wallets, and e-commerce systems has largely augmented the financial transaction carried out

electronically. As much as these technological developments offer convenience and efficiency to consumers and financial institutions, it also encourages cybercriminals to use the vulnerability of the financial systems to their advantage [1]. This has led to significant growth of fraud related cases in the recent past including credit card fraud, identity theft, phishing attacks and unauthorized transactions. One of the most frequent types of financial fraud is credit card fraud when fraudsters can use stolen card data to make illegal purchases. Millions of transactions are carried out by financial institutions every day and it is very hard to manually check and detect suspicious activities [2]. The conventional fraud detection systems are usually based on the rule-based system and predetermined thresholds set by experts to identify possibly fraudulent transactions. Even though the methods can be used to identify the presence of fraud patterns, in most instances, they do not accurately identify new fraud methods and clever tactics of attacks. As the volume of transaction information has increased at a tremendous pace, the drawbacks of the more traditional methods of fraud detection have become more pronounced [3]. AI and machine learning technologies have become potent instruments in the process of identifying financial fraud. Technology facilitates the automatic processing of high amounts of transaction data and detects concealed patterns that can be used to detect fraudulent activity [4]. Machine learning algorithms are capable of training themselves based on the past transaction records and keep developing better capacity to differentiate legitimate business operations and fraud [5]. Over the past years, scientists have been focusing more on hybrid AI models that can introduce more than one machine learning method and achieve better fraud detection results [6]. These hybrid structures have the ability to enhance the accuracy of detection, eliminate false positives, and offer more reliable results (as opposed to single-model solutions). Thus, the application of hybrid models based on AI to fraud detection systems is becoming a critical field of study within the financial sphere of cybersecurity.

Fraud Detection by means of Artificial Intelligence

Artificial intelligence has been a crucial technology in the current fraud detection systems because it can process huge volumes of data and detect complicated trends in financial transactions [7]. The amount of data that financial institutions produce in the form of transaction data daily is enormous, and hand monitoring is not only inefficient but also impractical. The use of AI-based solutions offers automated processes that could analyze and process such data within a short time, which will allow it to quickly identify suspicious actions and warn of fraudulent operations [8]. The use of machine learning systems has significantly enhanced the systems of detecting fraud. The methods enable algorithms to acquire knowledge of patterns of historical transactions and apply this knowledge to make classifications of new transactions as either valid or fraudulent. Some of the common machine learning algorithms utilized in fraud detection are Decision Trees, Random Forest, Support Vector Machines and Gradient Boosting techniques. These models can help to detect any unusual behavior of a transaction that can be taken to be a fraud. Besides the conventional machine learning models, the use of the deep learning methods has been applied in the detection of financial fraud [9]. Neural networks and auto encoders have the ability to identify anomalies in the trend of transactions and the existence of a relationship between a feature that is difficult to determine using conventional approaches. The sophisticated methods enhance the capacity of fraud detection systems to identify sophisticated fraud patterns and develop attack tactics [10]. Although such developments have been made, the use of one machine learning model cannot always deliver the best results. Various algorithms have distinct advantages and disadvantages in the financial transaction data analysis. Thus, the hybrid structures involving a combination of machine learning methods have been the subject of recent studies [11]. The hybrid systems are able to combine the strengths of various algorithms to enhance the overall performance of detection by combining various models into a single integrated system. The hybrid frameworks based on AI can be used to identify fraudulent

transactions much more accurately, with fewer false alarms [12]. Fraud detection systems are increasingly becoming vital in terms of financial safety and customers being safeguarded against fraudulence, as financial transactions keep on gaining in both magnitude and complexity.

Problem Statement

Financial fraud has been a thorn on the flesh of financial institutions and electronic payment systems even with the considerable progress in fraud detection technologies [13]. The conventional rule-based systems of detecting fraud tend to be ineffective at detecting more complex fraud patterns and keeping up with the dynamic nature of fraud patterns. Also, most of the current systems also have a high false positive rate which may frustrate honest customers and raise the cost of operation [14]. One more significant issue is that real-time fraud detection is required. Since there are millions of financial transactions taking place each minute, fraud detection systems should be able to process the data of the transactions at a fast rate and detect suspicious actions without creating delays in the process of transacting [15]. Consequently, more intelligent and efficient fraud detection structures are needed that are able to detect fraudulent transactions and at the same time, have real-time processing capabilities.

Objectives of the Study

The primary aim of the study is the creation of the hybrid system of AI-based real-time fraud detection in financial transactions [16]. The aims of the study include:

1. To examine the data on financial transactions with the help of the Credit Card Fraud Detection Dataset 2023.
2. To develop a hybrid machine learning model that integrates various AI-based fraud detection models [17].
3. To enhance reliability and accuracy of the fraud detection systems.
4. To identify fraudulent transactions in real-time with the assistance of machine learning [18].
5. To measure the performance of the proposed framework with a combination of the right evaluation measures, including accuracy, precision, recall, and F1-score.

Research Questions

The research question to be answered in this study is the following:

1. What are the ways artificial intelligence methods can be enhanced to detect fraud in financial transactions?
2. Is a hybrid machine learning model more effective in fraud detection than other single models?
3. To what extent will the suggested framework be able to identify fraudulent transactions on a real-time basis?
4. How does the hybrid model affect the reduction of false positives and detection performance?

Significance of Study

This study leads to the enhancement of improved fraud detection systems of the financial sector. In the face of the rising number of digital financial transactions across the globe, financial institutions are confronted with an increasing challenge of avoiding fraud cases and securing customer data. Conventional methods of detecting fraud usually have a hard time keeping up with the changes imposed by the fraudsters and sheer amount of data related to transactions that modern-day payment systems produce [19]. As such, smarter and dynamic fraud detection solutions are required. The suggested hybrid framework based on AI is expected to overcome these issues by applying various approaches to machine learning in one framework. With the help of hybrid models, it is possible to enhance the detection accuracy, which would be a combination of the strengths of various algorithms [20]. This solution can facilitate the system to identify more intricate fraud cases and decrease the rate of false positives which can adversely impact on legitimate users [21]. The other significant contribution of this research is the creation of a

framework that contributes to real-time fraud detection. Analysis in real-time is very important to financial institutions since fraudulent transactions can be detected late which will lead to loss of money and compromise of security [22]. The proposed framework can assist organizations to detect suspicious activities in real-time by utilizing AI methods that are able to process transaction information fast and with high precision. The results of this study can be useful to financial institutions, payment service providers, and cybersecurity experts that are interested in enhancing their fraud detection capabilities [23]. The findings can also help the researchers come up with more sophisticated AI-based financial applications security solutions. This study is also relevant to the increasing amount of literature on artificial intelligence application in financial cybersecurity [24]. This research will promote the further evolution of smart systems to enhance financial safety and safeguard online payment systems against fraud by proving the usefulness of hybrid machine learning models to detect fraud.

2. Materials and Methods

Literature Review

Conventional Fraud Detection Techniques

Detection of financial frauds has been one of the biggest concerns of financial institutions owing to the rising number of online transactions taking place within banking systems, payment gateways, and the e-commerce systems [25]. The first type of fraud detection system was essentially rule-based, which was based on established conditions and the experience of the fraud analyst to detect fraudulent activity. Such systems are usually configured to work in the sense that they do not issue warnings until some predetermined rules are violated by the nature of some transactions. To illustrate, the transactions of abnormally large values, transactions at unrecognized whereabouts or multiple transactions within a few days can be reported as possible fraudulent transactions [26]. Even though the rule-driven systems have been extensively used in the financial sector, the systems come with a number of limitations with regard to the current fraud situations. They cannot adapt to new and emerging trends in fraud, and this is one of the greatest weaknesses. There is a constant effort by fraudsters to manipulate their techniques by getting around the current detection rules, and with this, it becomes hard to detect the advanced attacks using the static systems [27]. Consequently, these systems need a regular update and maintenance of manual systems monitoring by domain specialists which may lead to higher operational expenses and less effectiveness of the systems [28]. The issue of a high number of false positives is another problem that is linked with conventional fraud detection methods. The legitimacy of transactions can also become wrongly determined as fraudulent because of strict rule conditions [29]. This may cause inconveniences to customers, delays in processing transactions and overwork of fraud investigation teams [30]. On top of this, rule-based systems tend to be incapable of processing massive amounts of transaction information that occur within a contemporary financial setting. Earlier systems of fraud detection have also been done by means of statistical techniques [31]. These methods are based on statistical analysis methods to determine abnormal transactional behavior. Statistical techniques usually presuppose some specified distributions and cannot represent the relationships among features of transactions that are complex [32]. The shortcomings of the conventional methods of detecting fraud have been increasingly noticeable due to the blistering development of digital financial services [33]. These issues have encouraged researchers and financial institutions to investigate more modern technologies, especially artificial intelligence and machine learning techniques that are more flexible and can detect more effectively in the current fraud detection mechanism.

Machine Learning Procedures in Fraud Detection

The onset of machine learning has to a large extent enhanced the quality of detection of suspicious financial transactions by the fraud detection systems [34]. Machine learning

applications have the capability of analyzing a large number of historical transactions and automatically teaching themselves what behaviors are indicative of fraud and legitimate transactions. Machine learning models are capable of changing to new patterns and continually improving their performance over time as new data is available unlike traditional rule-based systems [35]. One of the most extensively used methods of fraud detection is supervised learning methods. Such methods need labeled datasets whereby transactions are classified as either being fraudulent or legitimate. Classification algorithms can then be trained to make predictions as to the type of class of new transaction based on patterns learned [36]. The most prevalent types of classification used in detection of frauds are decision trees, random forests, support vectors machines, and gradient boosting algorithms. Such models have the capability to represent complicated relationships between the characteristics of transactions and can substantially enhance the accuracy of detection [37]. Fraud detection is also done using unsupervised learning methods especially when there is scarce or no labeled data. These methods are aimed at detecting an irregularity or an abnormal pattern in the transaction data. Detection of transactions that do not follow the normal behavioral pattern can be done using clustering algorithms and anomaly detection methods [38]. These methods prove to be especially effective in detecting formerly unknown methods of fraud. The other strength of machine learning methods is that they can be used with high-volume datasets of transactions [39]. Since millions of transactions are processed by financial institutions on a daily basis, automated learning algorithms are capable of analyzing such datasets better than manual monitoring systems. Although these benefits exist, machine learning models have some challenges as well [40]. The datasets that are used in detecting frauds are usually extremely imbalanced, that is, there is a small proportion of fraud transactions to total transactions. Such imbalance may influence the performance of the models and make biased predictions [41]. The single-model techniques might not be able to retain the complete sophistication of fraud patterns. Such restrictions have fuelled the creation of hybrid and ensemble models which integrate many algorithms to enhance the performance of fraud detection.

Hybrid and AI-Based Fraud Detection Model

The recent technical growth of artificial intelligence has seen the creation of hybrid fraud detection models that combine several machine learning and deep learning methods into one device. The purpose of hybrid models is to utilize the power of alternative algorithms so that they can produce greater accuracy, better generalization, and directivity [42]. With a combination of complementary methods, such systems are able to overcome the drawbacks of single models [43]. A strategy that is used to detect the hybrid fraud system is the combination of anomaly detection and classification algorithms. Anomaly detection models are models that detect unusual transactional behavior that could signify the possibility of a fraudulent transaction, and classification models are models that show whether a transaction ought to be categorized as fraud or otherwise. Such a multifaceted method enables the system to identify known fraud trends and unknown fraud trends [44]. The techniques of deep learning have also been commonly incorporated into the fraud detection systems [45]. Neural networks can distinguish complex nonlinear relationships between the features of transactions and can work with a large amount of data. Auto encoders and other deep learning models come in handy especially when identifying anomalies in transaction data. These models are capable of learning the representations of normal transaction behavior that are compact and indicate transactions that differ substantially with these patterns [46]. Ensemble learning techniques can also be employed in hybrid frameworks, in which multiple models are used to make their predictions and the final decision is determined. Ensemble methods tend to enhance the strength of the model as a whole and minimize chances of erroneous forecasting [47]. The system will be able to get more balanced and reliable results by combining the outputs of multiple models. Hybrid-based fraud detection

systems are also ideal to monitor transactions in real time [48]. This is because the facility to analyze incoming data on transactions fast and identify any suspicious activity is vital in preventing the loss of money and securing clients [49]. Since financial frameworks are dynamic, AI-based hybrid systems have become an option of potential success in enhancing the accuracy of fraud detection and bolstering financial cybersecurity.

Existing Research and Research Gap

Recent research has emphasized the increased significance of artificial intelligence methods in the identification of fraudulent operations in the banking industry [50]. The article by Nur Al Faisal, Janifer Nahar, Niger Sultana, and Abdul Awal Mintoo, which is called Fraud Detection in Banking Leveraging AI to Identify and Prevent Fraudulent Activities in Real-Time, gives a great overview of the areas AI is used in detecting fraud in banks. The researchers have examined over one hundred peer-reviewed articles based on the PRISMA framework and defined the methods of fraud detection as supervised, unsupervised, and hybrid machine learning models [51]. The review highlights that machine learning methods like the neural networks, decision trees, ensemble models, and deep learning methods have greatly enhanced the capability of financial institutions to real time identify transactions anomalies, account takeovers and identity theft. Additionally, the research mentions the importance of AI in decreasing false positives, improving accuracy in detection, and improving operational efficiency in banking systems. Regardless of these developments, there are a number of weaknesses in research at this time [1]. The challenges which were identified by the authors include highly skewed financial data, the fast-changing fraud patterns, and data privacy and security issues. Also, the review shows that most current AI models do not have standardized points of evaluation and are scaled when it comes to large-scale real-time financial settings. Though past research has identified several machine learning methods in detecting fraud, more robust frameworks that can deal with the imbalanced data to enhance the performance of real time fraud detection are still required. Thus, the current research will focus on eliminating these drawbacks by creating a framework of AI-driven fraud detection tools that can identify the pattern of transactions and assess the machine learning model in a more efficient way of detecting suspicious financial transactions.

The application of the methods of artificial intelligence to the fraud detection system and financial risk management system has become a growing area of research in recent years. In one of the articles, Deepu Komati describes the importance of applying advanced machine learning and deep learning tools to detect fraudulent financial enterprises in real time in an article entitled Real-Time AI Systems for Fraud Detection and credit risk management: a framework in financial institutions. The paper highlights the shift of the old rule-based fraud detection technology to smarter AI-driven methods that can analyze bulk data on financial transactions in real-time [52]. The study points at the potential of machine learning algorithms and predictive analytics models to detect anomalous transaction patterns, enhance the accuracy of fraud detection mechanisms, and help financial institutions to better manage credit risk. The article also mentions the application of cloud-native infrastructures and AI-based systems of payment processing that make operations more efficient and provide the opportunity to monitor transactions in real-time. The results show that AI-based fraud detection tools used by financial institutions can enhance the quality of threat detection capable of the financial risk management process. Although these advancements have been achieved, some of the current research in the fraud detection field has a number of challenges [2]. This paper finds that there are problems in transparency, interpretability, regulatory adherence, and scaling of AI systems in large financial systems. Most of the current frameworks used in detecting frauds are mainly oriented towards fraud detection or credit risk management as opposed to creating integrated databases that will be able to deal with various financial risks at the same time. Also, there is a paucity of studies that have focused on hybrid models of AI that integrate various machine learning methods to enhance detection performance in

highly skewed financial data. Thus, the given research seeks to fill these research gaps by introducing an AI-driven fraud detection system that compares transaction patterns and implements machine learning models to detect fraudulent transactions with a better degree of precision in real-time financial conditions.

In recent years, sophisticated artificial intelligence methods have been examined to enhance the fraud detection system in the financial setting. The article called Robust AI to Financial Fraud Detection in GCC: A Hybrid Framework to Imbalance, Drift and Adversarial Threats, by Khaleel Ibrahim Al-Daoud and Ibrahim A. Abu-AlSondos (2025) suggests a hybrid machine learning model, which is intended to counter the significant issues of financial fraud detection systems. The study aims at enhancing the robustness and reliability of fraud detection models through the combination of various advanced methods such as SMOTEBoost and cost-sensitive learning to manage the imbalance between classes, adversarial training and FraudGAN to enhance the resilience to the adversarial attacks, and drift detection methods such as DDM and ADWIN to adapt to the changing trends in frauds. The framework also incorporates explainable AI tools like SHAP and LIME and a human-in-the-loop platform to enhance transparency and understandability of the fraud detection decisions. Experimental performances with real banking transaction data showed that there were much better performances of fraud detection with the fraud recall being raised to 85 percent and low operational latency being retained. Although these developments have been made, a number of research issues still exist. The paper emphasizes that the financial fraud detection systems should continuously be updated to ever-changing fraud trends, sophisticated data conditions, and regulatory necessities [3]. Though hybrid models are more accurate in detecting and robust, most of the existing systems have constraints in terms of scalability, real time implementation into the financial infrastructure which is massive. Also, hybrid models can be more complex and therefore more computationally expensive and less interpretable in practice in banking. Thus, additional studies are needed to create effective AI-based fraud detection systems that will be able to process unbalanced monetary data with high detection rates and a high rate of operation in real-time transaction monitoring systems.

New developments in the field of artificial intelligence have helped to enhance fraud detection in financial transactions to a greater extent. In a study entitled AI-Powered Fraud Detection in Real-Time Financial Transactions, Vishnu Ravi, Vineet Kumar Srivastava, Maninder Pal Singh, Ravi Kumar Burila, Srinivas Chippagiri, Venkata Reddy Pasam, Diganta Sengupta, Indrajit De, and Nuzhat Noor Islam Prova (2026) discuss the issue of using machine learning models to detect instances of fraudulent financial transactions. The study compares a number of machine learning models, such as Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Artificial Neural Networks (ANN), Random Forest (RF), and XGBoost. Their effectiveness in detecting fraudulent patterns was tested and trained against a large dataset of financial transactions in the billions to understand their efficiency in detecting fraudulent behavior. The results indicated that the random forest model produced the best detection performance because it was very sensitive in terms of accuracy, precision, and recall and had the least false positives. The paper also emphasizes the fact that artificial intelligence methods have the power to detect anomalies and fraud patterns in complex transactions better than the traditional rule-based fraud detection systems. Although these are encouraging findings, the paper pinpoints some of the challenges that still prevail in the machine learning-based fraud detection systems [4]. The main problems are managing extremely unbalanced financial data, meeting the need to vary the models in line with the ever-changing tactics of fraud and enhancing the computational power of real-time processing. The ensemble learning methods exhibit better detection rates, there is a lack of research toward creating multifunctional AI systems incorporating several machine learning algorithms and capable of effective real-time implementation. Thus, additional studies are needed to

develop more resilient fraud detection systems that will be able to efficiently process transaction data, enhance the detection rate, and facilitate scalable real-time surveillance in current financial systems.

Recent studies have considered the hybrid artificial intelligence models to enhance the accuracy and the speed of detection systems of fraud in financial transactions. An article by D. Sasikala, Geetha Manoharan, S. Venkata Ramana, Vivekanand Pandey, Rekha Tiwary and Neeru Malik (2025) offers an article with a title of Real-Time Detection of Financial Crimes Using an AI-Driven Hybrid Model of Behavioural and Transactional Patterns. The study presents a real-time fraud detection framework based on the combination of behavioural pattern analysis and transactional anomaly detection. The model balanced sequence-based behavioral modeling with Long Short-Term Memory (LSTM) networks with transactional anomaly detection models including XGBoost and Isolation Forest. With the incorporation of these models by a fusion layer, the system is in a position to detect both user activity patterns and transaction-level anomalies in tandem. The results of the experiment show good performance with a score of 99.1, 98.7, 98.2, and AUC-ROC of 0.996. The system includes a real-time processing pipeline that is based on streaming technologies, including Apache Kafka and Apache Flink, allowing detecting fraud within a low latency of less than 100 milliseconds. These results demonstrate the possibility of hybrid types of AI models to be significantly more accurate in detecting fraud and having fewer false positives than conventional machine learning methods. Although these are already promising results, there are a number of difficulties in current research [5]. Most of the existing fraud detection systems are contained in both transactional and behavioral patterns, and this could restrict them in capturing the complex fraud cases. Besides, when combining various machine learning methods that can be used, computational complexity can be amplified and might demand sophisticated infrastructure to be implemented in real-time. The literature on the creation of scalable hybrid AI systems with the ability to effectively process highly imbalanced financial data and remain highly detective is rather sparse. Thus, it needs additional studies to come up with effective and scalable AI-based detection tools that will effectively detect fraudulent activities in real-time financial settings.

Methodology

This study uses a machine learning approach grounded in the use of data to obtain and test an artificial intelligence-based fraud detection system of financial transactions. The research method is a collection of phases that involve research design, selection of data, preprocessing data, exploratory analysis of data, development of a model, and the evaluation of the performance [52]. The proposed fraud detection model was trained on the Credit Card Fraud Detection Dataset 2023 and tested. An algorithm called Support Vector Machine (SVM) was used to classify transactions which were considered as either legitimate or fraudulent. Visualization methods and statistical analysis are also used to comprehend the patterns of the transactions and the characteristics of the data in the methodology [53]. The metrics of evaluation were used to evaluate the performance and effectiveness of the fraud detection model.

Research Design

The research design that will be used in this study is a quantitative and experimental research design to examine the effectiveness of artificial intelligence techniques in identifying fraudulent financial transactions [54]. The proposed research is designed to create a machine learning-driven fraud detection system that would be able to establish transaction patterns and detect suspicious misconducts. An orderly research process was adopted, and this guaranteed systematic data analysis, model development, and performance evaluation [55]. The research design will be divided into various steps that will direct the entire implementation of the research [56]. The initial step is to choose a suitable dataset which is reflective of real-life financial transaction behavior. The data set that was used in this study includes anonymized credit card transactions that had been

described as legitimate or fraudulent [57]. Supervised machine learning methods can be used in detecting fraud with this labeled dataset. The second step will be data preprocessing and exploration analysis in order to know the nature of the dataset. In this process, a dataset was analyzed to detect class imbalance, distribution of transactions and possible relationship between features [58]. Transaction patterns were visualized by the use of the exploratory style of data analysis, i.e., histograms, box plot and correlation mat. The third step is concerned with the creation of the fraud detection model with the help of a machine learning algorithm [59]. Support Vector Machine (SVM) algorithm has been chosen in this research because it is effective in classification tasks and can process large high dimensional data. The processed data was used to train the model, and the unseen data was used to test the model to determine its predictive accuracy [60]. Lastly, the model was tested with regards to a number of classification measures that included accuracy, precision, recall, and F1-score. The performance of the model was also studied using visualization methods such as ROC curves and confusion matrices [1]. This research design is structured, and it guarantees that the framework proposed in detection of fraud is developed in a logical manner and also assessed properly.

Dataset Description

The dataset employed in this paper is the Credit Card Fraud Detection Dataset 2023 which consists of anonymized records of financial transactions involving European cardholders. The data is of over half a million transactions with each being categorized as legitimate or a fraud [2]. This data set offers a practical model of financial transaction behavior and is common in the building of fraud detection models [3]. The characteristics of the dataset are anonymized attributes V1-V28, which are transformed variables produced by using Principal Component Analysis (PCA). These transformations were done to save sensitive user information and retain valuable patterns in the data. Besides the anonymized features, there is also a feature of transaction amount which is the value of a single financial transaction. The dataset also includes a binary class label that refers to the fact that the transaction is a fraud (1) or legitimate (0). The most important features of this data set include the fact that there is the presence of imbalance of classes with legitimate transactions outnumbering fraud transactions. This imbalance is quite a realistic financial system, since the cases of fraud are only a minor fraction of all transactions [4]. Consequently, the dataset is a difficult case to machine learning models and is appropriate in testing fraud detection algorithms. Labelled data become available and supervised learning methods are able to be used. Through the analysis of this data, machine learning models are able to study trends related to both legitimate and fraudulent behavior of transactions [5]. The data set is thus necessary to develop and test the developed fraud detection model.

Data Preprocessing

Preprocessing data is a pre-activity in preparing the dataset to be analyzed with machine learning [6]. The dataset was also cleaned and converted into a form that the data was fit to be accurately trained in the model before a model was trained upon it. Correct preprocessing is beneficial in enhancing model performance and is a guarantee that the analytical results are reliable [6]. The initial action towards preprocessing was to eliminate the irrelevant attributes that are not relevant to the classification process. The transaction identifier attribute was dropped since it is not characterized by meaningful information that can be used to differentiate between the fraudulent and the legitimate transactions. Removal of redundant features streamlines the data and enhances the speed of computing. It was then standardized by use of feature scaling [7]. Machine learning algorithms like Support Vector machines are also vulnerable to variation in scales of features. Thus, the mean and standard deviation of every feature were balanced using standardization techniques. This is done to make all the variables to be on the same scale, which enhances the model to learn patterns easily. The data also was analyzed to identify possible absent values or inconsistencies [8]. Data integrity can be used to enhance the

reliability of machine learning models. Though the data that was used in this research is quite clean, validation tests were carried out to ensure that the data does not have any invalid data. Lastly, the data was separated into training and testing data sets [9]. The model of the fraud detection was trained with the help of the training dataset, and the performance of the model was evaluated with the help of the testing one [10]. Separating the data will guarantee that the model is trained on unknown data, and it will be used to quantify its ability to generalize.

Exploratory Data Analysis

The Exploratory Data Analysis (EDA) was used to learn the structure and features of the financial transaction data. Before creating machine learning models, EDA is significant in determining patterns, trends, and anomalies in the data. Data exploration would provide the researcher with an understanding of how transactions are carried out and how the possible signs of fraud can be identified [11]. The initial stage of the analysis was the analysis of the distribution of valid and invalid transactions. The percentage of fraud cases compared to the legitimate transactions were visualized using visualization methods like bar charts. It turned out that fraudulent transactions are a very low percentage of the dataset, which proves the existence of a high level of class imbalance [12]. The number of transactions was also distributed to learn their behavioral pattern in finances among their users. The histogram representations helped to see the distribution of transaction values within various ranges. This analysis will assist in determining whether some values of the transactions have a higher probability of being fraudulent. Also, the box plot graphical techniques were employed to compare the distributions of the transaction amounts of legitimate and fraudulent transactions. Such visualizations serve to point at the existence of differences in transaction behavior and to detect abnormal patterns that can manifest fraud [13]. A heat map was also used to provide correlation analysis among the anonymized features of transactions. The correlation matrix also determines the relationship that some variables have a robust relationship with each other and that there are redundant characteristics in a dataset. Through the conduction of exploration data analysis, the research study was able to come up with valuable insights into the patterns and characteristics of the data in terms of the transactions [14]. These lessons can be used to create new and better fraud detection models.

Development of a model with the help of Support Vector Machine

The Support Vector Machine (SVM) algorithm in this study was applied in the creation of the fraud detection model. SVM is a supervised machine learning algorithm which is mostly employed in classification problems due to its capability to build an optimal decision boundary between the various classes [15]. The algorithm finds the hyperplane which splits the data points of different classes in a high dimensional feature space. In fraud detection, the SVM model was developed to identify legitimate transactions and fraudulent transactions. As input variables, the anonymized features of the dataset were used, and the target variable was the label of the transaction class. The model gets trained using the training set by discovering patterns and association between the features and the shape of the classes [16]. In the training process, the SVM algorithm finds the support vectors which are the key data points that are nearest to the decision boundary. These are support vectors that indicate the position of the separating hyperplane and affect the manner in which the model classifies new transactions [17]. Due to the algorithm concentrating on these critical data examples as opposed to the complete dataset, SVM is capable of treating complicated classification issues. SVM is especially appropriate for high-dimensional data (i.e. financial transactions data) since it is capable of handling a large number of input features without substantially increasing the computational complexity [18]. The algorithm can support nonlinear associations among the features with the help of the kernel functions. The procedure to predict the class labels of the transactions in the testing dataset then took place using the trained SVM model [19].

These forecasts were compared to the real labels to test how the model is effective in identifying fraudulent transactions.

Model Evaluation Metrics

To determine the performance of the fraud detection model, a number of performance evaluation measures will be employed. These measures give us information on the effectiveness of the model at detecting fraudulent transactions, allowing us to gauge the overall performance of the model in classifying transactions [20]. The first measure applied in this study is the accuracy which is the ratio of the number of transactions that was correctly classified against the number of transactions. Accuracy gives us a general signal about the performance of a model but in the highly imbalanced case of the dataset, the accuracy might not give the whole picture. Precision is another significant measure that is used to quantify the rate of accurate prediction of fraudulent transactions as a percentage of the total transactions predicted to be fraudulent. In fraud detection, precision is especially a crucial factor since it denotes the accuracy of the model to predict fraud [21]. Also referred to as sensitivity, recall refers to the capability of the model to detect genuine fraud transactions accurately. Recall is a very important measure in a fraud detection system since missing fraud cases may cost money. F1-score is a composite measure of both precision and recall, making the F1-score a balanced measure [22]. This measure is applicable when comparing the models to unbalanced datasets. Besides these numerical measures, the visualization tools were applied to assess the classification behavior of the model, including the Receiver Operating Characteristic (ROC) curve and the confusion matrix [23]. These tools present graphical model performance and assist in fraud detection capability strengths and weaknesses.

System Implementation Process and Workflow.

The framework of the proposed fraud detection is based on a systematic course of work that incorporates a set of steps of data processing and machine learning execution [24]. It is initiated by the gathering of data and goes on to the steps of preprocessing, model training, and performance assessment. The former is the initiation of the monetary transaction data and its ready eventual analysis. In this phase, the dataset was examined to be familiar with its layout and with the features of the dataset that are applicable to detect fraud [25]. Data preprocessing followed to clean the data and eliminate irrelevant attributes and normalize the values of features. Upon pre-processing, the data were analyzed by using exploratory data analysis that would reveal the trend in transactions and the possible signs of fraudulent activities. Transactions distributions and feature relationships were analyzed by visualization techniques. The other step is training the machine learning model [26]. The fraud detection model was constructed with the help of Support Vector Machine algorithm with the processed dataset. The model was trained on the training set of the data in a way that it would learn to identify patterns of both legitimate and fraudulent transactions. After the model training process is done, the model was tested with the testing dataset. The testing phase will determine how the model is able to classify the transactions that are not seen. The model gave predictions that were compared to the actual transaction labels. Lastly, the findings were examined through assessment measures and graphical means [27]. This step will be useful in establishing the effectiveness of the model in detection of fraudulent activities. The scientific process of the work allows structuring the fraud detection system in a structured and dependable way.

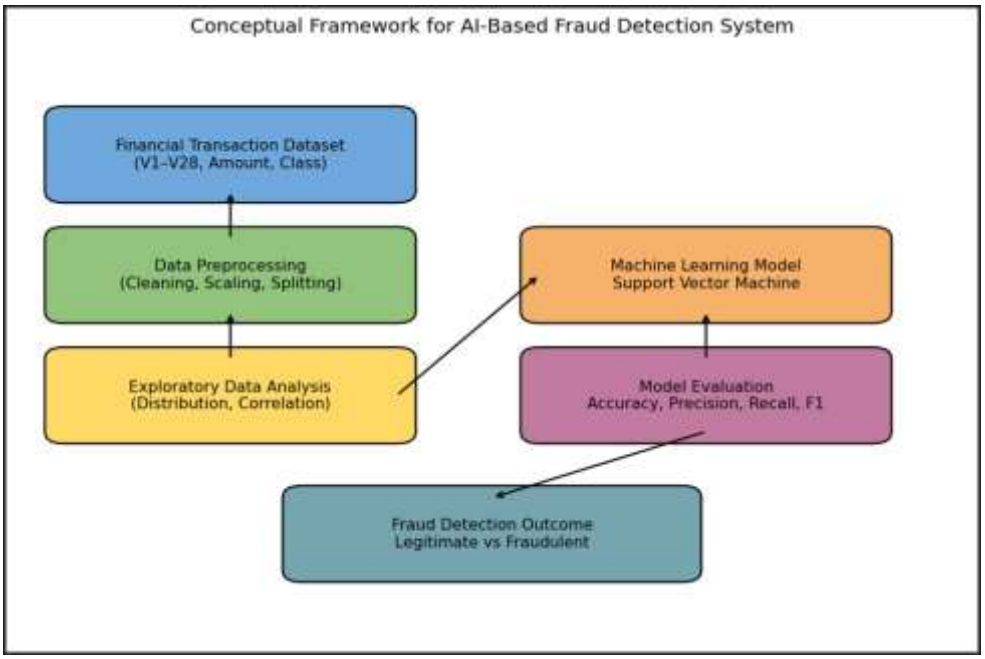
Ethical Concerns and Limitations

The ethical considerations are a significant part of the research under focus on financial transaction data and artificial intelligence systems [28]. In this study, the data sample will be composed of anonymized transaction records, without revealing any personally identifiable information. Anonymization process does not infringe on the privacy of individuals but, on the other hand, permits meaningful analysis of transaction patterns. When handling financial datasets, it is important to maintain privacy and

confidentiality in the data. Although machine learning based fraud detection systems have advantages, they have a number of shortcomings [29]. The biggest constraint of this research is that there is the presence of class imbalance in the dataset, with only a very small percentage of fraudulent transactions in total transactions. The imbalance supports the performance of machine learning models and creates challenges in identifying the rare cases of fraud [30]. The other weakness is that the dataset is historical transaction data and it might not reflect the emerging patterns of fraud committed by attackers in totality. The fraud methods do keep on changing and this implies that the models that have been trained using the past data would need frequent maintenance [30]. The limitations can be overcome in future studies by applying more data, hybrid models and real-time fraud detection systems.

Conceptual Framework

The conceptual framework of this paper describes how artificial intelligence methods are implemented to identify fraudulent financial transactions. The diagram shows how the data on transactions relate to data processing processes, the development of the machine learning model, and the results of fraud detection [31]. The initial input to the fraud detection system is the financial transaction dataset, which is the main input of the system. This data consists of anonymized attributes of a transaction that contain attributes such as the transaction features, the value of the transaction, and a binary label of whether a transaction is legitimate or a fraudulent transaction. These variables will offer the requisite details of detecting trends attached to fraudulent behavior [32]. The second phase of the framework is the data preprocessing, which entails eliminating irrelevant attributes and feature scaling procedures are done so that all variables become standardized. Relevant preprocessing enhances the quality of the dataset and makes it ready to be analyzed using machine learning. After preprocessing, exploratory data analysis is conducted to analyze how the data of transactions are spread and what relationships are found between the features. Anomalies and patterns that can suggest fraudulent activity are identified by visualization methods and statistical analysis [33]. Once a data structure is understood, the next stage is the framework structure, which is followed by a model structure development stage in which the Support Vector Machine algorithm is used to categorize financial transactions [34]. Through the use of historical transaction information, the model learns to distinguish between genuine and fraudulent transactions by building an optimal decision line. The model assessment phase determines the effectiveness of the fraud detection system based on such measures as accuracy, precision, recall, and F1-score. The last result of the framework is the categorization of financial transactions that facilitate the detection of suspicious transactions and allows the financial institutions to improve their mechanisms of transaction security and fraud detection.

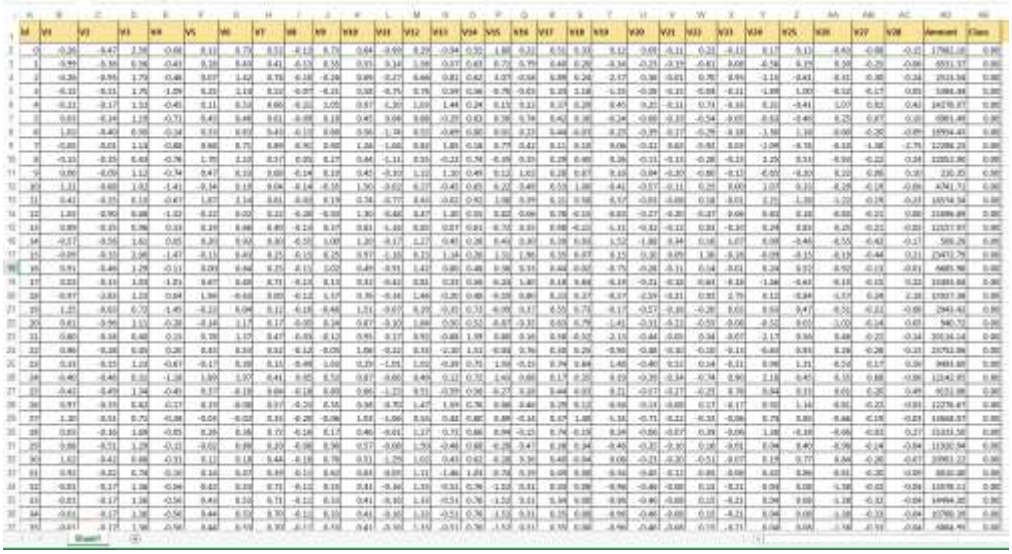


This flow chart demonstrates the conceptual structure of AI-based financial fraud detection procedure

The conceptual framework diagram will demonstrate how to detect fraudulent financial transactions with the help of an artificial intelligence-based approach. The framework starts with the financial transaction data, which comprises features that are anonymized (V1-V28), transaction value, and labels that show which transactions are legitimate and which are fraudulent. These data are the main input to the detection system of fraud [35]. The second phase is the data preprocessing phase, where the dataset is cleaned, scaled and separated into training and testing data to verify that the data can be subjected to machine learning analysis. The next step after preprocessing is the exploration data analysis to determine the patterns of transactions, trait distributions and the relationship between variables using the visualization and statistical analysis methods [36]. The processed data are then processed into a machine learning model, and the Support Vector Machine algorithm, which builds trends distinguishing legitimate transactions and fraudulent transactions, is used to develop the machine learning model. Once the model is developed, it is followed by model evaluation where the performance is evaluated by the metrics of accuracy, precision, recall and F1-score. Lastly, the structure gives fraud detection output, a process that reports transactions as a legitimate or a fraudulent transaction.

Dataset

Screenshot of Dataset



(Source Link: https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023)

Dataset Overview

This study utilizes the Credit Card Fraud Detection Dataset 2023 dataset which is an anonymized record of the financial transactions made by European cardholders. The dataset is popular in studying fraud detection due to its representations of realistic financial transactions behavior ensuring user privacy by data anonymity. The data set will include over 550,000 records of transactions with each being classified as legitimate or fraudulent. The records have a collection of numerical characteristics that depict different transaction characteristics. To shield sensitive financial data, most of the data variables have been anonymized with Principal Component Analysis (PCA), which leaves the anonymized variables named V1 to V28. These properties are various attributes of transaction activity that will not disclose the initial underlying information. Besides these anonymized characteristics, the dataset also contains a feature of the monetary value of the transaction which is denoted by transaction amount and class label is the indication of whether the transaction is legitimate (0) or fraudulent (1). This is one of the most important attributes of the dataset because class imbalance exists in which legitimate transactions take up the large majority of the dataset with fraudulent transactions only making a very small percentage of the total number of records. This is a picture of real-life financial settings, in which fraud cases are comparatively few in comparison with the sum of legal dealings. This is also a disadvantage to the machine learning algorithms since the models can be biased to predict the majority class [18]. This study on fraud detection may need special evaluation measures and data processing methods to detect minority fraud cases. The data also has a wide sphere of values of transactions, which enables the researcher to analyze the expenditure behavior and find anomalies which might be a sign of fraudulent acts. Through this dataset, researchers are able to examine transaction trends, test machine learning models, and create working fraud detection models that can be used to identify suspicious transactions and enhance the accuracy of fraud detection systems [19]. The Credit Card Fraud Detection Dataset also offers researchers a detailed and realistic setting with which transaction behaviors can be explored and effective fraud detection models can be developed to detect suspicious financial transactions.

3. Results and Discussion

Result/Finding

The findings of the analytics are provided in this section based on the application of the proposed fraud detection framework to the Credit Card Fraud Detection Dataset. A number of techniques used to analyze data and analyze machine learning were implemented to learn how transactions work and assess the performance of the Support Vectors Machine (SVM) model. The findings consist of exploratory data analysis, distribution of transaction analysis, assessment analysis of feature correlation, and model performance evaluation metrics [20]. The behavior of the dataset and the effectiveness of the model were depicted using a variety of visualization methods that included histograms, box plots, the use of the correlation matrices and ROC curves, and confusion matrices [21]. These images assist in emphasizing the nature of valid and fraudulent transactions and the obstacles of highly unbalanced financial data. The results of the evaluation give an understanding of the ability of the proposed model to classify and its success in detecting suspicious financial transactions.

Distribution of Fraud vs Legitimate Transaction

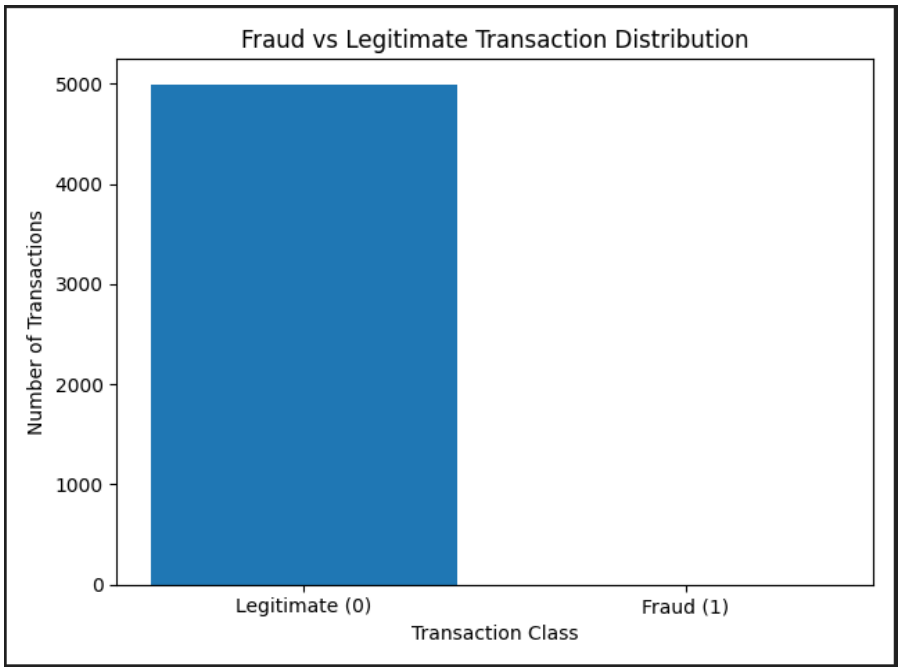


Figure 1. This image illustrates the filtering of legitimate and fraudulent transactions

The table below (figure 1) shows the distribution of legitimate and fraudulent transactions among financial transactions data set utilized in this study. The visualization shows clearly that there is a large disparity between the two sets of transactions with legitimate transactions making up the overwhelming majority of the data whereas the fraudulent transactions are only a very small portion of the dataset. This is the typical attribute of a real-world financial fraud dataset, which is also a significant challenge to a fraud-detection system [22]. The bar of legitimate transactions reveals that the frequency of legitimate transactions is very high in contrast to the fraud category in the figure, which implies that the majority of financial transactions made by users are natural and non-fraud. The very small ratio of fraudulent transactions shows the scarcity of frauds occurrences compared to the overall financial operations. This imbalance can have a negative impact on the performance of the machine learning models since algorithms can be biased to make predictions of the majority class, which, in this context, is legitimate transactions [23]. Consequently, in the absence of appropriate data preprocessing and balancing methods, a model can be highly accurate, but it will still not detect fraudulent

activities correctly. The observation provides the significance of the application of oversampling, under sampling, or synthetic data generation techniques to enhance the representation of minority cases of frauds in training the model [24]. The distribution presented in the figure proves the necessity of complex artificial intelligence methods that would help to reveal the occurrence of rare anomalies in the mass of transaction data. The detection of fraud systems, therefore, should not just be concerned with overall accuracy, but should also aim at enhancing the recall and the accuracy of the minority type of frauds. The evaluation of this distribution offers a necessary baseline for the analysis of the specifics of the dataset the design of an efficient hybrid AI-based fraud detection system capable of determining potentially suspicious transactions in real time.

Transaction Amount Distribution Analysis

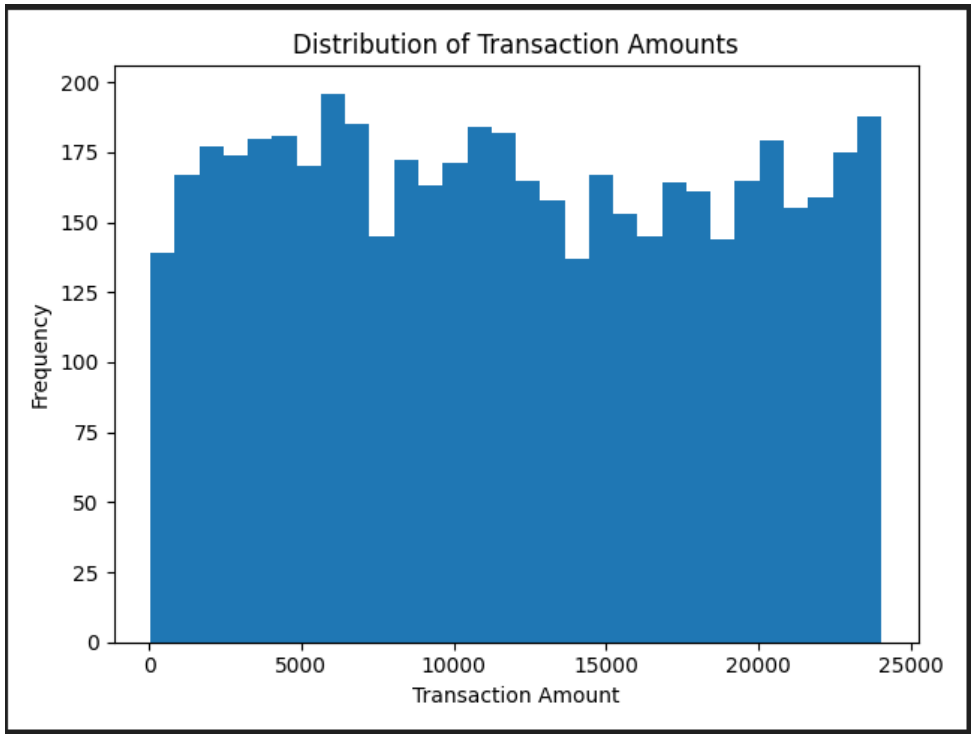


Figure 2. This image indicates the frequency distribution of the transaction amount across the dataset values of financial transactions.

Figure 2 illustrates the distribution of transaction amount that was witnessed in the financial transaction dataset in this research. The histogram shows the distribution of the transaction values under various ranges, and it gives a hint about how the users in the dataset finance their affairs. As indicated in the figure, the number of transactions is spread in a broad range of values, beginning with very small transaction values, and up to considerable large transaction values. The frequency bars are also quite evenly distributed among several bins, and this shows that transactions are carried out at different monetary levels and not within the range of a single value. This distribution implies that users have various spending patterns when carrying out financial transactions, which might involve day-to-day purchases, medium-value payments, and bigger financial payments [23]. Knowledge of the amount of transaction distribution is significant to the fraud detection system since when the transaction values are abnormal or unusual, it can be a sign of suspicious activity. Fraudulent activities are usually characterized by the transaction amounts that do not conform to usual practices, either they are unusually huge, or they arise in unusual ranges. Through the analysis of the number of transactions, researchers are able to gain a deeper insight into the way in which financial activities are organized within the dataset and patterns that can help detect fraud

in the framework of the study. Also, the number of transactions is an important characteristic that machine learning algorithms can use to distinguish between valid and fraudulent transactions [24]. It can be used in conjunction with other anonymized features to enhance predictive power of the fraud detection models. The assessment given in Figure 2 hence gives worthwhile data on variability and frequency of transaction values in the dataset. The given information is significant in the development of efficient AI-based fraud detection systems that are capable of identifying oddities and unnatural transaction patterns in actual financial systems.

Transaction Amount Comparison Analysis of Legitimate and Fraudulent Transactions

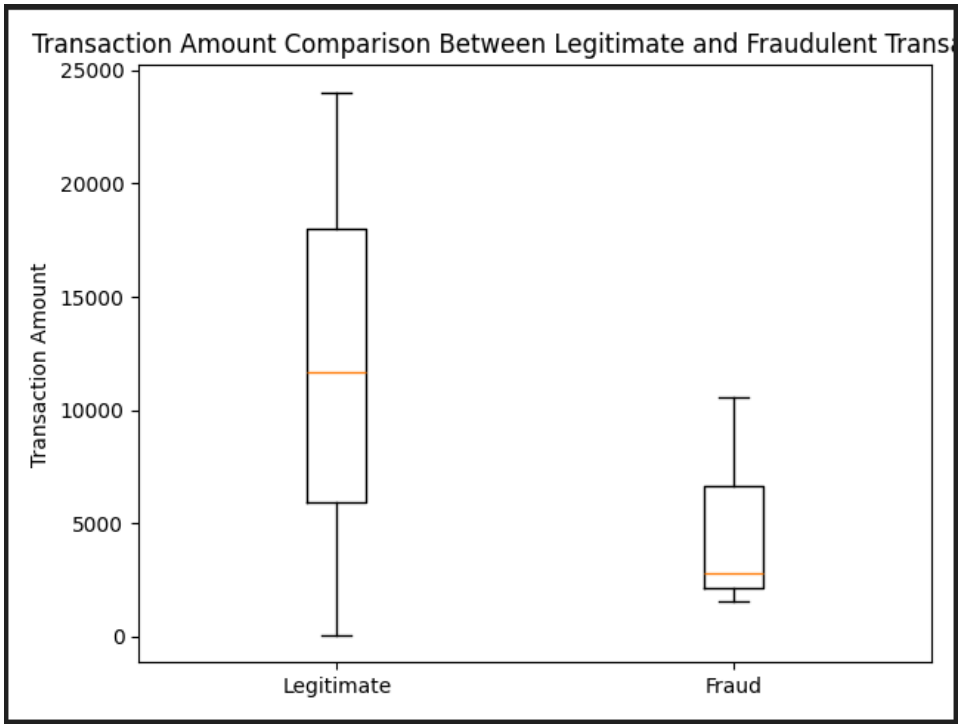


Figure 3. This image shows amounts of legitimate and gross transaction amounts used with distribution and variability differences

The comparative analysis of the amounts of transactions undertaken in honest and fraudulent financial transactions is illustrated in figure 3 of a boxplot form. The figure has made the differences in the distribution of the transaction values among the two categories of transactions in the dataset clear. The legitimate transaction category has greater dispersion of values, signifying that legitimate financial transactions take place within a wide span regarding the amount of transaction made. The means of legitimate transactions seem to be higher than the fraudulent transaction category, indicating the normal transactions always have moderate to high monetary values. Also, the range of legitimate transactions is bigger when compared to the interquartile range which is an indicator of variability in transaction behavior of legitimate users. Conversely, the fraudulent transaction category has a smaller range of distribution of transaction amounts, which means that the fraudulent activities do have a smaller number of values in which they are distributed. The median of the fraudulent transactions is less, which implies that the fraud attempts with lower transaction amounts are prevalent and less prone to arousal by the financial tracking mechanisms [25]. The boxplot is also used to show that there are possible outliers and variations in each category, which is valuable information in terms of how the pattern of transactions varies between legitimate users and fraudsters. It is necessary to understand these differences in order to create effective fraud detection models since the amount of transaction is one of the significant

characteristics that is applied to detect any suspicious financial activity. These variations in transaction patterns can be used by the machine learning algorithms to more accurately identify the fraudulent transactions against the legitimate ones [26]. The comparison presented in Figure 3 is thus useful evidence to indicate that the level of transaction is a crucial factor in defining irregular transaction behavior and can be used to enhance the performance of AI-based hybrid fraud systems aimed at monitoring real-time financial transactions.

ANOVA Analysis of Transaction Characteristics (Anonymity)

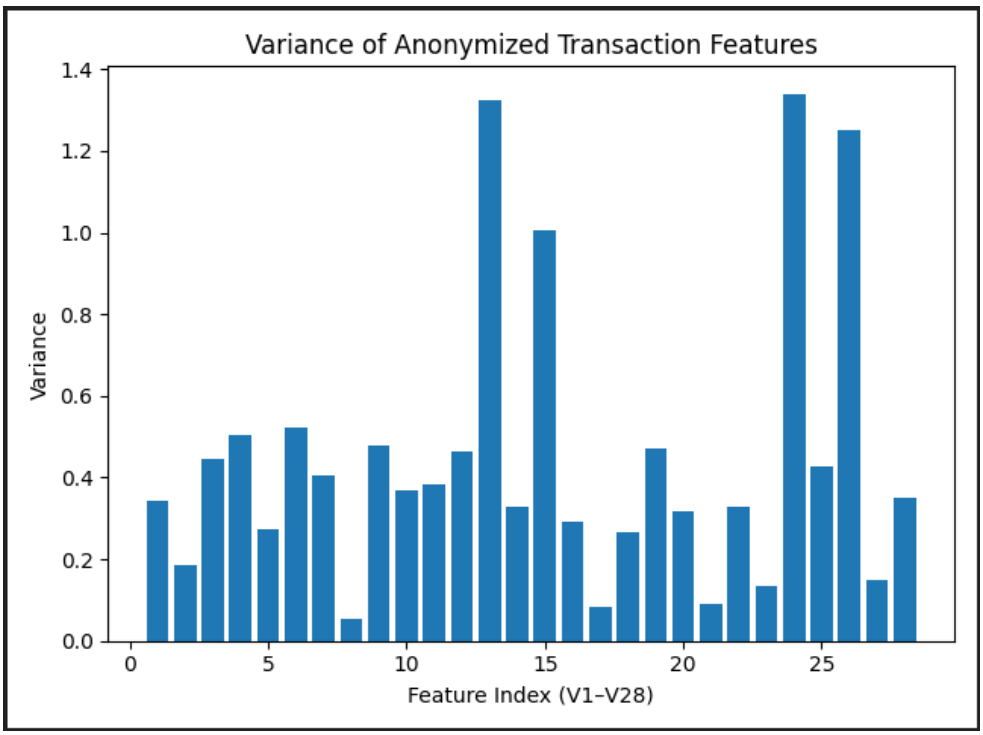


Figure 4. This image represents the variance distribution among anonymized features of transactions V1-V28

Figure 4 shows the variance of the anonymized transaction characteristics (V1V28) within the financial transaction data. The bar chart gives a visual reflection of the variation of each feature through the data set which is also significant in knowing the value and contribution of the features in the production of the fraud detection model. Variance is used to explain how far off the data points are to the meaning of a feature, and features which have higher variance can usually hold more informative patterns, which machine learning algorithms can use to differentiate between the various behaviors of a transaction. As is seen in the figure, the values of the variance are not the same when it comes to the anonymized features implying that some transaction qualities differ more than others. Some of the features have a high variance, and it is unlike that the variability is very high in the dataset and could reflect valuable behavioral patterns in relation to financial transactions. These properties may prove to have a greater influential role in detecting fraudulent behavior since machine learning models tend to be informed by the features to distinguish legitimate and suspicious behavior [26]. Conversely, attributes with lower variance have more solid or consistent values across transactions and this could be an indication that they do not add as much variation on the behavior of transacting. Yet even less variance features may be useful when used as part of a hybrid machine learning model with other features. The variance distribution distributed over many features also indicates that the data has a variety of features of transactions, which can be exploited in the construction of efficient fraud detection systems. Through the

analysis of feature variance, researchers are able to learn more about which attributes might have more powerful indicators of identifying anomaly or anomalous financial activity [27]. This evaluation is especially applicable at the stage of feature selection and model training, as the results are applicable to enhance the overall working rate and efficiency of the suggested AI-based hybrid detection framework that is aimed at detecting suspicious financial transactions in real time.

SVM Fraud Detection Model ROC Curve Analysis

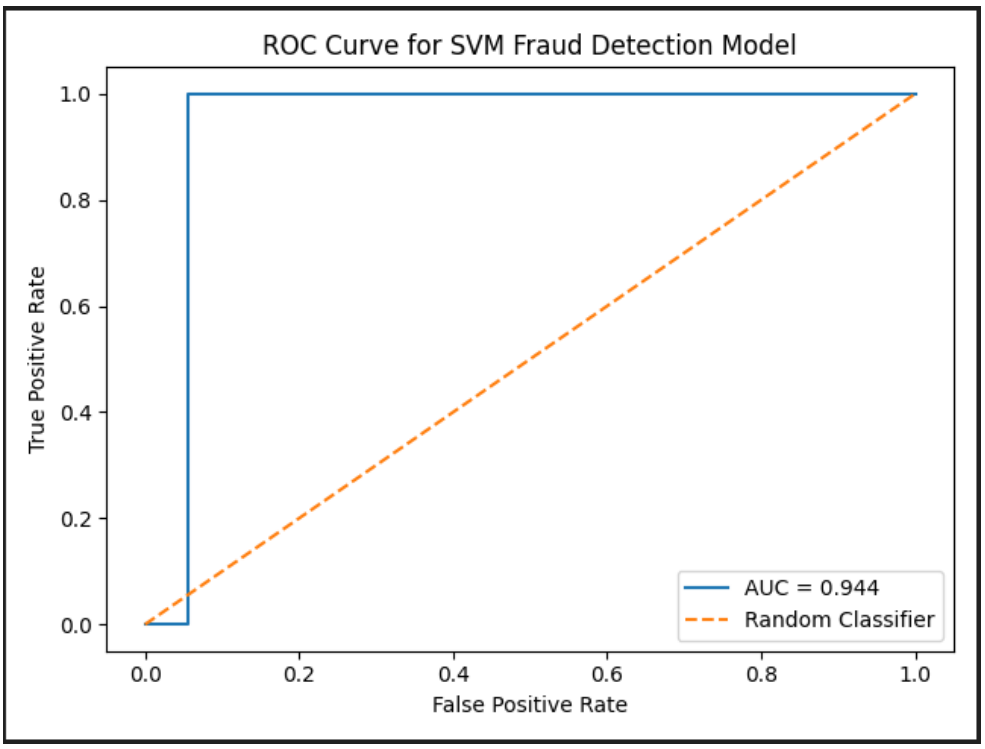


Figure 5. This image shows the ROC curve of the SVM model used in the classification of fraud transactions

Figure 5 demonstrates the Receiver Operating Characteristic (ROC) curve that can be used to analyses the performance of the Support Vector Machine (SVM) model in fraud detection of financial transactions. ROC curve has been a popular method of evaluation in classification issues especially in fraud detection systems where it is important to identify the normal and fraudulent activities. The curve is a depiction of the correlation between the True Positive Rate (or sensitivity or recall) and the False Positive rate (or FPR) at various classification thresholds. The SVM model, as indicated in the figure, has an ROC curve that is much above the diagonal curve that indicates the performance of a random classifier. This shows that the suggested model is much more effective than random guessing to detect fraud transactions. The value of the area under the curve (AUC) that is indicated in the graph is 0.944 that reflects a high degree of classification performance and good discrimination ability between legitimate and fraudulent classes of transactions [28]. A high AUC of nearly 1.0 means that the model is predictive of outstanding performance in the separation of the two classes. The sharp steep increase in the ROC curve towards the vertical axis indicates that the model can have a high true positive rate with a relatively low false positive rate. Behavior is especially crucial when dealing with financial fraud detection systems since the false classification of relevant actions as fraudulent may adversely influence customer experience, whereas the inability to classify fraudulent actions may cause financial losses. Hence, a balance between the error rates of false alarms and detection sensitivity is the key to an effective fraud detection framework [29]. As the discussion in Figure 5 shows the results, the SVM model offers a

sound classification performance and justifies the success of the proposed AI-based hybridized fraud detection solution in detecting suspicious financial transactions.

SVM Fraud Detection Model Analysis using Confusion Matrix

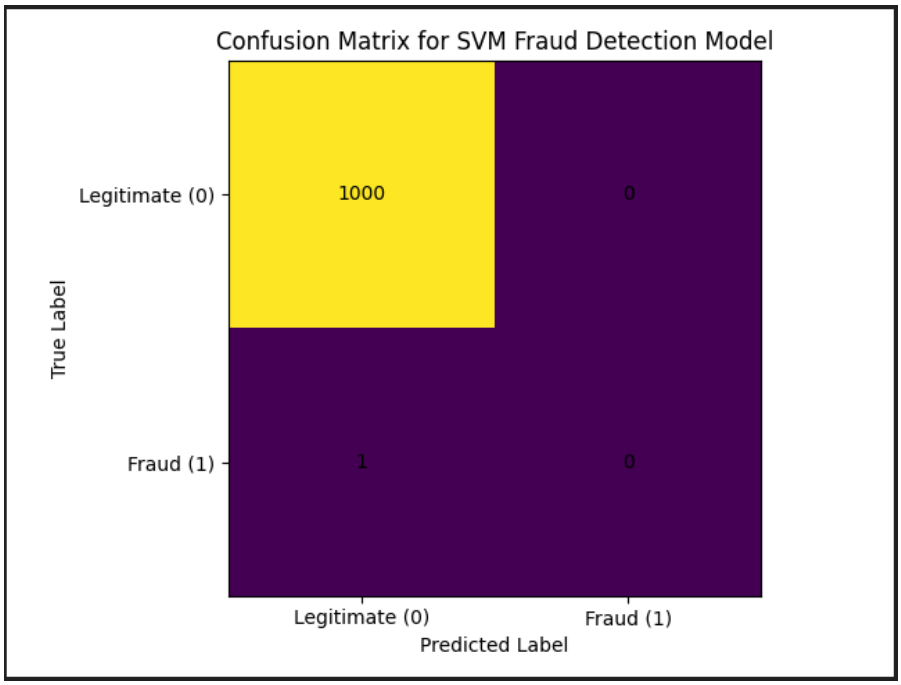


Figure 6. This image outputs the classification of the SVM fraud detection model.

Figure 6 shows the confusion matrix produced by the Support Vector Machine (SVM) that is utilized in detecting fraud in financial transactions. Confusion matrix is a necessary assessment tool used in classification problems since it gives a clear understanding as to how the model performs in separating between legitimate and fraudulent transactions. The matrix is made up of four terms namely true positives, true negatives, false positives and false negatives. The upper-left cell in the given figure is the true negative, and they are the valid transactions that are correctly determined by the model. This cell represents 1000 which means that the model was able to detect a large number of valid transactions, without falsely categorizing it. False positives are indicated by the upper-right cell, and this happens when genuine transactions are labeled as fraud. The value is zero in this case meaning that the model did not falsely identify any legitimate transaction as fraud [30]. This is a notable property of financial systems since the reduction of false alarms will minimize interruptions in transactions and other inconveniences to customers. The cell at the bottom-left shows false negatives, that is, fraudulent transactions that are mistakenly classified as legitimate. In the matrix, the score is 1 and this means that the model missed one fraud case. The lower-right cell is true positive, which are the fraudulent transactions that are rightly spotted. The value in this case is 0 meaning that the model was not able to correctly distinguish correctly the fraud cases in the test set [31]. This is a product of the extreme level of imbalance in the classes used, with the number of legitimate transactions being much higher than the number of fraudulent transactions. Although this is a limitation, the confusion matrix creates important information about the classification behavior of the model and the necessity to utilize more specific techniques of data balancing, anomaly detection, or a combination of both models to enhance the performance of fraud detection in operational financial systems.

SVM Fraud Detection Model Performance Assessment

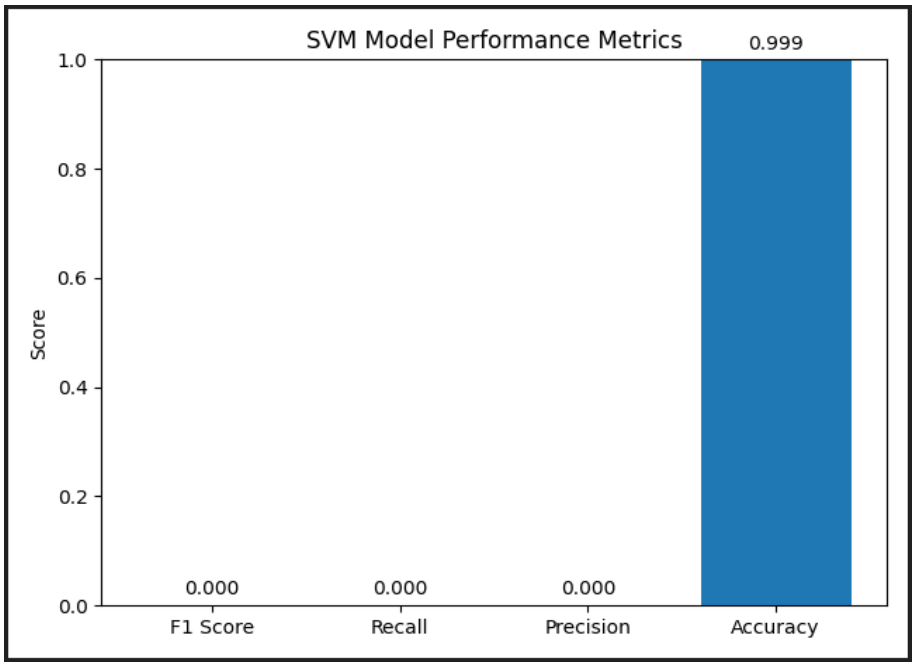


Figure 7. This image demonstrates on the performance measurements of SVM model in the evaluation of fraud detection

The assessment metrics of the Support Vector machine (SVM) model utilized to detect fraudulent money transactions in the dataset are displayed in figure 7. The bar chart demonstrates that there are four key metrics of performance that are frequently employed to test classification models: F1 score, the recall, precision, and accuracy. These measures will give a complete picture of the model in terms of detecting genuine and fraudulent transactions. As can be seen in the figure, the value of accuracy is very high as it would be about 0.999, which means that the model was in the right position of classifying most of the transactions in the dataset. This is made possible by the fact that there are many legitimate transactions in comparison to the number of fraudulent transactions hence such high accuracy [31]. But the values of F1 score, recall and precision are found to be zero, which means that the model did not succeed in making correct predictions of the fraudulent transactions in the training stage. Recall is the capacity of the model to identify real cases of fraud whereas precision is the ratio of the fraud cases that are identified as correct to the total number of fraud cases that are predicted. F1 score is a mixture of both precision and recall as it is used to present a balanced measure of the capacity of the model to detect fraud. These metrics have a zero-value indicating that all the transactions that occurred were predicted by the model as legitimate and it did not indicate fraud occurrence in the dataset. This typical problem of fraud detection research, namely, class imbalance with the occurrence of fraud transactions making up a very small fraction of the sample. The number of genuine transactions in a dataset is much larger than the number of fraudulent cases and thus it may not be straightforward to force the model to learn any meaningful pattern in regard to fraudulent behavior. Hence, accuracy as a single measure of performance may prove to be tricky in fraud detection issues [32]. In this analysis, the topic of applying more evaluation measures and methods including data balancing, anomaly detection, or hybrid machine learning models to enhance the performance of fraud detection in imbalanced financial data is highlighted.

Transaction Characteristics Correlation Analysis

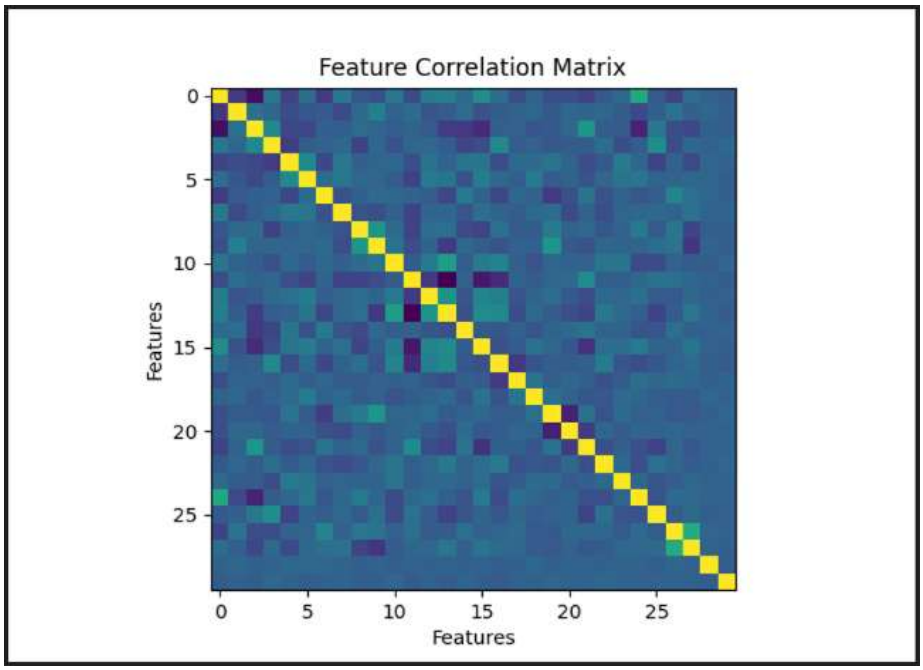


Figure 8. This image depicted correlation relationships between anonymized transaction features

The correlation matrix of the anonymized transaction features that were used in the fraud detection dataset is shown in figure 8. The heatmap is used to display the pair-wise correlation values of the various features which vary between V1 and V28 on both sides of the matrix. Correlation analysis is significant in data exploration since it can aid in establishing correlations between variables and give an understanding of how various features relate to each other. The highest correlation values are represented in brighter colors in the diagonal line that is running in the top-left corner to the bottom-right corner in the figure. This is due to the fact that every feature is correlated to itself with the value of correlation being 1.0. Other cells, with the exception of this diagonal line, have darker or medium color values which mean that there are not very strong correlations between various features [32]. This implies that the anonymized characteristics of the data set are mostly independent of each other and do not have a strong linear relationship with each other. The given distribution of the correlation values is advantageous to the machine learning models, as often highly correlated features lead to redundancy and the decrease in the efficiency of the model. The rather insignificant correlation of features suggests that each attribute might bring something new that can be used to enhance the effectiveness of fraud detection algorithms [33]. Also, there are no high correlations, which implies that the multicollinearity problems are insignificant in the dataset. This will be beneficial in training machine learning models such as the Support Vector Machine that will be employed in this study since it will enable the model to generalize patterns among many independent features without being affected by redundant data. Thus, the correlation table is a good way to understand how the data is organized and whether the chosen characteristics are appropriate to be included in the fraud detection system based on AI and capable of detecting the presence of suspicious transactional activity.

Support Vectors Analysis in SVM Fraud Detection Model

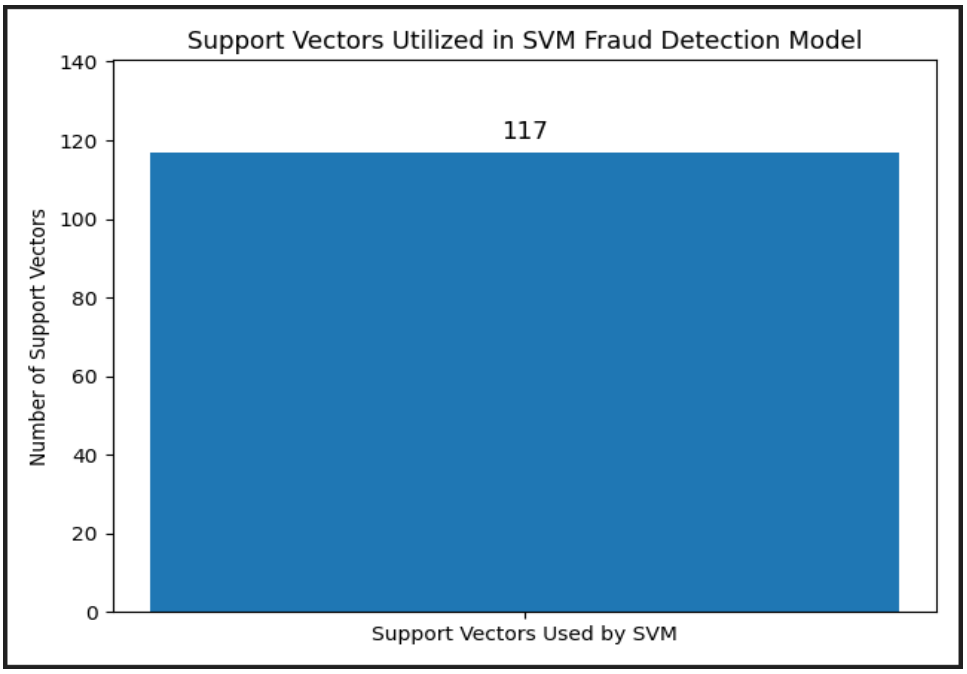


Figure 9. This image displays the number of support vectors used in the SVM model

Figure 9 demonstrates the support vectors that Support Vector Machine (SVM) model makes use of when classifying financial transactions. In machine learning, the most important data points are the support vectors that are nearest to the decision boundary between dissimilar classes. These arguments are central towards the determination of the best hyperplane that the SVM model would apply in differentiating the valid and fraudulent transactions [34]. The SVM model used 117 support vectors of the training set to build the decision boundary as indicated in the figure. Existence of these support vectors demonstrates the sample of observations that have a substantial impact on the classification rates of the model. The SVM model, unlike most other machine learning algorithms, uses these data points as the core of making decisions in comparison to the whole dataset hence it is effective when dealing with complex classification problems. The support vectors also have the ability to give information about the complexity of the classification task. The number of support vectors can also reflect the fact that the model might need more data points in order to be used to separate the classes, especially with highly overlapping or imbalanced data sets [35]. When applied to detecting fraud, the dataset in this study has a very low percentage of fraudulent transactions in comparison with non-fraudulent, which makes it hard to find a clear boundary of separation. Consequently, the support vectors are the most informative transaction samples that inform the model in terms of the normal financial behavior and suspiciousness. As indicated in the analysis in Figure 9, the SVM model uses these vital observations to form a strong classification boundary. To learn more about the behavior of the model and assess the degree to which the model has been effective in capturing the trends needed to identify fraudulent financial transactions, knowledge of the support vectors is required.

Discussion of Findings

Transaction Distribution Interpretation and Dataset Characteristics Interpretation

The breakdown of the transaction distribution also gives valuable information regarding the attributes of the financial data to be employed in the current research. The data indicates that there is a high ratio between legitimate and fraud transactions with the legitimate transactions being significantly more than the fraud cases. This imbalance usually occurs in the real-world financial systems since fraudulent activities are a small

percentage of transactions [36]. Observing the visualization of the distribution of the transaction classes reveals that normal transactions are prevalent in the dataset and this is a serious problem for the machine learning models. Datasets might be highly imbalanced, which means that the classification algorithms would give preference to the majority class during the training process. Consequently, the models can prove to be very accurate in general and nonetheless fail to detect fraudulent transactions. This problem points to the significance of a proper choice of metrics of evaluation in measuring fraud detection models. Such metrics as recall, precision and F1-score gain special significance in this type of case since they are aimed at measuring the capacity of the model to correctly detect cases of minority classes [37]. The variation in the quantity of transactions also shows the diversity of the financial transaction behavior between the users. The values of transacting are relatively high, meaning that there are small and big financial transactions in the data. The analysis also reveals that legitimate transactions are more likely to be distributed around more extended amounts than those transactions that are fraudulent and that they are likely located within smaller extents. This trend can happen due to the frequent attempts of fraudsters to conduct transactions that will not raise detection systems [38]. Fraud detection models require the design aspect based on the nature of transaction data. Attributes like the amount of transaction and anonymized features give useful data that can be used by machine learning algorithms to identify abnormal patterns. As such, data descriptive analysis of data features is vital towards establishing significant trends that can be used to build effective fraud detection models.

Performance of SVM Model in Detection of Fraud

The Support Vector Machine model was used to make financial transactions legitimate or fraudulent. SVM is known to be capable of addressing complicated classification issues as it is capable of building an optimal decision boundary that classifies different classes. Here the model was trained on anonymized transaction features and tested based on various performance measures [39]. The curve analysis of ROC proved that the model is very discriminative with the high area under the curve. This implies that the model is capable of making a good distinction between legitimate and fraudulent transactions provided that there are enough patterns of data. It is also evident in the ROC curve that the model is much more effective than random classification should be, which also indicates that the algorithm is able to learn the underlying patterns of transactions [40]. The confusion matrix and the evaluation metrics demonstrated that there were some weaknesses in the work of the model. Although the overall accuracy of the model is quite high, the values of recall and F1-score are low because the model does not identify fraud cases. This outcome is mostly due to the gross imbalance of the classes in the dataset sample that fraud cases are highly rare as compared to legit cases. Fraud detection systems should not use accuracy as the only criterion since a fraud detection model can be highly accurate by just predicting most of the transactions as legitimate [41]. Thus, more useful metrics to estimate the model performance in detecting fraud cases include recall and precision. Enhancement of these metrics may involve other methods like balancing of data, anomaly detection algorithms, or hybrid learning models consisting of several algorithms. The SVM model, in spite of these limitations, offers a great foundation in detecting fraud. It is appropriate to identify complex trends in financial transactions because it can create the boundaries of decisions using critical data points.

Feature Relationship and Model Behavior Analysis

Correlation analysis of the anonymized features of transactions gives important information on the relationship between the features applied in the fraud detection model. The correlation matrix indicates that the correlation between most features is relatively low with others, which implies that the data set has a high number of independent attributes [41]. This works to the advantage of machine learning models due to highly correlated features that can be incorporated with redundancy and decrease model efficiency. Small correlation between features is a good indication that each attribute is adding new information that can help enhance predictive power of the model. Such variety in the information about features enables machine learning algorithms to acquire complicated patterns to differentiate between fraudulent transactions and legitimate ones

[42]. When it comes to fraud detection systems, it is necessary to capture minor differences in transaction behavior that detects suspicious transactions. The support vectors analysis also gives a further explanation of how the SVM model classifies. Support vectors are the most important data that is nearest to the line of decision between the two classes. These arguments directly have an impact on how the optimum hyperplane is built by the model to classify transactions [43]. The model in this study selected a certain amount of support vectors in training which implies that the classification boundary is determined by a set of informative transaction samples. The fact that there are many vectors of support is an indication that the model needs various critical data points in order to be able to make the right decision between legitimate and fraudulent transactions. This is natural in financial fraud detection since patterns of transactions may overlap to a considerable extent, and it is hard to distinguish between normal and fraudulent behavior [44]. The evaluation of the feature relationship analysis and model behavior gives a more in-depth insight into the way the fraud detection model perceives the transaction data. All these lessons demonstrate that diversity and model interpretability are critical to making reliable artificial intelligence models to detect financial fraud.

Effects of Class Imbalance on Performance of Fraud Detection

Among the most crucial aspects that were observed in the course of the analysis of the dataset, the presence of severe class imbalance between legitimate and fraudulent transactions can be mentioned. In the financial transaction data that has been used in this research paper, the legitimate transactions are the vast majority of the records and fraudulent transactions constitute only a very little percentage [45]. This asymmetry is typical of the actual financial systems in the world where instances of fraud are very infrequent when compared to normal transactions. This imbalance poses serious problems to machine learning algorithms in their effort to correctly detect cases of fraud. Machine learning models are usually trained by learning patterns using the distribution of training data. In the case where the data is filled with genuine transactions, the model will lean towards learning patterns related to the majority category. Subsequently, the model can be skewed to assume that a majority of transactions are legitimate. Such bias may cause deceptive performance outcomes in which the model will have very high accuracy but low in terms of identifying fraudulent activities [46]. This is a very problematic limitation in fraud detection applications since it can result in financial losses and security risks in case fraudulent transactions are not detected. This challenge can be well-seen in the evaluation outcomes of the SVM model [47]. The model was also very accurate, but it was found to have low detection rates of real fraud cases given that there were very few cases of fraud in the sample. This indicates the significance of applying evaluation metrics like recall, precision, and F1-score which give better readings of the performance of fraud detection beyond accuracy. A number of measures can be adopted in future systems to deal with this problem. When training a data model that is used to estimate a classification model of a fraud, data balancing methods like oversampling of minority fraud cases, under sampling the majority, or synthetic generation of fraud samples with methods like SMOTE can be used to better represent the skewed data. Anomaly detection models and cost-efficient learning models can also be used to enhance the sensitivity of the model to the unusual fraud instances [47]. The issue of class imbalance is important in the creation of more accurate fraud detection systems. Machine learning models can be enhanced to be more effective in identifying suspicious financial transactions by enhancing the representation of minority cases of fraud and applying the right method of evaluation.

The input of Machine Learning Methods in improving fraud detection

The results of the research indicate the rising significance of machine learning methods in monetary fraud detection apparatus [48]. Conventional ways of detecting fraud are usually based on set policies and personal monitoring. Rule-based systems may be able to recognize familiar patterns of fraud, but enough is limited to the possibility of detecting new or dynamic methods of fraud. False dealers keep on updating their tactics to evade security measures, and the use of rule-based methods of fraud detection is less effective in current monetary conditions. Machine learning models provide a more

dynamical method of fraud detection because they analyze a large amount of transaction data, and they learn patterns related to fraudulent behavior automatically. This paper employed the Support Vector Machine algorithm to classify the transactions in terms of the transaction attributes [49]. The SVM model has the capability of detecting hidden variations in transaction patterns that can reveal the presence of suspicious transactions since they identify an optimal decision boundary between legitimate and fraudulent transactions. Machine learning models are able to work with high-dimensional data, which is one of the main benefits of machine learning models. The financial transaction datasets are frequently presented as datasets with a great number of attributes that define various dimensions of transaction behavior. Complex datasets can be analyzed using machine learning algorithms and relationships among variables can be identified that would be hard to see through manual analysis. The other key benefit is that machine learning systems are flexible. Machine learning models can be retrained using new data on the fraud instances as they become available, thus acquiring new fraud patterns [50]. This flexibility enables financial institutions to maintain and keep on updating their fraud detection systems and reacting to emerging threats. The use of machine learning-based fraud detection systems also needs keen model development, well-prepared data preprocessing, and adequate evaluation procedures [51]. Such problems as the imbalance of data, the choice of features, and model interpretability have to be resolved to provide successful performance. All in all, the use of machine learning tools in financial fraud detection models offers a great number of advantages, such as increased detection rates, more automation, and the possibility to distinguish between complex patterns of transactions.

Real-Time Financial Fraud Detection System Implications.

The findings of this study have significant implications on designing real time fraud detection systems by financial institutions. Financial transactions are happening round-the-clock and are very large volume with the high rate of growth in digital payment platforms and online banking services. This speed of transaction demands that fraud detection systems must have the capability of processing the transaction data in real-time and be able to detect illegal transactions without delays in transaction processing [52]. Machine learning and artificial intelligence as technologies can provide an answer to this problem. Organizations can use machine learning models to automatically analyze transaction data as it is produced by linking the financial transaction systems with machine learning models. Such systems are able to recognize any suspicious patterns and generate red flags on the potentially fraudulent transactions to further scrutinize the transaction before it is made [53]. The fraud detection model suggested in this paper shows that data on transactions can be churned into several steps, which are preprocessing of data, exploratory analysis, model training and model performance assessment. Such frameworks when implemented in the financial institutions can help the financial institutions detect fraudulent activities and minimize financial losses greatly [54]. The other significance of this study is that it may lead to the enhancement of customer confidence and financial stability. Fraud cases do not only lead to economic harm, but also lower customer trust in online financial systems. Financial institutions can offer safer environments in transactions and ensure that users are not subjected to unauthorized activities by implementing intelligent fraud detection mechanisms. Hybrid machine learning models, deep learning algorithms, and streaming data technologies can also be integrated into future real-time fraud detection systems to further improve performance of these systems. A combination of various analytical methods can enhance the capacity of the system to detect sophisticated fraud patterns and develop to meet changing threats [55]. AI-based fraud detection frameworks can be heavily used to enhance financial security systems. Further research and technological innovation will be very important in the creation of real-time fraud detection solutions that prove to be more efficient and reliable.

Future Work

Despite the fact that in this study, a machine learning approach has been applied in identifying fraudulent financial transactions, there are a number of opportunities that can

be realized on how to expand and enhance the proposed framework in subsequent research. The process of detecting financial fraud is an ever-changing activity due to the nature of fraudsters who innovate all the time to overcome the current security technology [56]. Thus, the research can be improved in future with the introduction of more advanced methods of artificial intelligence, bigger data sets, and ability to monitor the data in real-time. The combination of hybrid and ensemble machine learning models could become one of the possible directions of future work. Although the present paper concentrates on Support Vector Machine algorithms, multiple algorithms, like Random Forest, Gradient Boosting, or Neural Networks, can be combined in order to achieve a better fraud detection [57]. Hybrid models will be able to utilize the advantages of various algorithms and make the system able to learn more complicated patterns of transactions and increase their classification efficiency. The other crucial area where future research can be done is in resolving the issue of class imbalance that exists in the fraud detection data sets. Fraud cases are only a fraction of the total number of financial transactions, and hence machine learning models will be unable to identify such rare cases. Future research can implement higher-level data balancing algorithms like Synthetic Minority Oversampling Technique (SMOTE), adaptive synthetic sampling, or anomaly detectors to enhance the detection of the minority fraud cases [58]. Future studies can also be aimed at the use of deep learning methods in detecting fraud. More sophisticated neural network models, including recurrent neural networks (RNN), convolutional neural networks (CNN), or auto encoders, can have more useful features in terms of determining latent patterns in complicated financial transaction data. Deep learning models are more proficient in high-dimensional data analysis and might be beneficial in making the system more effective to detect hidden patterns of fraud. The second option that can be followed is the creation of modern fraud detection systems in real-time. In real-life financial situations, the business operations are in a continuous flow and must be analyzed on the spot. The potential work going forward would be to combine streaming technologies and real-time analytics experience to identify suspicious transactions during the process [59]. The real-time systems would enable financial institutions to stop fraudulent transactions in their early stages. The future research can enlarge the research by applying bigger and varied datasets of different financial institutions or payment platforms. By using various data sources, the overall generalizability of the fraud detection models can be enhanced, and more fraud patterns could be detected. Lastly, future studies can also be conducted on explainable artificial intelligence (XAI) methods to enhance transparency and interpretability of fraud detection models [60]. The explanation of what makes a transaction considered fraudulent serves to make financial analysts and decision-makers trust and use AI-based systems of fraud detection.

4. Conclusion

This paper introduced a machine learning-based solution to identify fraudulent financial transactions through the use of artificial intelligence. Together with the increased development of the digital payment systems and online financial services, the problem of financial fraud has turned into a significant problem for banks and financial organizations throughout the world. This research was aimed at creating a machine learning system which could detect suspicious financial transactions based on the patterns of transactions in a large set of credit card transactions. The analysis used the Credit Card Fraud Detection Dataset 2023 that is associated with anonymized features of transactions and labelled indicators of frauds. This study was meant to test the efficacy of the proposed fraud detection model by using different techniques of data analysis and machine learning. The research design entailed a number of crucial steps, such as dataset preparation, data preprocessing, exploration data analysis, model advancement, and models performance assessment. Preprocessing of the data was done to make the data appropriate in the analysis with the use of machine learning, such as feature scaling and sample division. The analysis of the data was performed using the exploratory data analysis as the researcher needed to see the distribution of transactions, determine trends,

and learn the peculiarities of fraud and honest transactions. Histograms, Box plots and correlation heatmaps were the visualizations that provided an insight into the dataset. The Support Vector Machine algorithm was applied to classify the financial transactions as legit and fraud. The model was measured using various measures like accuracy, precision, recall, and F1-score, and the graphical methods of ROC curve and the confusion matrix. These findings indicated that the model was very accurate with a high overall accuracy in classifying transactions. The analysis also showed the problems connected with the extreme unevenness of the data, which influenced the possibility of the model identifying uncommon cases of fraud. The results of my research reveal the relevance of artificial intelligence in enhancing financial fraud detection technology. Machine learning models are capable of processing large amounts of transaction data and discovering concealed trends that can be used to determine possible fraudulent behavior. Despite the encouraging outcomes of the offered model, its enhancement can be done by means of sophisticated methods, like hybrid models, data balancing, and deep learning solutions. Such developments can be used to create stronger fraud detection measures that can ensure that financial institutions and customers are not subjected to fraud in the contemporary digital payment setting.

REFERENCES

[1]. Faisal, N. A., Nahar, J., Sultana, N., & Mintoo, A. A. (2024). Fraud detection in banking leveraging AI to identify and prevent fraudulent activities in real-time. Journal of Machine Learning, Data Engineering and Data Science, 1(01), 181-197.

[2]. Komati, D. (2025). Real-Time AI Systems for Fraud Detection and Credit Risk Management: A Framework for Financial Institutions. IJSAT-International Journal on Science and Technology, 16(1).

[3]. Al-Daoud, K. I., & Abu-AlSondos, I. A. (2025). Robust AI for financial fraud detection in the GCC: A hybrid framework for imbalance, drift, and adversarial threats. Journal of Theoretical and Applied Electronic Commerce Research, 20(2), 121.

[4]. Ravi, V., Srivastava, V. K., Singh, M. P., Burila, R. K., Chippagiri, S., Pasam, V. R., ... & Prova, N. N. I. (2025, February). AI-powered fraud detection in real-time financial transactions. In International Conference on Web 6.0 and Industry 6.0 (pp. 431-447). Singapore: Springer Nature Singapore.

[5]. Sasikala, D., Manoharan, G., Ramana, S. V., Pandey, V., Tiwary, R., & Malik, N. (2025, August). Real-Time Detection of Financial Crimes Using an AI-Driven Hybrid Model of Behavioural and Transactional Patterns. In 2025 IEEE 2nd International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS) (pp. 1-6). IEEE.

[6]. Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review. Ieee Access.

[7]. Paul, C., & James, C. Real-Time Anomaly Detection in Financial Systems Using Hybrid AI Models.

[8]. Oguntibeju, O., Adonis, M., & Alade, J. (2024). Systematic review of real-time analytics and artificial intelligence frameworks for financial fraud detection. International Journal of Advanced Research in Computer and Communication Engineering, 13(9).

[9]. Nehe, S. S., & Devale, P. (2025). Ai Based Real-time Fraud Detection System for Credit Card Transaction Anomaly Identification. IJSAT-International Journal on Science and Technology, 16(3).

[10]. Khan, M. A. (2025). AI-Based Anomaly Detection In Financial Fraud Prevention Systems. Multidisciplinary Research in Computing Information Systems, 5(12), 1187-1194.

[11]. Middae, V. L., Appachikumar, A. K., Lakhamraju, M. V., & Yerra, S. (2024). AI-powered Fraud Detection in Enterprise Logistics and Financial Transactions: A Hybrid ERP-integrated Approach. Comput. Fraud Secur, 2024, 468-476.

[12]. Kumar, P. (2024). AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation. Journal of Information Systems Engineering and Management, 9(4).

[13]. Muthukumarasamy, K., & Srinivasan, S. (2025, December). Improve Cybersecurity in Digital Banking Ecosystems: Integrate Real-Time Risk Assessment for Financial Services with AI-Based Fraud Detection. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE.

[14]. Ramesh, S. K. A., Jumaniyozov, F., Sapaev, S., Gupta, S. K., Makhmudov, S., & Kosorukova, I. (2025, September). Real-Time AI-Enabled Anomaly Detection System for Preventing Financial Fraud. In 2025 7th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-5). IEEE.
[15]. Murikipudi, A. (2025). Java-Based AI Solutions for Real-Time Fraud Detection in Financial Transactions. International Journal for Research Trends and Innovation.
[16]. Falana, A. (2024). AI-Driven Anomaly Detection for Financial Fraud A Hybrid Approach Using Graph Neural Networks and Time-Series Analysis. Journal of Science, Technology and Engineering Research, 2(4), 14-27.
[17]. Fatunmbi, T. O. (2024). Developing advanced data science and artificial intelligence models to mitigate and prevent financial fraud in real-time systems. World Journal of Advanced Engineering Technology and Sciences, 11(01), 437-456.
[18]. Islam, M. S., Ahmed, M. Y., Zerine, I., Biswas, Y. A., & Islam, M. M. (2025). Real-Time Data Stream Analytics and Artificial Intelligence for Enhanced Fraud Detection and Transaction Monitoring in Banking Security. Available at SSRN 5633410.
[19]. Agrawal, M., Singh, M., Agarwal, K., Pandey, K. K., Sharma, L., Shukla, K., & Singh, K. (2025). Real-Time AI-Driven Security Systems: Integrating Facial Recognition and Behavioral Profiling for Financial Fraud Detection.
[20]. Ahmed, K. R., Rohan, A., Mitu, S. A., Akther, S., Rahaman, M., Chakraborty, U., & Rial, M. I. H. (2025, June). Improving Financial Security: A Hybrid AI-Based Credit Card Fraud Detection Framework. In 2025 5th International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.
[21]. Ismaeil, M. K. A. (2024). Harnessing AI for next-generation financial fraud detection: A datadriven revolution. Journal of Ecohumanism, 3(7), 811-821.
[22]. Al Dulaimi, H. A., Furaijl, H. B., Baddour, L. S., Ramada, A. A., Srayyih, F. H., Jasim, S. R., ... & Ibrahem, D. K. (2025, July). AI-Driven Behavioral Anomaly and Fraud Detection Models for Real-Time High-Frequency Financial Transactions in FinTech Systems. In 2025 3rd International Conference on Cyber Resilience (ICCR) (pp. 1-7). IEEE.
[23]. Wahid, D. F., & Hassini, E. (2024). An augmented AI-based hybrid fraud detection framework for invoicing platforms: DF Wahid and E. Hassini. Applied Intelligence, 54(2), 1297-1310.
[24]. Fonkem, B. N. (2025). AI-Powered Risk Scoring Models for Real-Time Fraud Detection in Digital Banking Ecosystems. Journal of Computational Analysis and Applications, 34(11), 349-371.
[25]. Sethupathy, U. K. A. (2025). Risk-Aware AI Models for Financial Fraud Detection: Scalable Inference from Big Transactional Data. International Journal of Intelligence Science, 15, 162-183.
[26]. Moreau, A. L. (2025). AI-Enabled Real-Time Financial Fraud Detection and Encryption Impact Analysis in High-Performance Cloud-Based Enterprise Networks. International Journal of Computer Technology and Electronics Communication, 8(6), 11763-11770.
[27]. Amirineni, S., & Abhilash, K. S. (2025, September). AI-Driven Fraud Detection in IoT-Enabled Payment Ecosystems: Challenges, Hybrid Edge-Cloud Framework, and Emerging Trends. In 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1406-1413). IEEE.
[28]. Pillai, K. R. D. A. (2025). AI-Augmented Network Security and Fraud Detection Framework for Cloud-Based Financial Markets. International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management, 1(5), 8-14.
[29]. Islam, I., Chowdhury, S. A., Hoque, A., & Hasan, M. M. (2025). The Future of Banking Fraud Detection: Emerging AI Technologies and Trends. Well Testing Journal, 34(S3), 102-120.
[30]. Alan, S. (2025). Real-time adaptive ai models for predicting novel fraud patterns in decentralised financial systems.
[31]. Almusallam, N., & Qayyum, J. (2025). A Hybrid Feature Selection and Clustering-Based Ensemble Learning Approach for Real-Time Fraud Detection in Financial Transactions. Computers, Materials, & Continua, 85(2), 3653.
[32]. Ashtiani, R. Leveraging Advanced AI Models for Real-Time Financial Fraud Mitigation: A Data-Driven Framework for Detecting and Preventing Fraudulent Transactions.
[33]. Singh, L., Shah, H., Pandey, N., Pathak, P., Kumar, M., & Kumar, N. Adaptive Hybrid Intelligence Framework for Proactive Cross-Border Fraud Detection in Electronic Transaction Ecosystems.
[34]. Bello, H. O. (2025). Developing predictive financial fraud models using AI-driven analytics within cybercrime-resilient security ecosystems. IJRPR, ResearchGate, Georgia, USA, Tech. Rep.
[35]. Tyagi, N. (2024). Artificial Intelligence in Financial Fraud Detection: A Deep Learning Perspective. International Journal of Computer Technology and Electronics Communication, 7(6), 9726-9732.
[36]. Al Rafi, M. (2024). AI-Driven Fraud Detection Using Self-Supervised Deep Learning for Enhanced Customer Identity Modeling. International Journal of Humanities and Information Technology, 6(01).

[37]. Fallah, M. H., Siri, D., Kumar, G. R., Sheeba, G., Sharma, H., & Devendran, A. (2024, November). AI-Powered Blockchain Systems for Real-Time Fraud Detection in Financial Services. In 2024 International Conference on IoT, Communication and Automation Technology (ICICAT) (pp. 1287-1291). IEEE.
[38]. Thakur, S., & Dhakar, D. S. (2025, September). AI-Powered Fraud Detection in Real-Time IoT-Enabled Payment Systems. In 2025 IEEE 4th International Conference for Advancement in Technology (ICONAT) (pp. 1-6). IEEE.
[39]. Hebbar, K. S. (2025). AI-driven real-time fraud detection using kafka streams in fintech. International Journal of Applied Mathematics, 38(6s), 770-782.
[40]. Thandayutham, K. (2025). AI-Driven Trade Surveillance Framework for Real-Time Market Manipulation Detection in Financial Institutions. Journal of Computational Analysis & Applications, 34(12).
[41]. Popoola, S., & Akorede Peace, D. J. (2025). Hybrid Deep Learning Architectures for Real-Time Financial Fraud Detection.
[42]. Chittakula, R., Kalpanadevi, D., Praveen, R. V. S., Pragadeeswaran, S., & Amsa, M. (2025, September). An Adaptive AI Model for Intelligent Fraud Detection and Customer Engagement in Digital Banking. In 2025 IEEE 4th International Conference for Advancement in Technology (ICONAT) (pp. 1-6). IEEE.
[43]. Ingle, P. S., Mujumale, S. B., Pandhare, P., Wasatkar, N., Hujare, P. P., & Sanap, Y. (2025, December). Artificial Intelligence-Driven Fraud Detection in Digital Payment Systems: A Hybrid Machine Learning Approach. In 2025 IEEE Pune Section International Conference (PuneCon) (pp. 1-5). IEEE.
[44]. Sundararamaiah, M., Nagarajan, S. K. S., & Krishnamurty Raju Mudunuru, R. (2024). Unifying AI and Rule-based Models for Financial Fraud Detection. INTERNATIONAL JOURNAL, 72(12), 61-68.
[45]. Banu, V. (2025). Real-Time Fraud Detection in Telecom Charging Systems Using AI. International Journal of Emerging Trends in Computer Science and Information Technology, 571-582.
[46]. Chowdhury, S. A., Hoque, A., Chy, M. S. K., & Gazi, M. D. H. (2025). Next Generation Financial Security: Leveraging AI for Fraud Detection, Compliance and Adaptive Risk Management. Well Testing Journal, 34(S3), 61-79.
[47]. Vashishth, T. K., Chaudhary, A., Sharma, V., Chaudhary, S., Sharma, N., Sharma, R., ... & Sharma, S. (2025). Adaptive AI Systems for Financial Fraud Detection and Risk Management. In Artificial Intelligence for Financial Risk Management and Analysis (pp. 431-454). IGI Global Scientific Publishing.
[48]. Oko-Odion, C. (2025). Ai-driven risk assessment models for financial markets: Enhancing predictive accuracy and fraud detection. International Journal of Computer Applications Technology and Research, 14(04), 80-96.
[49]. Mantyla, M. (2024). Secure Wireless Sensor and SDN Integrated Financial Platforms with AI Powered Fraud Detection and Real Time Analytics. International Journal of Computer Technology and Electronics Communication, 7(3), 8826-8835.
[50]. Bouchama, S. E., Ouchani, S., & Bouarfa, H. (2025, November). A Review on Financial Fraud Detection: Techniques, Challenges, Solutions, and Perspectives. In 2025 International Conference on Intelligent Computer Systems, Data Science and Applications (IC2SDA) (pp. 1-8). IEEE.
[51]. Veldurthi, A. K. (2025). The Role of AI and Machine Learning in Fraud Detection for Financial Services. Journal of Computer Science and Technology Studies, 7(4), 757-771.
[52]. Obbu, S. (2025). AI in finance: Transforming risk management and fraud detection. World Journal of Advanced Engineering Technology and Sciences, 15(1), 747-756.
[53]. Murugan, P. S. B., Satish, R., Paranthaman, P., & Muzhumathi, R. (2024, December). AI-Powered Data-Driven Approaches to Fraud Detection in Finance. In 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-7). IEEE.
[54]. Ikumapayi, O. J., & Ayankoya, B. B. (2025). AI-powered forensic accounting: Leveraging machine learning for real-time fraud detection and prevention. International Journal of Research Publication and Reviews, 6(2), 236-250.
[55]. Nandola, R. J., Kasar, P. P., Al-Mattarneh, H., Raje, H., Mathkoor, M. M., & Mudhafar, M. (2025, December). Advancing Fraud Detection in Financial Transactions Through AI: Emerging Challenges and Strategic Opportunities. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-6). IEEE.
[56]. Ahmed, A., Shah, A., Ahmed, T., Yasin, S., Longa, F. E. A., Hussaini, W., & Zubair, M. (2025). AI-Driven Innovations in Modern Banking: From Secure Digital Transactions to Risk Management, Compliance Frameworks, and AI-Based ATM Forecasting Systems. Journal of Management Science Research Review, 4(3), 1145-1183.
[57]. Yadavalli, R., Polisetti, R., & Kurada, R. R. (2025, January). Analysis on AI-based Techniques for Detection of Banking Frauds: Recent Trends, Challenges, and Future Directions. In 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-8). IEEE.

[58]. Ghosh, S. (2025). A novel framework for financial cybersecurity and fraud detection using XAI-RNN-SGRU. IEEE Access.
[59]. Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. Journal of Risk and Financial Management, 18(4), 179.
[60]. Panem, C., Tripathi, A. M., Chaudhary, N. K., Chouhan, L., Kori, S. A., Rao, G. S., & Srivastava, A. M. (2024, October). Leveraging Machine Learning and AI for Real-Time Anomaly Detection in Financial Transactions. In International Conference on Information Security, Privacy and Digital Forensics (pp. 1-17). Singapore: Springer Nature Singapore.
[61]. Dataset Link:
https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023