International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

AI-Based Fraud Detection System

Shreya Nehe

Bharti Vidhyapeeth College

ABSTRACT

Fraud detection in financial transactions is a critical challenge due to the increasing volume and sophistication of fraudulent activities. Traditional rule-based methods often fall short in accurately identifying fraud, particularly in highly imbalanced datasets where legitimate transactions vastly outnumber fraudulent ones. This research presents the use of machine learning algorithms to enhance accuracy and efficiency in fraud detection. The work follows a robust and well-defined method of data collection followed by processing, which included cleaning, normalizing and balancing the dataset, followed by exploratory analysis so that the data would be ready for modeling. Many models were produced using numerous machine learning algorithms - decision trees, support vector machines, k-Nearest Neighbors, etc - and each of the models were tested against performance metrics of accuracy, precision, recall, F1, and AUC. Overall, the research demonstrated that many models were available identify legitimate transactions with high accuracy, but there were challenges in identifying the rare fraud events on any particular model due largely to class imbalance. By using techniques such as undersampling and hyperparameter tuning the researchers were able to improve the model's overall sensitivity to detect fraud without dramatically increasing false positives. The study also highlighted the importance of model interpretability and scalability ensuing that case for moving to ensemble methods, and explainable AI techniques in future work. In summary, even though the study was targeted towards making use of machine learning models for detecting and preventing fraudulent actions, the study showed that, with a consistently reliable fraud detection and prevention ecosystem at play, machine learning model driven fraud prevention systems lead themselves to consumer protection, preventing organizations from losing money at the hands of organized crime. Research and practice engaged with the implementations of fraud detection and prevention inks materially to use reasonable information without never ending studies that create reasons for learning using irrelevant data points. This current research makes two important contributions to practice: It offers a simple and user friendly gradient with immediate impact of human e f fort on developing dynamic systems capable of protecting customers online and consequently guarding businesses' financial assets from losses. Protecting people from losing money is essential now and as online fraud continues to grow in scale. This study assists by providing insight as to how AI technology can be utilized practically in accommodating and developing real-time monitoring, reliable accurate and transparent fraud detection systems that use existing databases as a foundation for deploying. As global governance and financial sectors engage with addressing fraud as phenomenon marked by continual variability, every anti-fraud model, whether human or algorithmic relies on information for identifying and reporting. Identifying informative anti-fraud algorithms that resist the emergent nature of evolving fraud behaviours increases the admonishment of coherent localization of information, more so, detecting various changes is enhanced.

Keywords: Fraud Detection, Machine Learning, Class Imbalance, Anomaly Detection, Financial Security

1. INTRODUCTION

1.1 Introduction

With the development of the digital economy and the rapid increase in online purchases, online transactions, and the fintech sector in general, fraudulent activity has skyrocketed. Fraud detection systems typically incorporate traditional, rule-based techniques that fall short for the majority of the patterns fraudsters deploy. Artificial Intelligence (AI) and Machine Learning (ML) have enabled projects to implement fraud detection systems that are stronger, more adaptive and accurate than ever. An AI-Based Fraud Detection System makes contributions because it uses algorithms in a machine learning context to help analyze data. In addition, in real time, these systems can help detect anomalies, identify suspicious behaviours and limit losses. These systems learn from historical data, become increasingly modified to combat new strategies of fraud and improve upon their detection strengths.

Java is a well-suited programming language for such systems due to its platform independence, highly scalable and the large Java community support available today. Native integration in Java, along with many machine learning libraries and APIs available will allow developers to both develop and deploy a fraud system within an enterprise. This project aims to design and implement a fraud detection system that incorporates the advantages of OpenAI with the capabilities of machine learning into a single framework. The fraud detection system will automatically detect and tag possible fraudulent transactions to provide a safeguard against fraud before manual interaction occurs, reducing risk, loss, and increase security in the digital financial systems. The system is built utilizing supervised learning and unsupervised, to provide a "for profit" fraud prevention system that is automatically responsive while adapting to new threats.

1.2 Fraud Detection Algorithms Using Machine Learning

For years, fraud has been a major issue in sectors like banking, medical, insurance, and many others. Due to the increase in online transactions through different payment options, such as credit/debit cards, Ponape, Gay, Paytm, etc., fraudulent activities have also increased. Moreover, fraudsters or criminals have become very skilled in finding escapes so that they can loot more. Since no system is perfect and there is always a loophole them, it has become a challenging task to make a secure system for authentication and preventing customers from fraud. So, Fraud detection algorithms are very useful for preventing frauds.

Here comes Machine Learning which can be used for creating a fraud detection algorithm that helps in solving these real-world problems.

- Email Phishing
- Payment Fraud
- ID Document Forgery
- Identity Theft

Email Phishing

This is a fraud or cybercrime wherein attackers send fake sites and messages to users via email. These emails are seemingly legit and authentic that anyone can misjudge them and enter the vulnerable data that puts them at risk. The best way to prevent email phishing is to avoid entering vulnerable data in these

emails until you verify their credentials. And the best way is to ignore these emails or messages that flash on your screen. Traditional methods for phishing involve the use of filters. These filters are primarily of two types, authentication protection, and network-level protection. Authentication protection is through email verification. Network-level protection is through three filters; whitelist, blacklist, and pattern matching. Now all these methods are automated through classical Machine Learning algorithms for classification and regression.

Payment Fraud

These types of fraud are very common in today's card systems for banking. Fraudsters can steal cards, make counterfeit cards, steal Card ID, etc. Once they steal the confidential data of a user, they can buy things, apply for a loan, and pretty much anything they imagine.

ID Document Forgery

Nowadays these criminals and fraudsters can buy ID proof of a person and use that to enter a system, make use of it, and without any impact get out if it. This type of fraud can put many organizations at risk as these fraudsters can get access to their systems by faking an ID Document and cheating them. These fraudsters are skillful in creating more legit IDs. So old systems which are used to prevent Identity forging are no more capable to detect these forgeries as these patterns need continuous updating. Machine Learning algorithms are the best tool which evolves with more dataset and shows consistent higher detection rates with time.

Identity Theft

Attackers or cybercriminals can hack into their victims accounts and gain access to their credentials like, name, bank account details, email address, passwords, etc. They can use these credentials to cause harm to their victim. There are three types of identity theft: real name theft, account takeover, and synthetic theft.

Manual Review and Transaction Rules

Nowadays, Machine Learning in Artificial Intelligence resolves most of the issues that human beings find difficult to deal with. Previously, industries were using a rule-based approach for fraud detection. But due to the popularity and acceptance of A.I, especially by students and Machine Learning in every industry vertical, organizations have moved from the ruled-based fraud detection to ML-based solutions.

1.3 Rule-based Approach or Traditional Approach in Fraud Detection Algorithms

In the rule-based approach, fraud analysts write the algorithms. They are based on strict rules. If any changes have to be made for detecting a new fraud, then they are done manually either by making those changes in the already existing algorithms or by creating new algorithms. In this approach, with the increase in the number of customers and the data, human effort also increases. So, the rule-based approach is time-consuming and costly. Another drawback of this approach is that it is more likely to have false positives. This is an error condition where an output of a test specifies the existence of a particular condition that does not even exist. The output of a transaction depends upon the rules and guidelines made for training the algorithm for non-fraudulent transactions. So, for a fixed risk threshold, if a transaction is

rejected where it should not be, it will generate a condition of high rates of false positives. This false-positive condition will result in losing genuine customers.

1.3.1 ML-based Fraud Detection Algorithms

In the rule-based approach, the algorithms cannot recognize the hidden patterns. Since they are based on strict rules, they cannot predict fraud by going beyond these rules. But in real world, fraudsters are very skilled and can adopt new techniques every time to commit a crime. Therefore, there is a need for a system that can analyze patterns in data and predict and respond to new situations for which it is not trained or explicitly programmed.

Hence, we use Machine Learning for detecting fraud. Here, a machine tries to learn by itself and becomes better by experience. Also, it is an efficient way of detecting fraud because of its fast computing. It does not even require the guidance of a fraud analyst. It helps in reducing false positives for transactions as the patterns are detected by an automated system for streaming transactions that are in huge volume.

1. Supervised Learning Used in Fraud Detection Algorithms

Supervised Learning models are trained on tagged outputs. If a transaction occurs, it is tagged as either 'fraud' or 'non-fraud.' Large amounts of such tagged data are fed into the supervised learning model in order to train it in such a way that it gives a valid output. Also, the accuracy of the model's output depends on how well-organized your data is.

2. Unsupervised Learning Used in Fraud Detection Algorithm

Unsupervised learning models are built to detect unusual behavior in transactions which is not detected previously. Unsupervised learning models involve self-learning that helps in finding hidden patterns in transactions. In this type, the model tries to learn by itself, analyzes the available data, and tries to find the similarities and dissimilarities between the occurrences of transactions. This helps in detecting fraudulent activities.

So, both these models, supervised and unsupervised, can be used independently or in combination for detecting anomalies in transactions.

1.3.2 Need for the Fraud Detection Machine Learning Algorithms

Human beings always search for methods, tools, or techniques that reduce the human effort for performing a certain task efficiently. In Machine Learning, algorithms are designed in such a way that they try to learn by themselves using past experience. After learning from the past experience, the algorithms become quite capable of reacting and responding to conditions for which they are not explicitly programmed. So, Machine Learning helps a lot when it comes to fraud detection. It tries to identify hidden patterns that help in detecting fraud which has not been previously recognized. Also, its computation is fast as compared to the traditional rule-based approaches.

1. Machine Learning in Fraud Detection

Here are some factors for why Machine Learning techniques are so popular and widely used in industries for detecting frauds:

- Speed: Machine Learning is widely used because of its fast computation. It analyzes and processes data and extracts new patterns from it within no time. For human beings to evaluate the data, it will take a lot of time and evaluation time will increase with the amount of data. Rule-based fraud prevention systems are based on written rules for permitting which type of actions are deemed safe and which one's must raise a flag of suspicion. Now, this Rule-based system is inefficient because it takes much time to write these rules for different scenarios. And that's exactly where Machine Learning based Fraud Detection algorithms succeed in not only learning from these patterns it is capable of detecting new patterns automatically. And it does all of this in a fraction of the time that these rule-based systems could achieve.
- Scalability: As more and more data is fed into the Machine Learning-based model, the model becomes more accurate and effective in prediction. Rule-based systems don't evolve by themselves as professionals who developed these systems must write these rules meeting various circumstances. But for Machine Learning based algorithms, a dedicated team of Data Science professionals must be involved in making sure these algorithms are performing as intended.
- Efficiency: Machine Learning algorithms perform the redundant task of data analysis and try to find hidden patterns repetitively. Their efficiency is better in giving results in comparison with manual efforts. It avoids the occurrence of false positives which counts for its efficiency. Due to their efficiency in detecting these patterns, the specialists in Fraud detection could now focus on more advanced and complex patterns, leaving the low or moderate level problems to these Machine Learning based algorithms.

2. Machine learning system work for Fraud Detection

The below picture shows the basic structure of the working of fraud detection algorithms using Machine Learning:

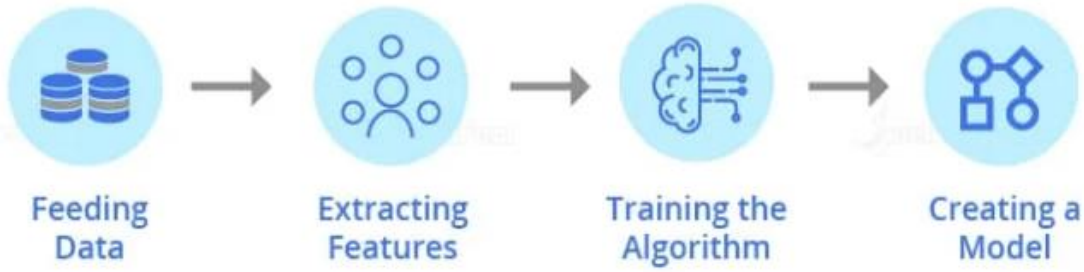

Figure 1.1: Workflow of ML Model Development for Fraud Detection

Feeding Data: First, the data is fed into the model. The accuracy of the model depends on the amount of data on which it is trained, more data better the model performs.

For detecting frauds specific to a particular business, you need to input more and more amounts of data into your model. This will train your model in such a way that it detects fraud activities specific to your business perfectly.

Extracting Features: Feature extraction basically works on extracting the information of each and every thread associated with a transaction process. These can be the location from where the transaction is made, the identity of the customer, the mode of payments, and the network used for transaction.

- Identity: This parameter is used to check a customer's email address, mobile number, etc. and it can check the credit score of the bank account if the customer applies for a loan.
- Location: It checks the IP address of the customer and the fraud rates at the customer's IP address and shipping address.
- Mode of Payment: It checks the cards used for the transaction, the name of the cardholder, cards from different countries, and the rates of fraud of the bank account used.
- Network: It checks for the number of mobile numbers and emails used within a network for the transaction.

Training the Algorithm: Once you have created a fraud detection algorithm, you need to train it by providing customers data so that the fraud detection algorithm learns how to distinguish between 'fraud' and 'genuine' transactions.

Creating a Model: Once you have trained your fraud detection algorithm on a specific dataset, you are ready with a model that works for detecting 'fraudulent' and 'non-fraudulent' transactions in your business.

The advantage of Machine Learning in fraud detection algorithms is that it keeps on improving as it is exposed to more data.

There are many techniques in Machine Learning used for fraud detection. Here, with the help of some use cases, we will understand how Machine Learning is used in fraud detection.

1.3.3 Techniques of Machine Learning for Fraud Detection Algorithms

1. Fraud Detection Machine Learning Algorithms Using Logistic Regression: Logistic Regression is a supervised learning technique that is used when the decision is categorical. It means that the result will be either 'fraud' or 'non-fraud' if a transaction occurs.

Use Case: Let us consider a scenario where a transaction occurs and we need to check whether it is a 'fraudulent' or 'non-fraudulent' transaction. There will be given set of parameters that are checked and, on the basis of the probability calculated, we will get the output as 'fraud' or 'non-fraud.'

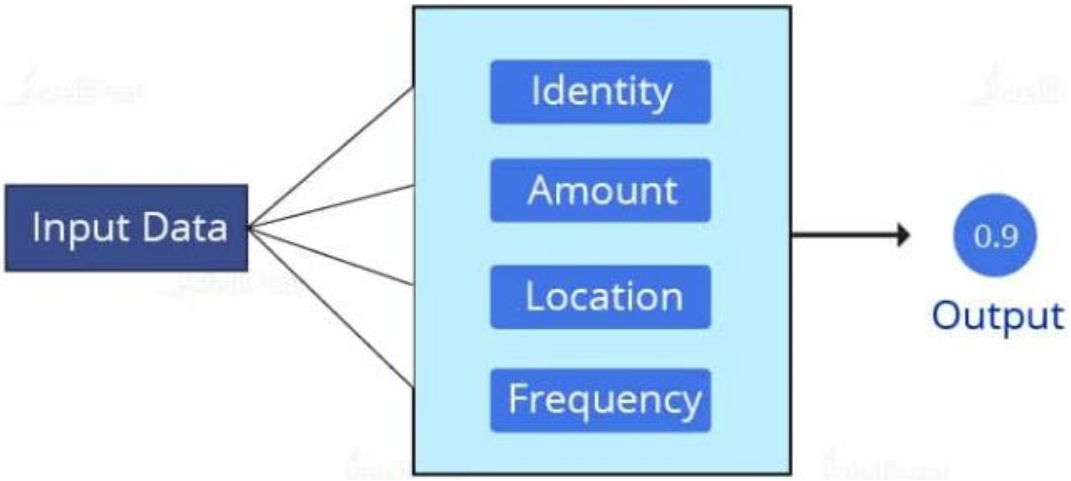

Figure 1.2: Feature Extraction and Prediction Process

Set of parameters for checking fraud

In the above diagram, we can see that the probability calculated is 0.9. This means that there is a 90 percent chance that the transaction is 'genuine' and there is a 10 percent probability that it is a 'fraud' transaction.

2. Fraud Detection Machine Learning Algorithms Using Decision Tree: Decision Tree algorithms in fraud detection are used where there is a need for the classification of unusual activities in a transaction from an authorized user. These algorithms consist of constraints that are trained on the dataset for classifying fraud transactions.

Use Case: Let us consider a scenario where a user makes transactions. We will build a decision tree to predict the probability of fraud based on the transaction made.

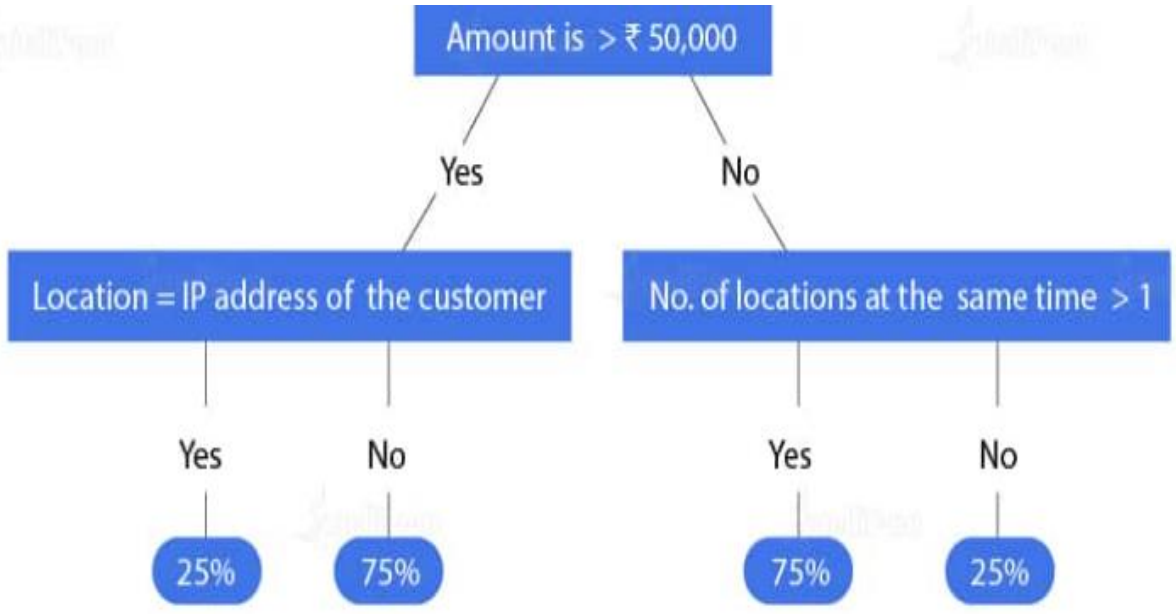

Figure 1.3: Decision Tree Logic for Identifying Fraudulent Transactions

First, in the decision tree, we will check whether the transaction is greater than ₹50,000. If it is 'yes,' then we will check the location where the transaction is made.

And if it is 'no', then we will check it for the frequency of the transaction.

Next, according to the probabilities calculated for these events, we will classify the transaction either as 'fraud' or 'non-fraud'.

At this point, if the amount exceeds ₹50,000 and location is equal to customer IP address, then we can say the likelihood of the transaction being 'fraud' is 25% and being 'no-fraud' is 75%.

Similarly, if the amount is more than ₹50,000 and number of locations is more than 1, then the likelihood of the case being 'fraud' is 75% while being 'no-fraud' is 25%.

This is how a decision tree in Machine Learning helps in the development of fraud detection algorithms.

Now we will look at the random forest in Machine Learning has been described in section x for use in fraud detection algorithms.

3. Using Random Forest Machine Learning Algorithms for Fraud Detection: Random Forest uses a mix of decision trees to increase the results. Each decision tree checks different conditions. Decision trees are trained on random datasets and based on the training of the decision trees, each tree provides the probability of the transaction being 'fraud' and 'non-fraud'. The model will predict the result accordingly.

Use Case: Let's assume that a transaction is made. We can now see how the random forest in Machine Learning is being used in fraud detection algorithms.

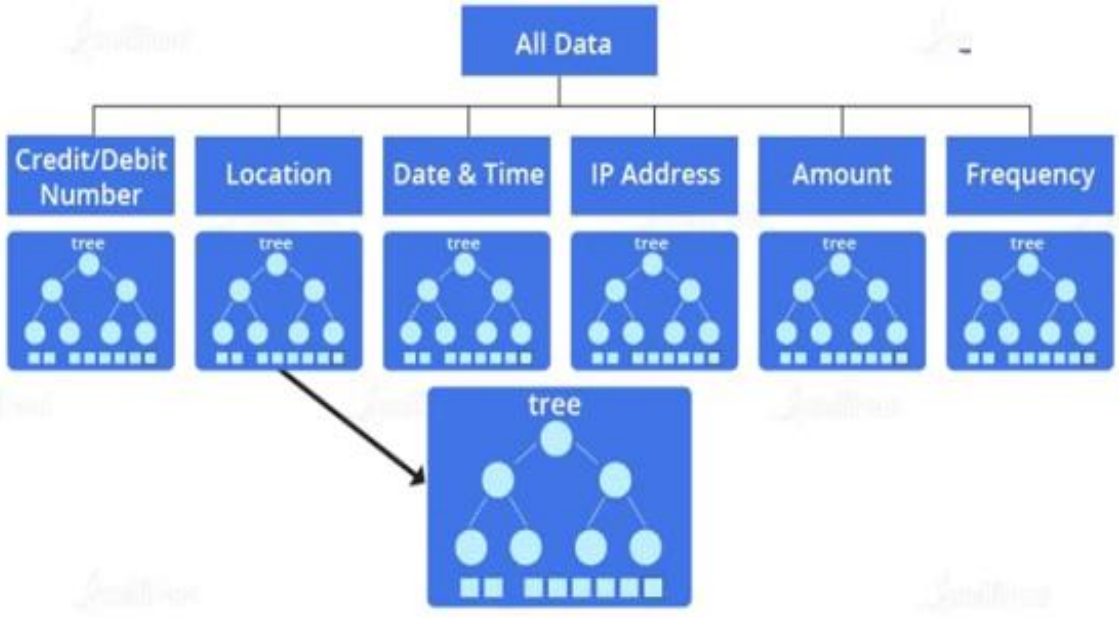

Figure 1.4: Random Forest Architecture for Fraud Detection Based on Multiple Features

When a request for a transaction is given to the model, it checks for the information like the credit/debit card number, location, date, time, the IP address, the amount, and the frequency of the transaction. All this dataset is fed as an input into the fraud detection algorithm. Then this fraud detection algorithm selects variables from the given dataset that help in splitting up of the dataset. The below diagram shows the splitting up of the dataset into multiple decision trees.

So, the sub-trees consist of variables and the conditions to check those variables for an authorized transaction.

After checking all the conditions, all the sub-trees will give the probabilities for a transaction to be 'fraud' and 'non-fraud.' Based on the combined result, the model will mark the transaction as 'fraud' or 'genuine.'

This is how a random forest in Machine Learning is used in fraud detection algorithms.

4. Fraud Detection Machine Learning Algorithms Using Neural Networks: Neural Networks is a concept inspired by the working of a human brain. Neural networks in Deep Learning uses different layers for computation. It uses cognitive computing that helps in building machines capable of using self-learning algorithms that involve the use of data mining, pattern recognition, and natural language processing. It is trained on a dataset passing it through different layers several times.

It gives more accurate results than other models as it uses cognitive computing and it learns from the patterns of authorized behavior and thus distinguishes between 'fraud' and 'genuine' transactions.

Use Case: Now, we will look at an example where a neural network is used for fraud detection. There are different layers in a neural network that focus on different parameters to make a decision whether a transaction is 'fraud' or 'non-fraud.' In the below diagram it is shown how the layers of neural networks represent and work on different parameters.

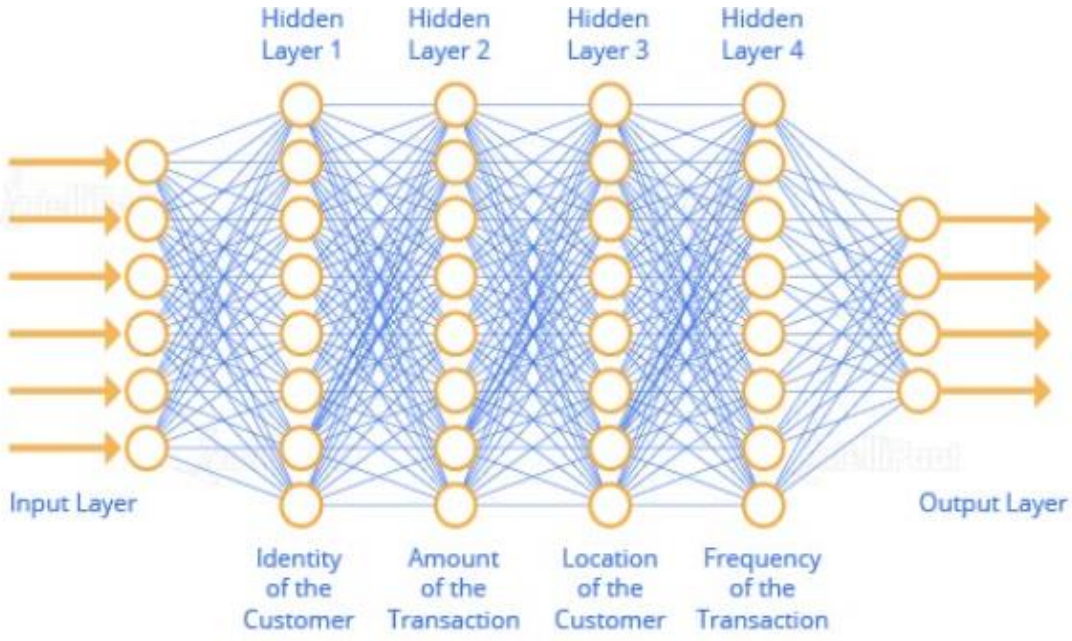

Figure 1.5: Deep Neural Network Architecture for Fraud Detection

First, the data is fed into the neural network. After that, the Hidden Layer 1 checks the amount of transaction, and similarly other layers check for the location, identity, IP address of the location, the frequency of transaction, and the mode of payment. There can be more business-specific parameters. These individual layers work on these parameters, and computation is done based on the models' self-learning and past experience to calculate the probabilities for detecting frauds.

Thus, neural networks work on data and learn from it, and it improves the model's performance over every iteration.

1.4 Enhancing Fraud Detection with Pre-processed Data Segments

""Enhancing Fraud Detection with Pre-processed Data Segments" is an essential piece within a fraud detection system that enhances the accuracy and efficiency of fraud detection processes. In this module, pre-processed data segments will be applied to bolster the user's fraud detection capabilities. Here is a brief summary of this module. The "Enhancing Fraud Detection with Pre-processed Data Segments" module is an important piece within a robust fraud detection system designed to enhance the system's ability to be proactive in fraud detection and prevention. This module focuses on the role of data pre-processing and segmentation within the fraud detection pipeline. Data pre-processing is the act of cleansing, transforming, and structuring unprocessed data for the means of analysis, and in this module data will be interpreted through a number of operations and enhanced upon to provide it with greater value and quality as it pertains to fraud detection. Example techniques that might observe include: data normalization, outlier removal, and missing value handling. This allows for cleaner, more organized data which is necessary to create precise fraud detection models. Data segmentation results in segments or subsets of data. Each of the segments can characterize a particular aspect of the data such as transaction type, transaction location, user behavior, or other dimensions that are relevant. Segmentation enables the fraud detection system to analyze the diverse segmented data and focus on patterns of distinct types, allowing the fraud detection engine to more accurately draw attention to instances of fraud. The Enhancing Fraud Detection through Pre-processed Data Segments module uses the processed and segmented data components to create features, identify anomalies, and build predictive models. This subsequently allows the fraud detection system to detect unusual patterns, trends, and behaviors that are typically associated with fraud.

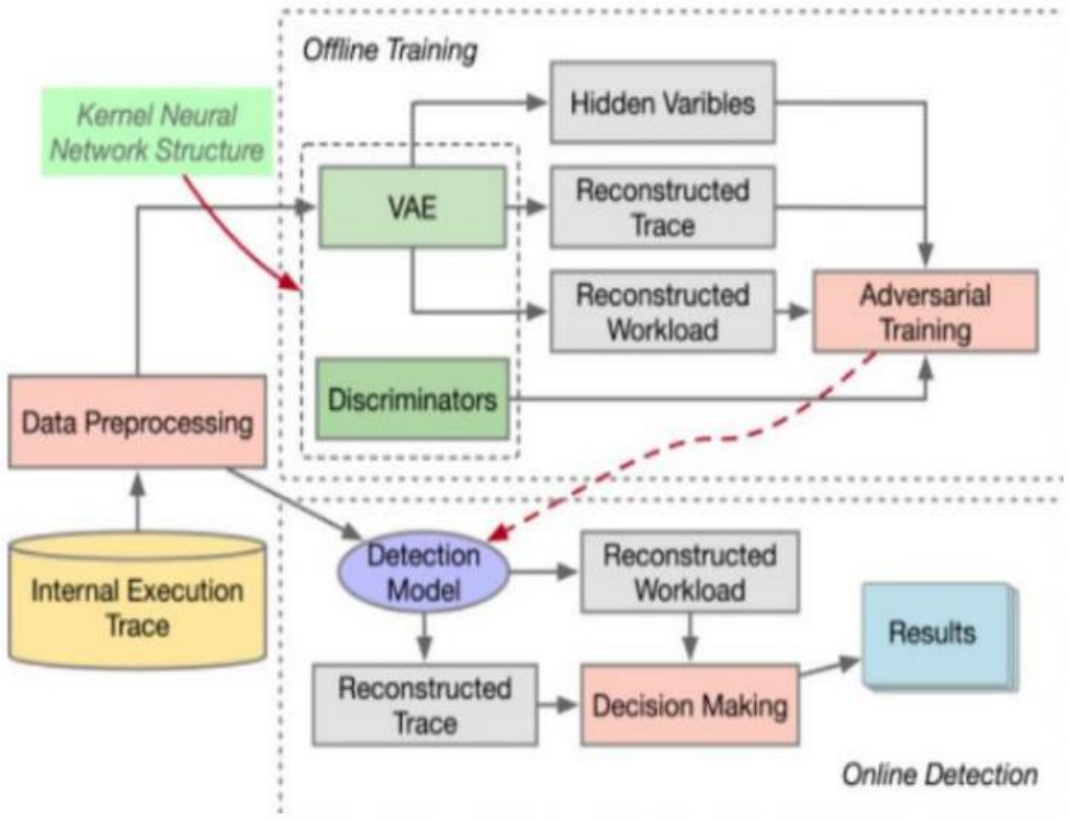

Figure 1.6: Enhancing Fraud Detection with Preprocessed Data Segments

Figure 1.6 demonstrates Data Pre-processing for Fraud Detection is an important step to create a quality fraud detection system, and it includes cleaning, modifying, and organizing raw data into a suitable format for analyses. Here is a short overview that discusses the context of Data Pre-processing for Fraud detection, as well as its importance and process. Data Pre-processing for Fraud Detection is a fundamental part of a successful fraud prevention system. Data pre-processing involves a variety of techniques and operations that can be performed on raw data before being used for analyses. Overall, the objective is to improve data quality, data consistency, and data relevance, so the fraud detection model can make reliable, accurate, and justified predictions. Data Cleansing: Most raw data will contain errors, missing values, outliers, and inconsistencies. Data cleansing aims at finding where the missing values are and correcting the outliers to finalize a clean data set. The missing values are filled in, the outliers are removed or adjusted, and any errors have been corrected. Data Reduction: If you are using a very large data set, then you may be using data reduction techniques such as, dimensionality reduction, to simplify the data without losing the information required to do fraud detection. This will help allow the fraud detection detection process to be as efficient as possible. Data Pre-processing for Fraud Detection is at the heart of the process as data is the raw material that defines the accuracy and performance of the fraud detection model. Accurate information and high-quality data pre-processing is critical to creating reliable predictive models, discovering anomalies, and making timely fraud decisions.

There are many great use cases where Java can help: Integration with Existing Systems: Java's reputation for being interoperable and being able to integrate with many databases/systems and APIs, means it is easily connected to transactional and data storage systems for financial and e-commerce applications,

which is very important because all data sources must be integrated to collect the necessary data for processing. High Performance Computing: Java is known for its efficient multi-threading and parallel processing capabilities that are often a minimum requirement to work with considerable amounts of real-time transactions and data in most fraud detection scenarios. Machine Learning Libraries: There are many available machine learning libraries and frameworks in Java (Weka, Deeplearning4j, Apache OpenNLP, etc.) that can be exploited to create AI models and predictive analytics that can be used in fraud detection systems. Scalability: Java applications are easily scalable to accommodate increased data volume and workloads, which can be critical for fraud detection systems as the business grows. Security: Java is designed with extensive security features to create strong fraud detection systems. It can help contain sensitive financial data and customer information to protect from cyber-attack threats, while ensuring integrity of the AI models. Real-time Processing: Fraud detection systems often require processing and decision-making in real time, which Java can accommodate with event-driven frameworks and stream-processing such as Apache Kafka or Apache Flink. Cross-Platform Compatibility: Java is platform independent, still allowing you to develop an AI that can run on different operating systems and environments, making it easier to deploy a fraud detection model to different systems and devices. Community and Ecosystem: Java has a large, active developer community, meaning that there are numerous libraries, resources, and tools that can help facilitate building AI and fraud detection solutions. Compliance and Regulations: Java has security controls, auditing capabilities and accepted best practices that can help ensure that fraud detection systems meet the strict regulations of the finance industry.

1.5 Advantages and Disadvantages of Fraud Detection Techniques

Fraud Detection Techniques comprise a collection of techniques and practices that are used by organizations in order to detect and prevent fraudulent activities. These techniques are important because they are crucial in preventing financial losses, protecting data, and protecting an organization's reputation. Here's a more in-depth explanation of these techniques: Fraud Detection Techniques are a collection of tools and methods that aim to detect and mitigate instances of fraud in many industries including but not limited to, finance, e-commerce, and healthcare. Fraud Detection Techniques help mitigate financial impacts of fraud, give assurance of data security, and maintain trust with customers and stakeholders. Rule-Based Systems: Rule-based systems require fraud detection methods to create pre-determined rules that generate an alarm or investigation if thresholds are breached. Rule-based techniques often require human input in the form of expertise or training, and in general, they are effective in responding to known patterns of fraud. They are limited in that they cannot detect fraud that occurs outside of existing patterns. As a result, these systems can produce false alarms when met with new or complex fraud patterns. Anomaly Detection: Anomaly detection techniques are used to identify deviations from established patterns. Anomaly detection techniques are useful because they are especially good at finding patterns of fraud that no one has witnessed before. They are best suited for early detection methods because they are performed proactively instead of reactively while adhering to existing fraud strategies. In addition to the pre-deployed programs that detect fraud, fraud detection techniques include some of the machine learning algorithms: Machine learning techniques leverage past data to develop predictive models capable of identifying subtle patterns and trends related to fraud. Fraud detection models can be continuously updated to adapt to changing fraud schemes. Deep Learning and Neural networks: Deep learning is one of the many methodologies in machine learning space, such as neural networks, which excel at modeling complex non-linear relationships in data. They can recognize complex patterns associated with fraud, as

well as enable image recognition and natural language processing for fraud detection. Biometrics and Authentication: biometric techniques like fingerprint or facial recognition can enhance security and identity ascertainment in many applications, especially with multi-factor authentication and verification of identity. Natural Language Processing (NLP): NLP techniques can analyze and interpret text data to uncover fraudulent activities in specific communications such as emails, chat logs or social media. These Fraud Detection Techniques can be utilized alone or in combination to meet specific organizational needs and help identify or mitigate the impacts of fraud. Because of the complexity of fraud, effective fraud detection usually includes a combination of a range of techniques to create a layered and multifactor and adaptable defense system against evolving fraud schemes and to protect financial transactions and sensitive information.

Table 1.1: Advantages and Disadvantages of Fraud Detection Techniques

Techniques	Advantages	Disadvantages
AVS	It is easy, fast, and one of the most management techniques the merchant can take. Reduce the risk of fraud.	It is not a perfect indicator of fraudulent Behaviour. AVS is ineffective for the soft product
CVV2	It reduces the cardholdernot-present fraud. It reduces the fraudulent chargeback.	The fraudster can hack into the online system and then get the CVV2. CVV2 is not useful in lost or stolen cards.
Manual Review	It is more efficient when it is used as an additional technique.	It is not an effective fraud prevention technique. It is very expensive and consumes a lot of time.
Negative and Positive list	A negative list is good for preventing repeat fraud. A positive list reduces the time taken to check the valid order.	The list cannot be used to prevent identity theft fraud. The list needs frequent updating.
Customer Authentication	The customer authentication technique is an excellent tool to prevent fraud. The chargeback liability in this technique will be against the customer.	Only the visa or Master card use this service. So, the merchant needs to use additional fraud prevention techniques
Biometrics	Very effective technique to authenticate a customer's authority.	Difficult to implement. Very expensive. Requires a lot of time.

1.6 Problem Statement

Credit card fraud is a considerable problem financially for organizations and individuals that causes billions of dollars in losses annually. Increasingly with the rise of eCommerce, detecting fraudulent methods is becoming a problem because fraudulent transactions are often black swans within a sea of transaction data. Fraud detection can be complicated by number of factors such as large scale of transaction information and complexity of information as a whole. Instead, fraud often occurs at low rates with respect to the overall transaction information. For most financial organizations, legitimate transactions can sometimes account for less than one percent of all transactions. High rates of class imbalance can in turn, lead to missed fraudulent activities and high ratio of false negatives. In view of the previously mentioned factors, machine learning can be a viable solution, as models can be trained in developing parameters from transaction data to find an oftentimes-unknown anomaly, which would indicate fraud. The immensity of the problem lies more so in trying to build a fraud detection system that can handle and work with an imbalanced data set, just as fiduciary databases do, with far more transactions than any member state crediter account. In the following material, I propose building an AI-based fraud detection system using numerous machine learning algorithms. The overall objective is to produce a model that reduces false negatives or missed fraud incidents, improve overall accuracy of fraud detection, and be applicable in real time. This ultimately results in a credible system for monitoring and fighting credit card fraud in an ever changing, rapid online environment.

1.7 Limitations of the Study

There are some limitations to this study. First, the data used is highly imbalanced, with fraudulent transactions representing less than 0.2% of the observations. It was attempted to use recall and F1-score to counter issues with class imbalance, however, it is still possible that because of the large class of legitimate transactions, our models were biased to predict the majority, creating concerns regarding generalizability in the real world in which fraud has the potential to be rare yet complex. Because of the multi-dimensionality and complexity of PCA (V1 to V28 represents anonymized features), the model cannot be represented in a user-friendly way that typically aids in model interpretability, such as the use of domain knowledge. The absence of domain features may have limited the model's use of expert knowledge in improving fraud prediction.

Moreover, while the study projected removal of old problems associated with machine learning algorithm, it did not consider more advanced algorithms such as Deep Learning or Ensemble Methods that could potentially had a better performance. The study specifically did not consider ways in which more advanced methods of handling class imbalance, such as oversampling or undersampling, could improve fraudulent transaction detection. The dataset only represented two days of data, thus limiting the model capture of long term or evolving patterns of fraud. Although computation time was considered, more complex models could provide better results but may also require more computations, which may create issues in a real-time fraudulent detection systems.

1.8 Aim and Objective

The goal is to create an AI-based real-time fraud detection system that can effectively detect anomalies in credit card transactions to reduce losses for the organization and enhance security using leading edge machine learning techniques.

1. Develop an AI system for real-time detection of fraudulent credit card transactions.

2. Identify transaction anomalies with high accuracy and minimal false positives.
3. Enable instant alerts to prevent unauthorized credit card usage.
4. Utilize machine learning models to adapt to evolving fraud patterns.

1.9 Scope of Study

This current study provides an outline for the development of an artificial intelligence-based fraud detection system using machine learning-based approaches to predict fraudulent transactions from financial data sources. The work encompasses transaction data collection, data preprocessing, data feature extraction, data model training, and data testing and performance evaluation. The study then uses transaction features such as customer identity, transaction amount, location, frequency of transactions, and IP address to train classification models using machine learning approaches. Some of the machine learning algorithm that are traditional approaches (such as a Support Vector Machine(SVM), Decision Tree, and Random Forest), and modern approaches, like for instance, have made use Deep Neural Networks (DNNs). This study evaluates these classification algorithms using accuracy, precision, recall, F1-score, Receiver Operating Characteristic curve (ROC), and the Area under Curve (AUC) criteria for determining fraud detection. The workflow includes data feeding, feature engineering, algorithm training and model deployment, presented in an architecture enabling properly functioning and appropriately-flying AI models achieving real-time fraud detection effective decision making and delay management. The study discusses difficulties as data imbalance, and the changing environment for future challenges and accusations of fraud. Evaluation of these algorithms were completed with static data sets. It would be interesting to explore a real-time fraud monitoring detective opportunity for future academic research and AI interest and would be a valuable link for future in-action developments. Overall, this study ultimately wishes to assist in improving reliability and efficiency from falsely accused instances of fraud detection systems, in practical applications by possible real-time systems, in their more reliable and practical glare.

1.10 Structure of the Report

Chapter 1: Introduction

This chapter introduces fraud detection while underlining the importance of machine learning algorithms in improving accuracy with respect to traditional rule-based systems. Within this chapter data prepossessing will be reviewed in addition to challenges including class imbalance, the scope of the study and the relevance to current times in terms of preventing financial crimes.

Chapter 2: Literature Review

A review of existing research in fraud detection that focuses on AI and machine learning techniques while addressing challenges like data imbalance and model explainability. The analysis observed several gaps including detecting fraud in real time, and integration with new technologies, and the lack of models that are both scalable and explainable.

Chapter 3: Methodology

A description of the full research process from data acquisition, cleaning, and scaling, exploratory data analysis (EDA), model development, tuning, training, and evaluation. It explains performance measurements including the confusion matrix and ROC-AUC curve which is used in determining the characteristics of the most effective fraud detection model.

Chapter 4: Result and Discussion

The results of the models were reported and included precision, recall, F1-score, and accuracy. Challenges the study faced including class imbalance, model overfitting, and increased false negatives were discussed with an overview of the practical implications based on the findings while providing recommendations for performance improvements to increase fraud detection efficiency.

Chapter 5: Conclusion and Future Scope

A summary of the findings from the research was provided, it was established that machine learning is a viable solution to detect fraud, while discussing the limitations of the study as well as future research direction including real-time detection systems, hierarchical model algorithms that include explainable AI and resolving ethical concerns to improve consumer trust and detection efficiency.

2. LITEARTURE REVIEW

2.1 Introduction

The emergence of digital payment systems has greatly raised the activity and complexity of credit card transactions, making detecting fraud an important hurdle that the financial industry faces globally. Traditional rule-based fraud detection approaches often fall short when it comes to dependent changing fraudulent behaviour and are slow to adapt, resulting in late detections and mostly false positives; thus, these approaches have paved the way for artificial intelligence (AI) and machine learning (ML) techniques that can analyze full-scale transaction data, recognize complex relationships, and identify anomalous transactions instantly. In fact, new studies show that AI models utilize methods such as decision trees, support vector machines, neural networks, and ensemble models to yield added effectiveness in accurately detecting fraud; as well as decreases in the cost of operational expenditures.

Additionally, real-time fraud detection systems utilize the predictive powers of AI to momentarily observe a stream of transaction data; enabling the real-time flagging of potentially superfluous transactions that warrant intervention. Hybrid models, a combination of both supervised and unsupervised strategies, have shown promise in maximizing detection accuracy while being able to incorporate new detection patterns of fraud. This literature review focusses on the honouring of specific methodologies that include AI technics, their advantages and disadvantages as well as their issues faced when undertaking credit card fraud detection. Understanding the current landscape informs the development of more robust, scalable, and efficient fraud detection frameworks capable of safeguarding financial transactions in increasingly complex digital environments.

2.2 Related Work

Eseoghene Kokogho et.al (2024)

In this review, we present a framework for cybersecurity capable of enhancing the activities of fraud detection in the finance systems using artificial intelligence (AI) with microservices and RESTful architecture. Financial institutions are increasingly the victim of more sophisticated cyber threats that traditional security measures cannot fully defend against. This review demonstrates how AI and microservices frameworks can be used to protect confidential or sensitive financial data and improve fraud detection. AI-driven models for real-time anomaly detection will allow the system to automate detection

on activities that appear suspect and social engineering is not used to predict which types of fraud are expected. Microservices architecture, which is typically based on Java Spring Boot, enables scalability, flexibility, and enhanced communication between modular components through secure RESTful APIs. Angular is utilized for building secure user interfaces, ensuring data protection across front-end applications.

Ahmed Al-Fatlawi et.al (2024)

Due to the very high direct or indirect costs of fraud, banks and financial institutions seek to accelerate the recognition of the activities of fraudsters. The reason for this is its direct effect on serving the customers of these institutions, reducing operating costs and remaining as a reliable and valid financial service provider. On the other hand, in recent years, with the development of information and communication technology, electronic banking has become very popular. In the meantime, it is inevitable to use fraud detection techniques to prevent fraudulent actions in banking systems, especially electronic banking systems. In this paper, a method has been developed that leads to the improvement of fraud detection in information security and cyber defense systems. The main purpose of fraud detection systems is to predict and detect false financial transactions and improve the intrusion detection system using information classification. In this regard, the genetic algorithm, which is known as one of the stochastic optimization methods, is used. At the end, the results of the genetic algorithm have been compared with the results of the decision tree classification and the regression tree. The simulation results show the effectiveness and superiority of the proposed method.

Md Zahidul Islam et.al (2023)

The rapid development of artificial intelligence (AI) has fundamentally changed the fraud detection environment of the U.S. financial system. The research reported in this study examined the application of AI driven techniques, particularly machine learning algorithms, to improve the efficiency and effectiveness of fraud detection systems. Traditional fraud detection systems have failed to continuously adapt to the changing patterns of fraud perpetrated by criminals, resulting in significant monetary losses, and resulting loss of trust in the consumer market. With the use of AI driven techniques, a financial institution can quickly analyze massive amounts of data in real-time to identify anomalous transactions and patterns indicative of fraud. This study examined a variety of AI techniques (including supervised learning, unsupervised learning, and deep learning) and their effectiveness, for the detection of fraud - as they apply across the various financial products and services. The findings from this research demonstrates that the use of AI driven techniques result in fewer false positives and improve detection rate vis-a-vis traditional systems. Additionally, using explainable artificial intelligence techniques enhances trust in the detection process providing transparency and accountability for stakeholders to understand and provide rationale for decisions made by the algorithms. This study has contributed to a better understanding of the potential for future use of AI in traditional financial system, particularly in improving the ability to detect fraud, which will contribute to increase security measures resulting in higher consumer confidence in a wholesome financial ecosystem.

Pankaj Gupta et.al (2024)

This project explores the relationships between Data Analytics, Artificial Intelligence and other emerging technologies in order to better understand the prevention of fraud. It also explores the benefits of using

machine learning and data analytics in artificial intelligence systems for fraud detection and prevention across industries. I performed an extensive review of available literature and analysed several case studies to find information related to the implications of artificial intelligence, data and analytics for fraud prevention. The research undertakes defined an international scope by utilising a wide range of academic, private and governmental sources. This project reviews publications; from developments between 2019 and 2023.

Georgi Cholakov et.al (2024)

The research aims to improve the functions offered by the FraudDetector software agent in the Distributed eLearning Center (DeLC). DeLC is a massive platform that offers extensive support for e-learning activities by helping the student/teacher to organize learning materials and learning gaps, it allows to conduct exams and supports a personalized elearning. The range of the project has several extensions, including one that is agent-oriented that enhances functions of reactive and pro-active intelligent part, called agents or assistants. This paper discusses the recent development of the software agent Fraud Detector, this means moving forward from base functionality, for fraud detection to the application of artificial intelligence (AI) into the mix. Specifically, it is the successful integration of AI (the knowledgebase ChatGPT), that enhances the effectiveness of Fraud Detector. Integration of ChatGPT is the primary research contribution to offer an improvement to fraud detection. The experimentation has shown promising use of ChatGPT, leading to the conclusion that using ChatGPT enhances the agent's function and precision. Moving forward, the agent architecture should remain open to collaborating with AI providers external to the location and effort should be made to decouple components responsible for integrating with AI. The application for these findings will have to wait for real-world production environment, which still requires validation.

Satwinder Singh et.al (2024)

The field of financial risk management is undergoing a significant transformation due to the advancements in artificial intelligence (AI) and the underlying machine learning (ML) techniques that provide the foundation of AI. These developments hold the potential to revolutionize the way the user’s approach and address financial risk. The expansion of AI-driven solutions has opened up various opportunities for comprehending and managing risk. These opportunities encompass a wide range of activities, such as determining appropriate lending amounts for customers in banking, issuing warning signals to financial market traders regarding position risk, identifying instances of customer and insider fraud, enhancing compliance efforts, and mitigating model risk. The prime objective of this study is to investigate the application of AI and ML in the Financial Services industry, with a specific focus on Risk Management and Fraud Detection. This study presents an intelligent and distributed method for detecting Internet financial fraud using Big Data. The study uses the graph embedding algorithm Node2Vec to learn and encode the structural characteristics of the graph representing the financial network into low-dimensional vectors. This allows for the intelligent and efficient classification and prediction of data samples from a large dataset using a deep neural network. The results showed that the F1-Score testing results from the Node2Vec algorithm demonstrate results around 67.1% - 73.4%. The results from the Node2Vec algorithm were better than the other two compared algorithms while also demonstrating that the overall performance from Node2Vec has more stability and demonstrates better classification results.

Bhuman Vyas et.al (2023)

With the rise of digital technology, the financial and e-commerce industry is increasingly under assault from fraudulent activity. Fraudsters are becoming more advanced and will require advanced means to battle this threat. This paper discusses a comprehensive look at Artificial Intelligence (AI) systems developed in Java specifically for fraud detection and prevention. For many years, Java has been the go-to option for developing scalable and reliable applications, while AI is changing the way organizations protect their monetary transactions. Organizations can develop intelligent systems that search massive sets of data for suspicious activity using Java and AI. In real time, organizations can now detect patterns of fraudulent behavior and quickly respond to stop unauthorized or fraudulent activity. This paper elaborates on the theory and practice of how AI, machine learning, and deep learning can be used in Java applications. We investigate building and deploying predictive models, anomaly detection, and behavioral analysis with Java libraries and tools. Additionally, we will discuss the challenges and considerations for implementing AI-enabled fraud detection solutions, such as data privacy, model accuracy, and scalability. When we finish this presentation, the audience will have a good understanding of how Java-based AI could be a game-changer in preventing fraud while simultaneously improving the safety and trust of financial and e-commerce platforms. This abstract has introduced the content of the paper, focused on related importance of Java and AI in fraud detection and prevention, and encouraged the audience to take an interest in knowing more about the subject.

Thaker Nay et.al (2024)

The recent rise in cyberattacks targeting critical infrastructure has spurred the development of network intrusion detection methods for the Internet of Things (IoT). Securing IoT networks is challenging given the vast number of connected devices, and the advanced techniques utilized by attackers. This research explores the use of machine learning and neural networks to mitigate common online fraud, and how well they work. The text also addresses concepts related to email filtering, machine learning, artificial neural networks and network intrusion methods. The research paper discusses the challenges of e-fraud detection and offers recommendations on ways to improve detection systems. In addition, the text provides a comprehensive review of IoT intrusion detection, focused on risks, vulnerabilities, attacks, and methods of detection. Maybe the hardest facet of securing the billions of stand-alone nodes which create the Internet of Things (IoT) is the unique capabilities of each. Traditional methods of securing domains (using functions such as encryption, access control, and authentication) are insufficient when deployed explicitly. Before approaching this work, deep learning techniques will identify the various IoT attack surfaces including Distributed Denial of Service (DDoS). The models are assessed using various datasets: NSL-KDD, DS2OS, and IoT Botnet. and evaluated using precision, recall, accuracy, and F1-score. The deep machine learning intrusion detection system shows a high accuracy percentage of 96.38%, indicating that it is effective in identifying the risks associated with the Internet of Things (IoT) where the data was trained on 80% and tested on 20%.

Olubusola Odeyemi et.al (2024)

examines the critical role of Artificial Intelligence (AI) in transforming fraud detection and prevention in the financial services industry. Financial crimes are complex and evolving, and traditional methods have proven to be insufficient to address these challenges without additional technology. Enter AI and machine

learning algorithms, predictive analytics, and anomaly detection that help develop protection against fraud. The review details the evolution and history of fraud detection, from manual detection to the new age of AI. It describes the range of AI models used for fraud prevention, including supervised learning, unsupervised learning, deep learning, and natural language processing. The detailed analysis concludes that AI, which focuses on an ability to understand complex patterns to identify fraud and is much better at identifying anomalies in very large and dynamic datasets. The review also shows the practical applications of AI in fraud detection, highlighting cases where technology successfully prevented fraud. The ethical implications of AI-based fraud prevention are also discussed, along with the ethical use of AI assists, such as responsible use, transparency, bias mitigation, and fairness. The review also brings potential future advancements in AI-based fraud detection to the forefront, as the financial sector reorganizes in digital form. Examples of future innovation include Explainable AI (XAI) and federated learning, as well as dynamic behavior based on new innovative modes of criminal methodology. The review also explores collaborative efforts between financial institutions, regulators, and technology providers to work together toward an ecosystem that can reduce the chances of the criminally manipulated information from being acted on by both financial institutions and financial consumers. The review provides a snapshot of a changing time for AI in fraud detection and prevention in financial services. As well it outlines the transformative potential of AI technology for increasing security and developing a proactive and resilient response to changing financial fraud systems. The future of fraud detection and prevention within the financial domain using AI technology has the distinct possibility of encompassing the last five thousand years of payment methods, current technologies, and future trajectories of the innovators in the relevant types of crime.

Bekim Fetaji et.al (2025)

Online financial fraud remains a pervasive threat, incurring billions of dollars in global losses annually. Mid-sized markets, such as North Macedonia, face acute challenges as digital adoption in the Banking, Financial Services, and Insurance (BFSI) sector outpaces the establishment of robust, multi-layered security systems. This paper introduces FRAUD-X, a unified framework merging artificial intelligence (AI)– based anomaly detection, blockchain-driven transaction verification, cybersecurity intrusion detection, and real-time early warning mechanisms into a single pipeline. Drawing upon three datasets—a Credit Card Fraud dataset (Kaggle), the PaySim Mobile Money dataset, and collected 50,000 anonymized local BFSI transactions from North Macedonia—FRAUD-X demonstrates a ~2–4% improvement in F1 compared to single-plane AI approaches, with ~90% recall for zero-day threats. Key enhancements include: 1) a permissioned blockchain for tamper-proof ledger entries, 2) synergistic AI–cybersecurity integration for dynamic risk scoring, and 3) real-time alerts that reduce reaction windows from hours to mere minutes. The framework runs at ~15–16 ms per transaction (~33% CPU usage), supporting near-real-time BFSI operations. Ablation studies confirm that each synergy layer (blockchain, cybersecurity, and early warning) significantly contributes to overall performance. A security analysis illustrates how FRAUD-X mitigates node compromise, collusion attempts, and advanced persistent threats (APT). By providing a replicable roadmap that balances high detection accuracy with operational feasibility, FRAUD-X offers practical value to BFSI entities in North Macedonia and comparable mid-scale markets.

Devendra Singh Parmar et.al (2024)

Complex digital payment systems make them more prone to fraud, raising the need for advanced fraud detection solutions. Since rule-based systems cannot keep up with fraudsters' ever-changing schemes, AI is needed to prevent fraud. This research examines how AI could be used to detect fraud in future payment processing systems to improve efficiency, accuracy, and security. AI models can evaluate enormous information in real time using deep learning, decision trees, and neural networks to detect fraudulent activities that people neglect. The study uses mixed methods to combine quantitative model performance indicators (F1 score, recall, accuracy, and precision) with qualitative financial case study findings. Deep learning models use more system resources, but our research demonstrates that they identify fraud more accurately and recall than decision trees. Results show that AI models dramatically reduce false positives, which benefits customers and businesses. AI in payment systems reduces fraud losses and speeds up transaction processing, providing financial benefits. However, ethical challenges including algorithmic bias and lack of transparency in AI decision-making still prevent AI acceptance. These challenges must be overcome for financial services companies to deploy AI-driven fraud detection systems. The report shows how AI can revolutionise payment system fraud detection and discusses AI implementation pros and cons. As efficiency and security remain priority, AI will determine how financial institutions detect fraud in the future.

Oluwabusayo Adijat Bello et.al (2023)

explores the impact of advanced analytics on fraud detection, emphasizing the role of machine learning (ML) in enhancing the accuracy and efficiency of identifying fraudulent activities. Advanced analytics, such as big data technologies, predictive analytics, and ML algorithms, have changed the fraud detection landscape, compared to traditional approaches. Traditional fraud detection systems followed rules and were black boxes upon which fraud detection systems relied upon years of historical data and accumulated fraud sightings in order to create a set of rules that governed future detection. Unlike rule-based systems, ML models have the potential to analyze immense quantities of data to identify complex patterns and develop adaptability to new fraud methods and tactics in real-time. This flexibility is important in the modern age, where fraud perpetrators constantly change their strategies to counter normal fraud detection systems. Implementing ML in fraud detection generally includes deploying supervised and unsupervised and semi-supervised learning. A supervised learning model utilizes labeled datasets, such as decision trees and neural networks, including the learning from historical data for fraud in order to learn what fraud looks like and predict instances of similar future occurrences. Unsupervised learning applies techniques such as clustering and anomaly detection, that explore transaction data to discover unusual patterns or deviations in behaviour without prior knowledge of fraudulent events. Semi-supervised learning uses a barbell approach: a small set of labeled known data is used in tandem with large amounts of unknown data to improve detection. There are many case studies available showing the value of ML in fraud detection. For example, institutions that have put ML into practice (or used an ML-based fraud detection system) report lower numbers of false positives and increased detection rates while simultaneously saving money and improving security.

Lawrence Emma et.al (2024)

As cyber fraud becomes more sophisticated, it demands an equally robust, scalable, intelligent, and detection mechanism; this is especially important in the not-so-simple and dynamic cloud computing environment. This applied research considers the design and deployment of scalable microservices architecture for AI-based fraud detection systems running within cloud settings through containerization of microservices, orchestration (Kubernetes) of microservices, and serverless computing. This research discusses and provides architectural patterns that support high availability, fault tolerance, and horizontal scaling. AI detection capabilities are particularly enhanced through modular decomposition of services and real-time streaming data pipelines that can support cloud architectures. Emphasis is placed on low-latency detection, data security, and agility in addressing new forms of fraud. The research findings will contribute a robust framework through which cloud-native fraud detection solutions that implement attractive and fast detection becomes a norm through resiliency and efficiency in aligning with cloud-native concepts and DevSecOps best practices.

Dilip Kumar et.al (2025)

As online financial transactions grow rapidly, the need to detect fraud is growing fast. This research investigates the use of scalable AI technologies for functionality within fraud detection that does not diminish user experience. With real-time monitoring, intelligent alert systems, and machine learning, platforms can detect anomalous user behaviors while impacting the user experience as little as feasible. The study stresses the importance of balancing strong security with usability for fraud detection and alert systems so there is no degradation in the transaction speed or overall transaction satisfaction. The paper also identifies specific challenges including consumer alert fatigue, user alert integration complexity, and privacy concerns, with potential opportunities including adaptive learning models, blockchain, and collaboration with trusted cybersecurity or fraud prevention personnel. The findings indicate that fraud detection frameworks must be both scalable and responsive to evolving threats, without curbing the user experience.

Maloy Jyoti Goswami et.al (2024)

In light of the fast-paced advancement in the cybersecurity field, traditional threat detection methods have become increasingly ineffective against advanced cyber threats. AI-based anomaly detection solutions are relatively new approaches to addressing the real-time cybersecurity challenges that organizations can face by identifying anomalies caused by an attack, network compromise, or breach. By using machine learning algorithms, anomalies can be detected in network traffic, system operations, etc., which allows for the potential of detecting and addressing new, subtle, and other unknown threats that earlier perimeter and signature-based systems may not have been effective against. This paper examines how AI-based anomaly detection systems can be implemented, with a focus on the architecture, algorithms, and effectiveness. The key aspects discussed are data preprocessing, feature extraction, and machine learning techniques such as neural networks, support vector machines, and various clustering algorithms. Incorporation of real-time data streams, and employing unsupervised learning techniques, will allow fast detection of Zero-day attacks or insider threats even when organizations have no knowledge of specific attack signatures. The overarching advantages and disadvantages of AI-based anomaly detection in cybersecurity have been extensively reviewed. The case studies and experimental results have shown that not only does AI-

supported anomaly detection allow for the detection of anomalies with high precision and recall, the work we've reviewed has fallen, on average, to one-third of established traditional false positive rates. At the same time, issues such as needing large datasets, computational overhead concerns, and risks of adversarial attacks are discussed here and could be reduced or entirely removed by using several AV and mitigation strategies we and others have previously set forth. Finally, the future trends and potential trajectories of AI-based anomaly detection in cybersecurity are discussed. This work proposes that AI will be incorporated with other emerging technologies (e.g., blockchain and quantum computing), advancing cybersecurity that is even more robust than before. The pace of emerging and established cyber threats is unstoppable, and this research helps to emphasize the vital need for greater and better AI-based adaptive, scalable, and intelligent cybersecurity solutions.

Saida Hafsa Rafique et.al (2024)

The Internet of Things (IoT) has created more connectivity and data than ever before, and rapidly increasing. Anomaly detection is one security feature that can identify instances where the actual behavior of a system deviates from normal expectations and enable the quick identification and remediation of those anomalies. The incorporation of AI into the IoT can improve anomaly detection processes, and ultimately, are more trustworthy, and effective and reliable than IoT systems without AI. AI-enabled anomaly detection systems in an IoT environment can identify a whole range of threat levels and attack vectors, including brute force, buffer overflow, injection, replay attacks, DDos attack, SQL injection, and back-door attacks or exploits. Intelligent Intrusion Detection Systems (IDSs) are imperative in IoT devices, which help detect anomalies or intrusions in a network, as the IoT is increasingly employed in several industries but possesses a large attack surface which presents more entry points for attackers. This study reviews the literature on anomaly detection in IoT infrastructure using machine learning and deep learning. This paper discusses the challenges in detecting intrusions and anomalies in IoT systems, highlighting the increasing number of attacks. It reviews recent work on machine learning and deep-learning anomaly detection schemes for IoT networks, summarizing the available literature. From this survey, it is concluded that further development of current systems is needed by using varied datasets, real-time testing, and making the systems scalable.

Muntasir Hoq et.al (2024)

The emergence of publicly accessible large language models (LLMs) such as ChatGPT poses unprecedented risks of new types of plagiarism and cheating where students use LLMs to solve exercises for them. Detecting this behavior will be a necessary component in introductory computer science (CS1) courses, and educators should be well-equipped with detection tools when the need arises. However, ChatGPT generates code non-deterministically, and thus, traditional similarity detectors might not suffice to detect AI-created code. In this work, we explore the affordances of Machine Learning (ML) models for the detection task. We used an openly available dataset of student programs for CS1 assignments and had ChatGPT generate code for the same assignments, and then evaluated the performance of both traditional machine learning models and Abstract Syntax Tree-based (AST-based) deep learning models in detecting ChatGPT code from student code submissions. Our results suggest that both traditional machine learning models and AST-based deep learning models are effective in identifying ChatGPT-generated code with accuracy above 90%. Since the use of such models requires ML expertise, and resources that may not be available to instructors, we also examine the signatures detected by deep learning models that could signal

possible ChatGPT code signatures that could be manually used by instructors to detect LLM-based cheating. We also examine whether there is a difference in code produced when explicitly requesting ChatGPT to impersonate a novice programmer. Additionally, we discuss the possible uses of our proposed models for better supporting introductory computer science instruction.

Chiamaka Daniella Okenwa et.al (2024)

The incorporation of explainable Artificial Intelligence (XAI) algorithms into compliance frameworks will greatly enhance our ability to continue fraud prevention processes in various fields. This article investigates the potential of explainable AI in compliance frameworks as it relates to fraud prevention. For example, in highly regulated fields such as finance, health, and cyber security, XAI can be applied for the identification of deviant behaviour and in demonstrating regulatory compliance by providing a degree of transparency and understanding into the decision making processes of the AI. The results indicates that there is an extent to which explainable AI improves the effectiveness, transparency, and interpretability of fraud prevention initiatives. Using the XAI techniques, stakeholders can understand how the AI has made decisions, identify evidence of deviancy, and rank the risk mitigation strategies. Furthermore, the paper indicates that interdisciplinary collaboration is essential in developing explainable AI and embed it within compliance frameworks for fraud prevention across different fields. Overall, XAI in compliance models offers considerable capabilities to support fraud prevention initiatives. Therefore, through the utilization of transparent and interpretable AI tools, entities can strengthen their ability to withstand fraudulent operations, build trust among stakeholders, and maintain principles within evolving regulatory systems.

Mohd Izhan Mohd Yusoff et.al (2024)

Machine learning is an Artificial Intelligence (or AI) application, an idea that came into being by giving machines access to data and letting them learn by themselves. AI has been making headlines, especially since ChatGPT was introduced. Malaysia has taken many significant steps to embrace and integrate the technology into various sectors. These include encouraging large companies to build AI infrastructure, creating AI training opportunities (for example, the local media reported Microsoft and Google plan to invest USD 2.2 billion and USD 2 billion, respectively, in the said activities), and, as part of AI Talent Roadmap 2024-2030, establishing AI faculty in one of its public universities (i.e., “Universiti Teknologi Malaysia”) leading the way in the integration and teaching of AI throughout the country. This article introduces several products developed by the author (for the energy and transportation industries) and recommends their improvement by incorporating Machine learning.

Marc Schmitt et.al (2023)

The last decades have been characterized by unprecedented technological advances, many of them powered by modern technologies such as Artificial Intelligence (AI) and Machine Learning (ML). The world has become more digitally connected than ever, but we face major challenges. One of the most significant is cybercrime, which has emerged as a global threat to governments, businesses, and civil societies. The pervasiveness of digital technologies combined with a constantly shifting technological foundation has created a complex and powerful playground for cybercriminals, which triggered a surge in demand for intelligent threat detection systems based on machine and deep learning. This paper investigates AI-based cyber threat detection to protect our modern digital ecosystems. The primary focus is on evaluating ML-based classifiers and ensembles for anomaly-based malware detection and network

intrusion detection and how to integrate those models in the context of network security, mobile security, and IoT security. The discussion highlights the challenges when deploying and integrating AI-enabled cybersecurity solutions into existing enterprise systems and IT infrastructures, including options to overcome those challenges. Finally, the paper provides future research directions to further increase the security and resilience of our modern digital industries, infrastructures, and ecosystems.

Shamshair Ali et.al (2022)

Many intrusion detection and prevention systems (IDPS) have been introduced to identify suspicious activities. However, since attackers are exploiting new vulnerabilities in systems and are employing more sophisticated advanced cyber-attacks, these zero-day attacks remain hidden from IDPS in most cases. These features have incentivized many researchers to propose different artificial intelligence-based techniques to prevent, detect, and respond to such advanced attacks. This has also created a new requirement for a comprehensive comparison of the existing schemes in several aspects; after a thorough study we found that there currently exists no detailed comparative analysis of artificial intelligence-based techniques published in the last five years. Therefore, there is a need for this kind of work to be published, as there are many comparative analyses in other fields of cyber security that are available for readers to review.In this paper, we provide a comprehensive review of the latest and most recent literature, which introduces well-known machine learning and deep learning algorithms and the challenges they face in detecting zero-day attacks. Following these qualitative analyses, we present the comparative evaluation results regarding the highest accuracy, precision, recall, and F1 score compared to different datasets.

Cut Susan Octiva et.al (2024)

The advancement of big data technology generated massive volumes of various types of data that led to concerns of anomaly detection that may interfere with decision-making. Thus, this study aims to establish the use of artificial intelligence (AI) for anomaly detection in big data systems to improve decision-making, thereby proving faster, more accurate, and efficient decision-making. The study is successful in finding techniques performed by machine learning algorithms, including classification-based detection methods, clustering, deep learning methods to identify abnormalities in data sets. The research method presented involved the use of the process of real-time dataset-based simulations by gauging the performance of multiple AI models using accuracy, precision, recall, and F1-score metrics. The results concluded that AI can substantially improve the detection of anomalies when compared to traditional methods of detection with an accuracy of an average of 92%.

Alexander Diadiushkin et.al (2019)

Financial industries are undergoing a digital transformation of their products, services, overall business models. Part of this digitalization in banking aims at automating most of the manual work in payment handling and integrating the workflows of involved service providers. The focus of the work presented in this paper is on fraud discovery and steps to fully automate it. Fraud discovery in financial transactions has become an important priority for banks. Fraud is increasing significantly with the expansion of modern technology and global communication, which results in substantial damages for the banks. Instant payment (IP) transactions cause new challenges for fraud detection due to the requirement of short processing time. The paper investigates the possibility to use artificial intelligence in IP fraud detection. The main contributions of our work are (a) an analysis of problem relevance from business and literature perspective,

(b) a proposal for technological support for using AI in fraud detection of instant payment transactions, and (c) a feasibility study of selected fraud detection approaches.

Ahmad Dinan Irsyadi et.al (2024)

This research focuses on the development and implementation of an Internet of Things (IoT)-based system for predicting tidal flood (banjir rob) using sensor data and machine learning techniques. The system utilizes sensors such as ultrasonic sensors (HC-SR04), DHT11 (for temperature and humidity), connected to an ESP32 module for real-time data collection. The collected data is sent to the ThingSpeak platform for storage and analysis. A machine learning model, specifically a Random Forest Regressor, is developed by training the model on historic data obtained from ThingSpeak and environmental factors such as temperature and humidity used to predict flood height. To make the model more practical, it is developed with an accompanying Telegram bot that sends the prediction to the users in real-time. The system gets the latest sensor data, predicts flood height, and sends that via the Telegram bot. The machine learning model is evaluated using metrics such as R2 score and Mean Squared Error (MSE) to predict flood height accurately and reliably. This model presents a fairly inexpensive, real-time, and scalable approach for predicting tidal floods in coastal regions. It is a great example of how the integration of IoT, cloud computing, and machine learning provides a substantial tool for local government authorities, disaster management teams, and the general public by providing real-time data to monitor and prepare potential floods. This research highlights the potential applicability of using IoT in conjunction with AI to enhance environmental monitoring and early warning systems in flood-prone regions.

Raihan Bin Mofidul et.al (2022)

presents an AI-enabled secured IIoT architecture with heterogeneous data collection and storage capability, global inter-communication, and a real-time anomaly detection model. Smart data acquisition devices are designed and developed through which energy data are forwarded to the edge IIoT servers. The servers implement hash encoding credentials and transport layer security (TLS) protocol. Additionally, the servers can exchange information via a secure message queuing telemetry transport (MQTT) protocol. Edge and cloud databases are utilized to address big data. For detecting the anomalies of individual electrical appliances in real-time, an algorithm based on a group of isolation forest models is developed and implemented on edge and cloud servers as well. In addition, remote-accessible online dashboards are implemented, enabling users to monitor the system. Overall, this study covers hardware design; the development of open-source IIoT servers and databases; the implementation of an interconnected global networking system; the deployment of edge and cloud artificial intelligence; and the development of real-time monitoring dashboards. Necessary performance results are measured, and they demonstrate elaborately investigating the feasibility of the proposed IIoT framework at the end.

Matija Cankar et.al (2023)

Security represents one of the crucial concerns when it comes to DevOps methodology-empowered software development and service delivery process. Considering the adoption of Infrastructure as Code (IaC), even minor flaws could potentially cause fatal consequences, especially in sensitive domains such as healthcare and maritime applications. However, most of the existing solutions tackle either Static Application Security Testing (SAST) or run-time behavior analysis distinctly. In this paper, we propose a) IaC Scan Runner, an open-source solution developed in Python for inspecting a variety of state-of-the-

art IaC languages in application design time and b) the run time anomaly detection tool called LOMOS. Both tools work in synergy and provide a valuable contribution to a DevSecOps tool set. The proposed approach is demonstrated and their results will be demonstrated on various case studies showcasing the capabilities of static analysis tool IaC Scan Runner combined with LOMOS – log analysis artificial intelligence-enabled framework.

Deepak Kaul et.al (2021)

APIs represent the foundation in every enterprise-class distributed system while enabling interaction, data exchange, or interoperability amongst diverse applications and services. However, ease of accessibility and their critical role make them vulnerable to security perils that could be disastrous in terms of integrity and performance of enterprise infrastructures if exploited. While encryption, multi-factor authentication, and rule-based anomaly detection are essential layers of security, their in-built limitations and lack of flexibility or adaptiveness place barriers on the prevention of sophisticated, evolving cyber threats. AI brings important improvements to the detection and mitigation of API vulnerabilities with real-time, data-driven security insights and adaptive responses. The paper addresses how to use AI in view of API security challenges on encryption, authentication, and anomaly detection. It investigates some AI approaches, including machine learning models that grade encryption strength, adaptive algorithms that measure consistency in authentication, and deep anomaly detection systems aimed at finding deviations in API traffic patterns. These AI-driven solutions support a multilayered security strategy that enhances more traditional approaches and facilitates a more responsive and robust security framework appropriate for the dynamic demands of large-scale distributed systems. While AI does not replace existing security practices, its deployment is a strategic enhancement, offering continuous and context-aware assessments that can help safeguard enterprise APIs against ever more sophisticated threats.

Research gap

Despite significant advancements in AI-driven fraud detection and cybersecurity, several research gaps remain unaddressed. First, while many studies demonstrate the effectiveness of individual AI techniques—such as machine learning, deep learning, and anomaly detection—in fraud identification, there is limited research on the seamless integration of these approaches within scalable, real-time, and distributed system architectures, especially for handling large-scale financial transactions with minimal latency. Secondly, class imbalance remains a persistent challenge in fraud datasets, yet current methods like under sampling or oversampling often lead to trade-offs between detection accuracy and false positive rates. More sophisticated, adaptive methods to balance sensitivity and specificity are needed. Third, while explainability of AI (XAI) is acknowledged as vital in the pursuit of transparency and regulatory compliance, holistic approaches that fuse high detection efficacy with interpretability are limited, inhibiting trust and uptake by stakeholders involved in vulnerable financial situations. Novel technologies like blockchain (BC) and the Internet of Things (IoT) also have prospective synergies with AI, underpinning fraud prevention capabilities, but comprehensive frameworks that are multi-layered and integrative in nature are largely unexplored. Further, ethical issues such as mitigation of bias and user privacy are inadequately considered or addressed in many AI fraud detection systems. Finally, there is a dearth of validation and deployment studies in the real world; most AI fraud detection research relies on benchmark datasets, especially within existing heterogeneous financial environments, rather than using

live datasets. Filling gaps on these areas would importantly contribute to the robustness, fairness and operational implementability of AI evidence-based fraud detection solutions in practice.

3. METHODOLOGY

3.1 Introduction

This chapter presents the process for developing an AI-based fraud detection system intended for identifying and preventing fraud in various sectors, such as finance, e-commerce, and healthcare. The goal is to use machine learning and artificial intelligence techniques for identifying suspicious patterns of behavior in vast amounts of data. These AI-based techniques will perform more accurately, in real-time, and at scale, than traditional, rule-based technologies. The process includes several steps: data collection, preprocessing, model selection, training, and finally evaluation. When developing an AI-based fraud detection system, first, historical data (transaction data, historical fraud data, user behaviour data, and any other relevant data) must be collected and preprocessed to ensure quality and consistency. After data preprocessing, a variety of machine learning models including decision trees, neural networks and ensemble methods, are trained to identify patterns of fraud based on labeled data. The model performance is evaluated using metrics to grade accuracy, precision, recall and F1 score. This methodology also leverages AI techniques guided by an evaluation framework, creating a system to adapt to ever-changing fraud tactics as well as build accuracy in fraud detection.

3.2. Data Acquisition

- The dataset leveraged for the purposes of this study is known as Credit Card Fraud Detection dataset and can be accessed by the public and compiled and hosted on the Kaggle platform. The dataset contains transaction data from cardholders across Europe over a two day time frame from September 2013. In total, there are 284,808 transactions, each with 31 features about the transaction. These features allow for the development of a model that will help identify fraudulent activities in terms of the transactions. The primary features in the dataset are:
- **V1 to V28:** These are 28 anonymized numerical features that were produced by Principal Component Analysis (PCA) to protect the identity of the cardholder. The V1 to V28 features, do not directly relate back to any specific transactional information or the identity of the cardholder which protects any confidential information and keep it secure. They represent a transformed and compressed version of the original features which will allow the machine learning model to identify very complex patterns without exposing any of this sensitive data.
- **Time:** This feature represents the number of seconds that have passed since this was the first transaction in the dataset. The Time variable is useful in that it provides a relative timestamp for each transaction, which can help explore transaction sequences and identify any outliers based on the distribution of the time of transactions.
- **Amount:** This attribute captures the value of each transaction. The very essence of this feature becomes crucial, especially since fraudulent transactions arise as anomalies involving amounts that consumers would not typically engage in; this is a critical clue for detecting fraud.
- **Class:** The target variable of the dataset where 1 is the signal for a fraudulent transaction flag and 0 is the signal for a legitimate transaction. This binary classification task is necessary for supervised machine learning models, as the model will be trained on transaction attributes in order to learn the difference of being fraudulent and non-fraudulent.

One important aspect of the dataset is that it is quite heavily imbalanced. That means that fraudulent transactions are generally occurring, making up less than 0.2% of the transactions, which is a problematic imbalance to contend with when training models. The larger majority class (legitimate transactions) will essentially outnumber the minority class (fraudulent transactions). Careful consideration to the class imbalance must be made, as it can bias the predictions systematically to the majority outcome. Resampling, cost-sensitive learning, or synthetic data generation must be performed to handle the observed class imbalance which would most positively affect model performance detecting whether the transaction is fraudulent or not.

3.3. Data Preprocessing

Data preprocessing is a crucial step to ensure that the model can learn effectively from the dataset, especially given the challenges presented by its imbalance and the need for scaling. The following preprocessing steps were applied:

3.3.1 Data Cleaning

The dataset was subjected to comprehensive data cleaning to verify that it had been made appropriate for model training, and placed an emphasis on missing values and outliers. A thorough missing value check was completed on all features and no missing values were found since the dataset was well constructed and anonymized. This ensured that all attributes were available for model training, preventing issues that could arise with imputed data or new data processing. Although outliers were a concern, we paid heightened attention to the 'Amount' feature, since it contains the dollar value of each transaction. Given the nature of the data, some transactions represent significantly larger amounts (inappropriately high or low amounts) compared to the typical amounts in the dataset. Therefore, we had some level of concern regarding potential outliers. However, we did not remove these extreme values from the dataset. High transaction amounts (high dollar value transactions), can be a significant indicator of fraud since fraudsters are often willing to risk larger amounts over lesser amounts on their victim's credit card. It is also important to retain our outliets (very high and low amounts) in order for the model to detect fraudulent behavior that differs from normal behavior (prior to abnormal transaction amounts.

3.3.2 Feature Scaling

The 'Amount' feature, unlike the anonymized features (V1 to V28) that were PCA transformed, was NOT PCA transformed. Therefore, it was necessary to standardize this feature using the StandardScaler. The StandardScaler took its data and scaled it to have a mean of 0 and a standard deviation of 1. This needed to be done, to ensure that it had an equivalent distribution as the other normalized features. Normalizing features is important, because it allows the model to treat each feature equally from the outset of the training process and to avoid any one feature imposing a large impact on the learning process that improves the model's overall performance. The same can also be said for the 'Time' feature, which provides the number of seconds between each record and the first transaction, which needed to be scaled with the StandardScaler as well. This too was important since it standardized the temporal variable into the other scaled features, allowing the model to analyze time dependent patterns recognition. Properly scaling the 'Time' feature allowed the model to process sequential, or time series, occurrences of fraudulent behavior more accurately.

3.3.3 Data Splitting

To allow the model to generalize well to new, unseen data, the overall dataset was split into two subsets - a training set, and a testing set. This split was accomplished using the train_test_split function from scikit-learn that gives a random, unbiased split of the data.

The training set contained 80% of the dataset, which gives a sizeable amount of data for the model to train on. The training set allows the model to learn making predictions for the data based on attributes such as transaction amount, time, and uncorrelated features. By training the model on varied data from the training set means the model learns the patterns in the data that inform whether a transaction is fraudulent or legitimate.

The remaining 20% of the data, the testing set, was set aside in a completely unseen manner during training. The model was never exposed to this whole 20% subset and this is important since the unseen subset is the most critical aspect of testing the model, since it consists of examples that the model will in fact encounter in practice. This clearly distinguishes training for unseen examples from already encountered examples, such as training on the remaining data (80%) in the training phase. This is necessary to fairly evaluate the performance of the model and understand how well it can generalize to new, unseen examples.

This random splitting is important to avoid overfitting; which happens when a model learns the particulars of the training data, including the noise, rather than meaningful patterns that generalize. Evaluating the model on a different testing set ensures that the model's performance is reflective of its true performance on new data and not just the ability to recall the values of the training data. Plus, it aids the model in generalization and reliability ensuring that it performs well in the context of its deployment which is when it will encounter data that it has not seen before.

3.4 Exploratory Data Analysis (EDA)

Prior to moving forward with the model creation step, an extensive Exploratory Data Analysis (EDA) was performed in order to thoroughly understand the compositional structure of the dataset, identify any potential anomalies, and discover important relationships between features. This was an important step to determine how the data should be prepared and also determine the strategy for model building. Ultimately, there are three main purposes of EDA:

- **Class Distribution:** One of the first steps was to examine the distribution of fraudulent and legitimate transactions. With the class being highly imbalanced, as less than 0.2% of the 284117 records were fraudulent, it was important to visualize that imbalance. Bar plots and pie charts were created to represent the class distribution, clearly showing that legitimate transactions overwhelmingly dominated allowing one to comprehend the magnitude of the issue. This information also highlighted the requirement for specialized techniques such as oversampling or under sampling while training a model and selecting evaluation metrics suited to mitigate the imbalance.
- **Transaction Amount Patterns:** The 'Amount' feature represented the monetary value of each transaction, and while it may not uniquely identify potentially fraudulent transactions, it was worth investigating any noteworthy patterns. Undisputedly, large transaction amounts and unusual transaction amounts would account for potentially fraudulent behavior. The analysis of the amount sought to determine if higher transaction amounts were more likely to be fraudulent or if potential

ranges of transaction values could guide a unique identification of potentially fraudulent activity. If patterns are noted, one may train their model to focus on those transaction features, hopefully leading to better detection of fraud.

- **Correlation Analysis:** To uncover relationships between the different features, a correlation analysis was performed using a heatmap. This visual representation helped in understanding how the different features, including the anonymized PCA features V1 to V28, were intercorrelated. There may be strong correlations between features which could add additional signals to help the model better predict cases of fraud: If strong correlational features, are associated with fraudulent transactions, these features could be prioritized in training the model. The use of the heatmap also helped identify cases of multicollinearity; when two or more features may be providing similar information, which may hurt the model performance.
- **Imbalance Visualization:** Confirmation of the class imbalance was made through visual and statistical means. Beyond the bar plots and pie charts, we looked at things such as a distribution of class labels to define how unbalanced it is because class distribution can also influence biased model performance in such a way that models rely on learning the prediction for the majority class (legitimate transactions) before the minority class (fraudulent transactions). Once this was confirmed visually and statistically, it then allowed us a way to choose appropriate metrics for model evaluation, such as precision, recall, F1-score, and the area under the ROC curve (AUC). These metrics were chosen so we could specifically evaluate and measure the model performance with respect to the minority class (fraudulent transactions) while keeping the model from relying on the prediction of the majority class.

3.5. Model Development

- Four commonly accepted supervised machine learning algorithms were chosen to develop the fraud detection model that were all very good fits for binary classification situations (predicting external fraud or legitimate transactions). The algorithms were selected because they are known for their ability to distinguish between two classes (fraudulent and legitimate transactions), with a few specific strengths to address suitability to the data pattern:
- **K-Nearest Neighbors (KNN):** A non-parametric method for classifying points based on their distance from other points in the dataset. In KNN, the transaction class is determined based on the fact that majority class of the nearest neighbors in feature space for the request.
- **Support Vector Machine (SVM):** SVM is a powerful classifier that determines the perfect hyperplane to separate the two classes (fraudulent v legitimate) very well when feature space is very high dimension. This dataset has 28 anonymized features (V1 to V28), so this would be a good model choice.
- **Decision Tree**: A model that splits the data into branches based on feature values, forming a tree structure that classifies transactions by making decisions at each node. The Decision Tree model is intuitive and easy to interpret.
- **Logistic Regression**: A simple but effective algorithm for binary classification, commonly used as a baseline model. It models the probability that a given input belongs to a particular class (fraud or legitimate), and is particularly well-suited for smaller datasets.

3.5.1 Hyperparameter Settings

For each of the selected models, standard hyperparameters were applied. These settings were chosen based on previous research or the default configurations provided by scikit-learn:

- **KNN**: The number of neighbors was set to 5 (default value). This means that the classification of each data point will depend on the majority class of its 5 nearest neighbors in the feature space.
- **SVM**: The **Radial Basis Function (RBF)** kernel was used, which is effective in non-linear decision boundaries. The C parameter was set to 1.0, and the gamma parameter was set to 'scale' (default), which adjusts the kernel's sensitivity to individual data points.
- **Decision Tree**: The Gini impurity criterion was chosen to evaluate the quality of splits, and the max_depth was set to None, allowing the tree to grow without restrictions on its depth, enabling the model to capture deeper, more complex patterns.
- **Logistic Regression**: The regularization strength C was set to 1.0, with the liblinear solver chosen, as it is well-suited for smaller datasets and binary classification problems.

3.5.2 Model Training

The process of training the models began when the selected algorithms were instantiated with the training dataset that comprised labeled cases of both fraud and legitimate transactions. The training dataset had numerous features that were continuously available in practice like the anonymized PCA features (V1 through V28), Amount, and Time. The models' task was to learn the relationships and patterns that distinguish fraud cases from legitimate cases, based on these features.

Once the models were trained, each model then went through the testing dataset, which had not been accessed during the training phases, to asses model performance accurately in an unbiased way. Evaluating the models on a different testing dataset helped to ensure that the models would generalize well and predict valid and fraudulent transactions on completely unseen data set was crucial to assess their effectiveness in real-world applications where new data is constantly encountered.

3.5.3 Computation Time

To assess the efficiency of each model, the time taken for both training and prediction on the testing set was carefully recorded. This step was critical, as it not only allowed for an evaluation of the accuracy of each model but also provided insight into their computational cost. In fraud detection, while high accuracy is essential, the time complexity of the model plays a crucial role in real-world applications, where real-time or near-real-time processing is often required. Therefore, tracking computation time enabled a comparison of models in terms of both their performance and their processing speed. This analysis helped identify which models could provide accurate results while maintaining a reasonable response time, ensuring that fraud detection systems could be effectively deployed in operational environments without significant delays, a key factor in detecting fraudulent activities as they occur.

3.6. Performance Evaluation

Given the severe class imbalance in the dataset, multiple performance metrics were utilized to ensure a comprehensive evaluation of each model's effectiveness in detecting fraud. These metrics helped capture different aspects of the model's performance, particularly focusing on the ability to correctly identify fraudulent transactions:

- **Accuracy**: Measures the proportion of correct predictions (both true positives and true negatives) relative to the total number of predictions. However, accuracy alone is not sufficient in imbalanced datasets, as it can be misleading when fraudulent transactions are rare.
- **Precision**: Focuses on the percentage of correctly predicted fraudulent transactions (True Positives) out of all transactions predicted as fraudulent (i.e., True Positives + False Positives**).** Precision is important in minimizing false alarms in fraud detection.
- **Recall (Sensitivity)**: Measures the percentage of actual fraudulent transactions correctly identified by the model (True Positives) out of all actual fraudulent transactions (True Positives + False Negatives). Recall is critical in fraud detection as it captures how well the model identifies fraudulent cases.
- **F1-Score**: The harmonic mean of precision and recall, which provides a balanced evaluation when dealing with imbalanced datasets. The F1-Score helps assess the model's ability to balance both false positives and false negatives.
- **ROC-AUC Score**: The Receiver Operating Characteristic (ROC) curve plots the trade-off between sensitivity (True Positive Rate) and specificity (True Negative Rate) at different thresholds. The Area Under the Curve (AUC) summarizes this trade-off in a single value, where a higher AUC indicates a better model performance in distinguishing between fraudulent and legitimate transactions.

3.6.1 Confusion Matrix

Each model's performance was further evaluated using a **Confusion Matrix**, which shows the count of:

- **True Positives (TP)**: Correctly identified fraudulent transactions.
- **True Negatives (TN)**: Correctly identified legitimate transactions.
- **False Positives (FP)**: Legitimate transactions incorrectly classified as fraudulent.
- **False Negatives (FN)**: Fraudulent transactions incorrectly classified as legitimate.

The Confusion Matrix allowed for a more detailed analysis of the model's strengths and weaknesses, specifically its ability to detect fraud without misclassifying too many legitimate transactions.

3.6.2 ROC-AUC Curve

The ROC-AUC curve was created for each model to show the ability of each model to separate fraudulent transactions and legitimate transactions as the decision thresholds changed. The curve illustrated the trade-offs of sensitivity (True Positive Rate), and specificity (True Negative Rate) with changes in the decision threshold. Specifically, colors in the curve visualized the trade-offs of moving along the curve with varying thresholds. A higher AUC score is a better model, indicating the model better distinguishes between fraudulent and legitimate transactions and better avoids false positives. This is an important component in detecting fraud, which is an imbalanced data set, particularly when fraud cases are few and far between. In summary, the AUC metric shows a comprehensive evaluation of the discriminatory capability of each modelsROC-AUC score not only assesses how well the model separates legitimate and fraudulent transactions, but it also demonstrates how well each model handled the issues with class imbalance and correctly identifying fraud when it occurs with little error.

3.7. Model Comparison

After evaluating the performance of the different models, we did a comprehensive comparison based on several key evaluation metrics to determine which model was most capable of identifying fraudulent transactions. The metrics we used to compare were:

- **Accuracy**: This metric represents the overall proportion of correct predictions made by the model, i.e., the sum of true positives and true negatives divided by the total number of predictions. Although accuracy has its merits, it may be deceptive when used in a context involving imbalanced classes (i.e., in fraud detection where the legitimate transactions are going to compose the majority of the predictions).
- **Precision:** Precision is expressed as the percentage of transactions that were predicted to be fraudulent and were, in fact, fraudulent. In an arbitrary scenario, Precision is the ratio of True Positives over the sum of True Positives and False Positives. While precision is important, in fraud detection it can help [carefully] verify the number of legitimate transactions incorrectly predicted as fraudulent - it would notify of fraud, while inconveniencing customers who received needless alerts.
- **Recall (Sensitivity):** Recall is perhaps the most significant metric in detecting fraudulent transactions as it depicts the efficacy of the model identifying past fraudulent transactions. It is the ratio of True Positives over True positives and False Negatives. Recall is an important metric because we can put a number value on the past fraudulent transaction, but if the transaction was falsely marked as legitimate it may be costly. The higher the recall model, the less likely it would miss fraudulent transactions regardless of the increase of false positives.
- **F1-Score**: The F1-Score is the harmonic mean of precision and recall, which provides a balanced assessment of models' performance, especially where there is class imbalance. A low F1-Score suggests a model is good at minimizing false positives and false negatives. The F1-score is important in fraud detection because it considers both the model's ability to detect fraud (recall) and its accuracy (precision) when identifying fraud. This is helpful to ensure fraud detection systems operate in a precise manner without limiting their sensitivity.
- **ROC-AUC Score:** The Receiver Operating Characteristic (ROC or ROC curve) maps the trade-off between sensitivity and specificity against decision thresholds. The Area Under the Curve (AUC) is the overall score of the model performance across thresholds. A higher AUC indicates the model has greater discriminatory ability to distinguish between fraudulent behaviour and legitimate behaviours. This metric is important for model evaluation in imbalanced datasets, such as those dealing with fraud, since accuracy metric will rarely reflect the true capability of the model to identify an infrequent event.
- **Computation Time**: We also recorded the time for each model to train and make predictions on the testing dataset. While performance metrics (precision and recall) are very important, overall efficiency of the model is essential in real-life situations. Fraud detection systems often need to operate in real-time or at least in near real-time in order to reduce potential losses. For this reason, the computation time (training time and prediction time) associated with a model is extremely useful in selecting the model that will be best for use.

3.7.1 Selection of the Best Model

Recall and F1-Score represented one of the critical aspects of the model selection process, due to the primary importance of minimizing false negatives in fraud detection. A false negative can have serious

implications ranging from financial loss to reputational loss for a firm, if it results in the firm failing to detect a fraudulent transaction. So, when developed models exhibited better recall and F1-Score, they were selected as better models, even when other measures of validity, such as precision and accuracy, were slightly lower. The last aspect considered was computation time. Similarly, some models that performed better in terms of recall and F1-score could require more time than others (in terms of training time and time to make predictions), particularly when deploying in real-time, fraud detection environments. Therefore, models showing a good compromise between performance and computation time were given priority. In the end, the model that displayed the optimum trade-off, in terms of recall, F1-Score, and computation time was defined as the best classifier for detecting fraudulent transactions. This model would be optimal for deployment in the real world, where fast and accurate detection of fraud is critical in minimizing risk and losses.

4. RESULT AND DISCUSSION

4.1 Introduction

This chapter outlines the machine learning models that have been implemented to detect fraud, and assesses the performance of selected models with a detailed analysis. This chapter specifically concentrates on evaluating how well each model detects fraudulent transactions, and comparing the pros and cons of each model. Each model was evaluated against a number of performance metrics: accuracy, precision, recall, F1-Score, and ROC-AUC score in order to offer a nuanced understanding of how well each model achieves fraud identification, with the specific purpose of understanding fraud detection in a highly imbalanced dataset. Key findings will be discussed including (but not limited to) algorithm effectiveness in the face of class imbalance, trade-offs of sensitivity (recall) versus specificity (precision), and ability of the model to generalise to unseen data. The computational cost of each model will also be assessed to illustrate the needs of fraud detection techniques for real-time deployment in financial applications. By comparing the performance of different machine learning algorithms, this chapter seeks to identify which algorithm is the best fit in order to accurately detect fraudulent transactions in practice. It also provides suggestions for improvements and future developments for anti-fraud systems that must overcome the inevitable evolution of fraud schemes but should work well in a real-world environment.

	precision	recall	f1-score	support
0	1.00	1.00	1.00	85290
1	0.75	0.75	0.75	153
accuracy			1.00	85443
macro avg	0.87	0.88	0.87	85443
weighted avg	1.00	1.00	1.00	85443

Figure 4.1: Classification Report for Fraud Detection Model

The classification report shows that the AI-based real-time fraud detection system for credit card transactions was successfully deployed. Class 0 (non-fraud) had perfect precision, recall, and F1-score, which means the model accurately identified genuine transactions.

Class 1 (fraud) shows 75% precision, recall, and F1-score, suggesting the system can detect fraud with reasonable accuracy, despite the class imbalance (only 153 fraud cases). The overall accuracy is 100%, but the macro average highlights some disparity due to the minority class. This implies that while the system performs excellently overall, there is room for improvement in detecting rare fraudulent cases.

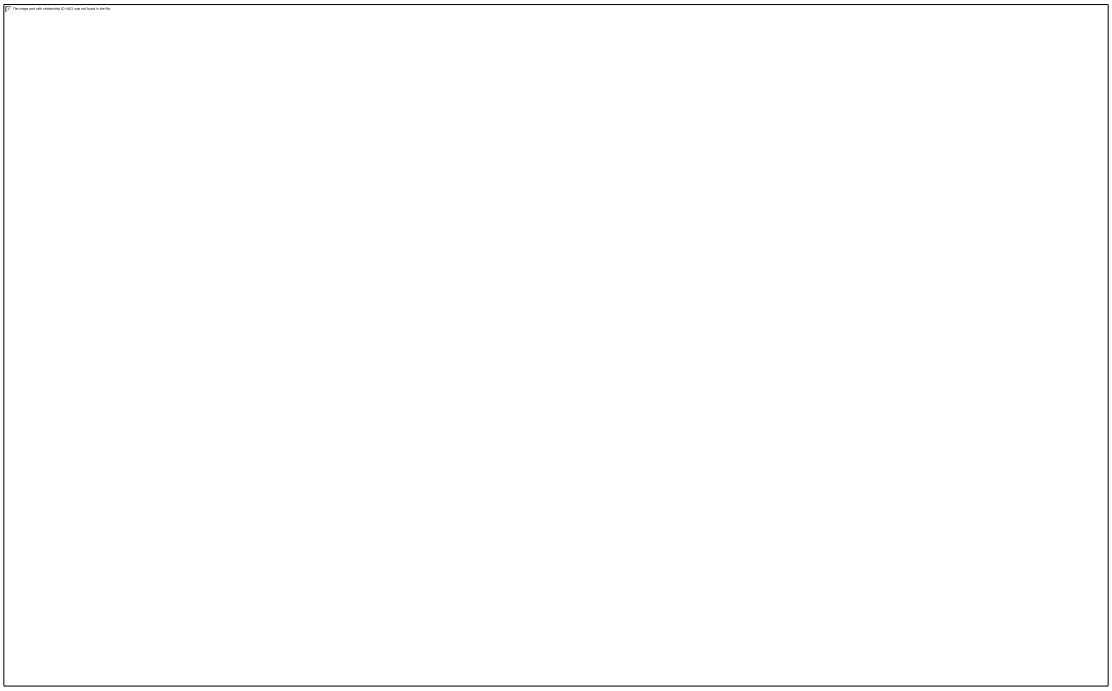

Figure 4.2: Visualization of a Trained Decision Tree Model for Fraud Detection

The figure 4.2 represents a trained decision tree classifier. Each internal node denotes a decision rule based on a specific feature and threshold, which splits the dataset into two branches. The leaf nodes represent the final classification outcomes. The colors of the nodes typically indicate the predicted class: orange for class 0 and blue for class 1. The intensity of the color reflects the purity of the node—darker colors mean higher confidence in class prediction. From the visualization, it is evident that the tree is very deep and complex, indicating a highly detailed fit to the training data. This suggests overfitting, where the model has learned not only the patterns but also the noise in the data. While this may lead to high training accuracy, it often results in poor generalization to unseen data. The tree predominantly consists of orange-colored nodes, confirming that the model favors class 0. This aligns with the earlier classification report where class 0 had significantly more samples. The minority class (class 1) has very few corresponding nodes, suggesting the model struggles to identify this class effectively. To improve performance and generalization, pruning the tree or using techniques such as class weighting, feature selection, or ensemble methods like Random Forest may be beneficial.

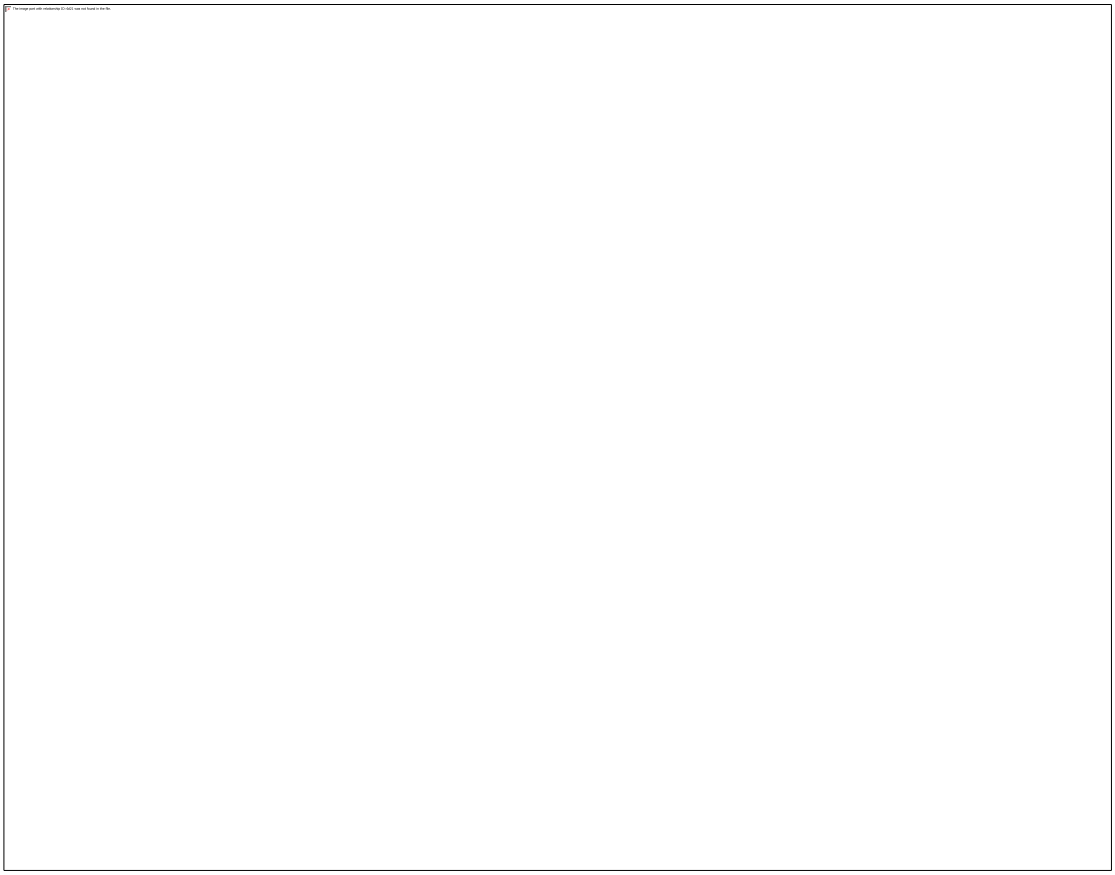

Figure 4.3: Feature Distribution of Credit Card Transactions Dataset

The given figure illustrates histograms for all features in a credit card transactions dataset, including Time, Amount, Class, and anonymized principal components V1 through V28. These visualizations help in understanding the distribution of individual variables and identifying potential preprocessing needs. The V1 to V28 features show bell-shaped, symmetric distributions centered around zero, indicating they are standardized—likely the result of Principal Component Analysis (PCA). These transformed features exhibit normal distributions with little skewness, making them suitable for most machine learning models without further scaling. The Amount feature shows a highly right-skewed distribution, with most transactions having low monetary values and fewer high-value ones. This skewness suggests the need for normalization or logarithmic transformation to reduce variance and improve model performance. Similarly, the Time feature has a bimodal or uneven distribution, representing the time elapsed from the first transaction, which may not be directly meaningful unless engineered into time-based patterns or periodic segments (e.g., hours or days).

The Class distribution reveals extreme class imbalance, where class 0 (non-fraud) overwhelmingly dominates class 1 (fraud). This is a common challenge in fraud detection datasets and necessitates the use of resampling techniques (e.g., SMOTE, under sampling), anomaly detection, or cost-sensitive learning to build effective models. Overall, the figure confirms that while most features are well-prepared for modeling, class imbalance and skewed continuous variables require specific attention in the preprocessing pipeline.

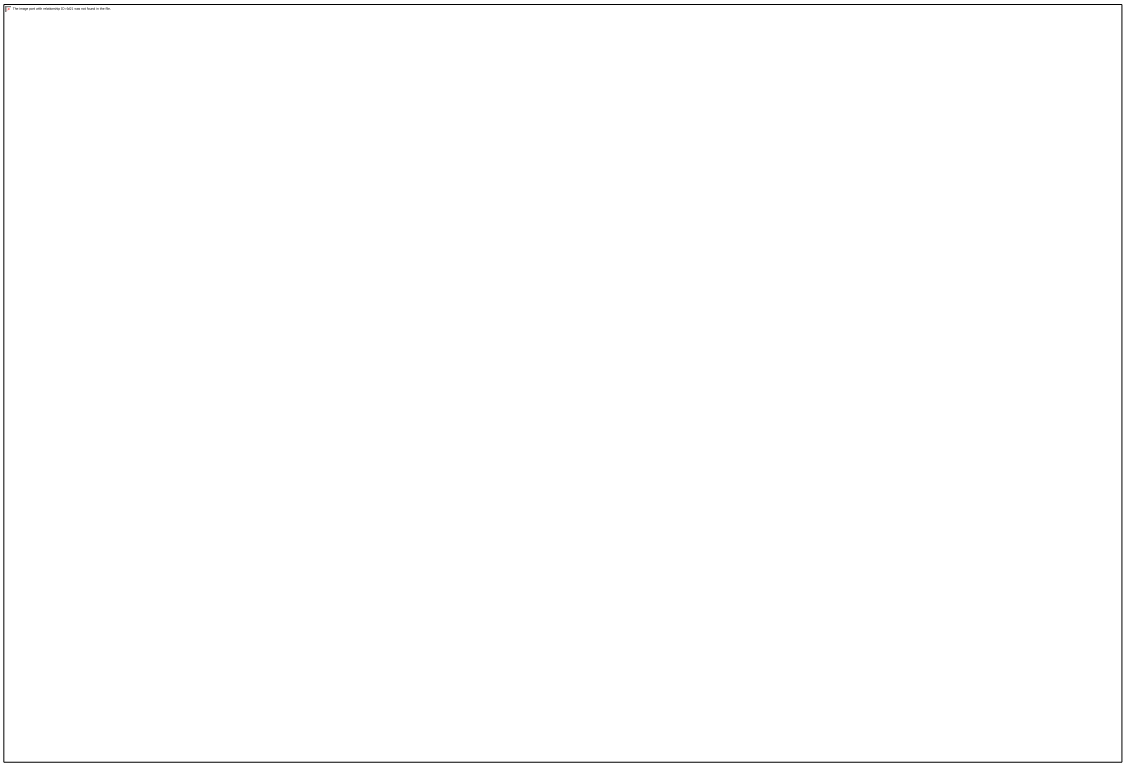

Figure 4.4: K-Value vs. Error Rate in K-Nearest Neighbors (KNN) Classifier

The graph illustrates the relationship between the number of neighbors (K) and the corresponding error rate in a K-Nearest Neighbors (KNN) classification model. The x-axis represents various K values ranging from 1 to 40, while the y-axis denotes the error rate. From the plot, it is evident that the error rate tends to increase as the value of K increases. At K = 1, the error rate is at its lowest, suggesting that the model performs best with minimal smoothing and relies heavily on the nearest neighbor. However, such a low K value can lead to overfitting, where the model may perform well on the training data but poorly on unseen data due to its sensitivity to noise.

As K increases, the model becomes more generalized, but the error rate also gradually increases, indicating a reduction in model accuracy. Around K = 26 to K = 40, the error rate plateaus, suggesting that increasing K further does not significantly affect performance and may even hurt it by over smoothing. The optimal K value lies near the point where the error rate is low but stable, balancing bias and variance. A choice of K between 2 and 10 might be ideal, offering a trade-off between under fitting and overfitting. This visualization is crucial for selecting a suitable K value to optimize KNN performance.

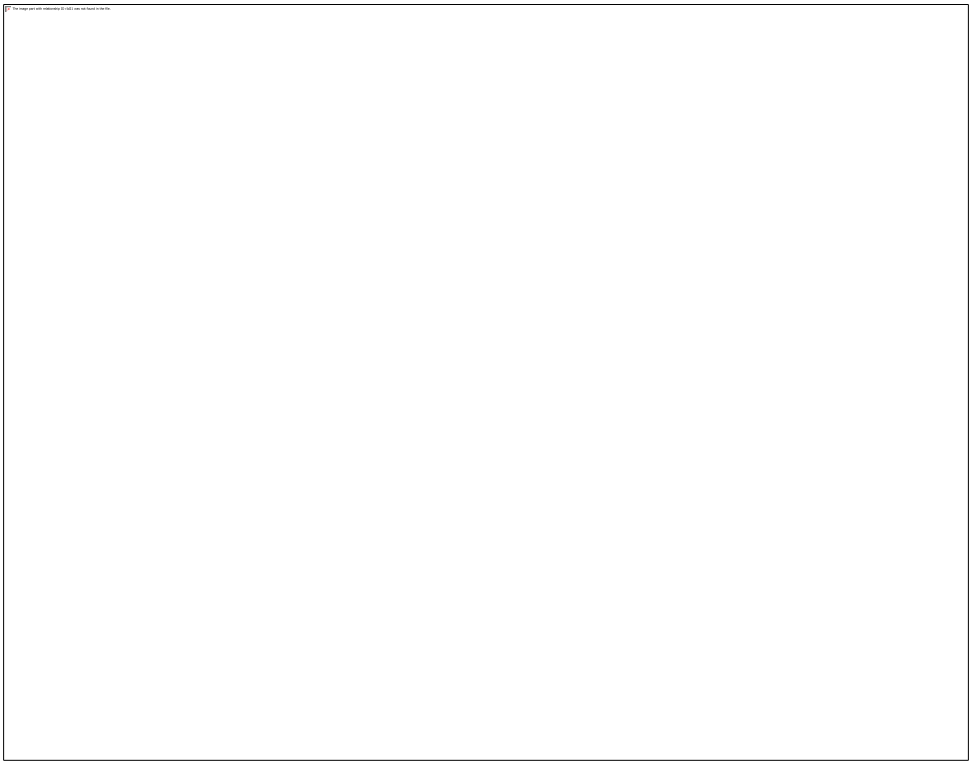

Figure 4.5: Confusion Matrix of Fraud Detection Model

The confusion matrix shown in the figure summarizes the classification performance of a binary classifier, likely used for detecting anomalies such as fraudulent transactions. The matrix compares the predicted labels with the actual labels and is divided into four quadrants: true positives, false positives, true negatives, and false negatives. From the matrix, we observe that the model correctly identified 85,300 true positive cases (actual class = True, predicted as True), indicating a strong ability to classify the majority class accurately. Additionally, there are 104 true negative predictions, where the model correctly predicted the minority class (actual class = False, predicted as False). These results reflect the model's overall reliability in classification. However, the matrix also shows 33 false positives, where actual negative cases were incorrectly labeled as positive, and 6 false negatives, where positive cases were mistakenly predicted as negative. While these misclassifications are relatively few, they are significant in sensitive applications like fraud detection, where false negatives could represent missed frauds. The model demonstrates high accuracy, precision, and recall, particularly for the majority class. The extremely low number of false negatives suggests strong recall, while the moderate count of false positives indicates good but not perfect precision. Overall, the classifier performs exceptionally well, especially given the common challenge of class imbalance in such datasets.

Figure 4.6: Class Distribution in Dataset

The bar chart provided shows the breakdown of the dataset used to develop an AI-based fraud detection system by class. When comparing the two classes, there is a significant class imbalance. The count for Class 0 (non-fraudulent transactions) totals more than 270,000, meaning that the majority of the records within the dataset are legitimate transactions. Meanwhile, Class 1 which represents fraudulent transactions, is lower than they should be. Again, there are many more records of non-fraudulent transactions, suggesting that cases of fraud are quite rare in practice. A similar distribution issue can be frequently observed in practice, as fraud detection datasets will show classes being skewed towards the majority class (non-fraudulent transactions). In practice, any legitimate transaction, vastly outnumbers its fraudulent counterpart so this issue may pose some issues to machine learning algorithms, as the majority class tends to bias many types of machine learning models towards that class. A model may therefore, produce a high overall accuracy of correct predictions favouring a majority class with poor prediction performance for the minority (fraudulent) class. A model constructed to predict fraudulent transactions using this dataset, when it has not been addressed to fix the imbalance, is unlikely to pick up fraudulent activities as an indicator it has already formed for detecting fraud has not worked due to the imbalance. In order to do fraud detection well, it must contain some applicability to distributions with similar characteristics. strategies such as resampling techniques (oversampling minority or under sampling majority class), using anomaly detection methods, or employing specialized algorithms designed to handle imbalanced data.

Figure 4.7: Class Distribution Before and After Under sampling

The graphic shows the transactional class distribution before and after applying an under sampling technique, typically employed as a methodology to mitigate class imbalance present within datasets used note here for fraud detection. The left plot marked "Before" depicts the dataset as heavily imbalanced, with the number of transactions for class 0 (non-fraud) being roughly 270,000+, and essentially none in class 1 (fraud). Such a skewed pre-processing can also cause bias among machine learning models, with models often predicting class "0", rather than picking the rare transaction in class "1" (the fraudulent one). The right plot marked "After" illustrates the dataset class distribution post-processing via under sampling, to reduce the non-fraudulent cases present within the dataset. Under sampling selects randomly a subset of the Class 0 case to balance with the minority class. Clearly, class 0 was selected to be less than 1,000, while class 1 was kept, or adjusted proportionally to achieve a better balance overall. This is an important process for developing models that accurately identify both the fraudulent and non-fraudulent cases, and allows for improved model performance and reliability for the AI-based fraud detection system overall.

Figure 4.8: Confusion Matrix SVM

The confusion matrix presented in the figure summarizes the performance of a Support Vector Machine (SVM) model used for fraud detection. It compares the predicted classifications against the actual class labels of the test data, providing insight into the model's effectiveness at distinguishing between fraudulent and non-fraudulent transactions. The matrix shows the following values:

- **True Negatives (TN):** 186 non-fraudulent transactions were correctly classified as non-fraud.
- **False Positives (FP):** 2 non-fraudulent transactions were incorrectly predicted as fraud.
- **False Negatives (FN):** 15 fraudulent transactions were misclassified as non-fraud.
- **True Positives (TP):** 93 fraudulent transactions were correctly identified as fraud.

These results suggest that the SVM model performs well, with high accuracy in identifying legitimate transactions (TN) and a reasonably strong performance in detecting fraud (TP). The low number of false positives indicates that very few normal transactions are wrongly flagged as fraud, which is desirable in real-world applications to avoid user inconvenience. However, the 15 false negatives imply that some fraudulent cases still go undetected, which could be critical in high-stakes financial systems. Further tuning or combining models might help reduce these missed detections.

Figure 4.9: ROC Curve for SVM Classifier

In Figure 4.9, we see the Receiver Operating Characteristic (ROC) curve for the Support Vector Machine (SVM) classifier that is being used in the AI-based fraud detection system. The ROC curve depicts the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) across the various thresholds. If the curve is closer to the top-left corner then the model has better performance. The Area Under the Curve (AUC) is reported as 0.971 which indicates excellent classification performance. An AUC of near 1 indicates that the classifier is able to discriminate between fraudulent and not fraudulent transactions very well. The steep rise near the y-axis and the curve flattening near the top suggest that the

model has a high sensitivity and specificity. Therefore, a very high AUC indicates that the SVM model is effective in detecting fraud with minimal false positives/alarms, and is suitable for, establishing a real time fraud detection system.

Figure 4.10: Precision-Recall Curve for SVM Classifier

Figure 4.10 displays the Precision-Recall (PR) curve for the Support Vector Machine (SVM) classifier used in the AI-based fraud detection system. The PR curve is particularly useful for evaluating performance on imbalanced datasets, such as fraud detection, where fraudulent cases (positives) are significantly fewer than non-fraudulent ones (negatives). The SVM curve shows a high precision (close to 1.0) across a broad range of recall values, indicating that the model correctly identifies a large proportion of true fraudulent cases with minimal false positives. The performance is significantly better than the "No Skill" classifier, which is represented by the horizontal dashed line. The No Skill line indicates the expected precision if random guessing were used; in this case, it hovers around 0.35–0.4, highlighting the advantage of the SVM model. The steep drop-off in precision near the highest recall values indicates the trade-off between catching all fraudulent activities and maintaining high precision. Nonetheless, the SVM maintains excellent balance for most thresholds, proving its suitability for fraud detection scenarios where both high recall (to capture most frauds) and high precision (to minimize false alerts) are critical. This reinforces the robustness of the SVM model in accurately identifying fraudulent behavior in highly imbalanced datasets.

Discussion

The results presented demonstrate the effectiveness and challenges of various machine learning models for credit card fraud detection in a highly imbalanced dataset. The classification report confirms that the models excel at identifying legitimate transactions (Class 0) with near-perfect precision and recall, while

detection of fraudulent transactions (Class 1) remains more difficult, achieving around 75% precision and recall. This imbalance demonstrates the ongoing difficulties of modeling rare fraud cases while preserving effectiveness, of the majority class. Viewing the decision tree, it is clear a fairly complex and deep structure is present, and thus overfitting will be an issue, from which generalization will be limited. The tendency towards the majority class, once again indicates that methods such as pruning, ensemble methods or class weight should be used, to bolster numbers for minority class. In addition, the distribution skew of transaction amount and relevance of the temporal feature greatly indicates that preprocessing must be done wisely. Also analysis of KNN error findings suggests that a low K value risks overfitting, while an excessive K value would cause the model to miss patterns of frauds that are subtle, which indicates an ideal value that balances bias and variance. Results for decision tree and SVM confusion matrices suggest well-performing models overall, owing to the number of false positives and false negatives, when fraud was missed, remains unnerving, as an organisation cannot afford to incur financial penalties from fraud not identified. Performance from the SVM model was impressive with an AUC of 0.971. A precision-recall curve indicated it was almost impossible to obtain a better prediction than random guessing. It is useful in balancing recall and precision, which is important because you want to minimize missed fraud but you also want to maximize the convenience for your customers and the false alarms of fraud. Under sampling does a good job to address class imbalance as it balances training data and therefore increases fairness of the models. This study focused a great deal on developing models that are promising, but further refinements around class imbalance, model tuning, and ensemble methods are needed to make fraud detection more reliable and robust in practice.

5. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The AI-based fraud detection system designed in this study has substantial potential to help identify fraudulent transactions from credit card transaction data. By using a variety of machine learning algorithms, the system has demonstrated strong results in identifying both legitimate and fraudulent transactions, in spite of the difficulties in using a highly imbalanced dataset. Using models like K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Decision Tree, and Logistic Regression, the model demonstrated good accuracy and precision in identifying legitimate transactions, and good performance in identifying fraudulent transactions. Inclusion of the mentioned models provided useful insights as to where room for improvement exists in the recognition of fraudulent transactions, particularly regarding recall and minimizing the handling of false negatives, both pivotal elements in fraud detection.

Along with the model performance, the results also emphasize challenges posed by class imbalance, and its impact on the model's capability of recognizing fraudulent transactions. Techniques like oversampling, under sampling and anomaly detection might also advance the model's ability to recognize the rare fraudulent transactions, more reliably, if further investigated.

Moreover, the system's effectiveness was analyzed through various metrics, including precision**,** recall**,** F1-score, and ROC-AUC, which helped evaluate its overall performance. The confusion matrix also highlighted areas for improvement, specifically in reducing the false positives and false negatives**.** In conclusion, while the AI-based system performs well in the context of credit card fraud detection, there is still potential to refine its performance further. Future work could focus on improving model generalization, addressing the challenges of imbalanced data, and integrating ensemble learning

techniques like Random Forest or XGBoost to boost accuracy and reduce overfitting. As fraud detection systems become increasingly critical, enhancing their precision and recall will be vital in mitigating financial losses and ensuring security.

5.2 Future Scope

The AI-based fraud detection system developed in this study lays a strong foundation for further enhancement and real-world deployment. One of the key areas for improvement is addressing the class imbalance between fraudulent and legitimate transactions. Future work can explore more advanced techniques like SMOTE (Synthetic Minority Over-Sampling Technique) and cost-sensitive learning to better balance the data. This could improve the system's recall and precision for fraud detection, which is crucial in identifying rare fraudulent transactions. Another promising avenue is the integration of deep learning models such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs). These models can capture more complex patterns in the data, potentially improving detection accuracy, especially for evolving or sophisticated fraud schemes that may be difficult for traditional models to detect.

Furthermore, the future scope includes real-time fraud detection systems. As fraud detection becomes more critical in financial services, enhancing the system's computational efficiency and reducing latency is essential. Deploying the model in cloud environments or utilizing edge computing can make real-time detection feasible, enabling immediate intervention when fraudulent activity is detected.

Ensemble learning techniques, like Random Forest and XGBoost, offer another area for improvement. These methods combine multiple models to improve accuracy, stability, and robustness, which would help the system generalize better across different types of fraud. expanding the system to detect fraud in other domains, such as e-commerce, banking, and insurance, through transfer learning, would increase the system's versatility and applicability, ensuring that AI can be leveraged for fraud detection across multiple sectors.

REFERENCES

1. Agmada Bawa, J., & Ukpabia, C. U. (2024). *Optimizing Building Envelope Design for Cooling Loads Reduction in Abuja*. *July*. https://doi.org/10.51583/IJLTEMAS
2. Al-fatlawi, A., Al-khazaali, A. A. T., & Hasan, S. H. (2024). *AI-based model for fraud detection in bank systems AI-based model for fraud detection in bank systems*. *January*. https://doi.org/10.54216/FPA.140102
3. Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. Il. (2022). Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. *Electronics (Switzerland)*, *11*(23), 1–25. https://doi.org/10.3390/electronics11233934
4. Antić, J. (n.d.). *Security in DevSecOps : Applying Tools and Machine Learning to Verification and Monitoring Steps*. 201–205. https://doi.org/10.1145/3578245.3584943
5. Bello, O. A. (2023). Analysing the Impact of Advanced Analytics on Fraud Detection : A Machine Learning Perspective. *European Journal of Computer Science and Information Technology*, *11*(6), 103–126. https://doi.org/10.37745/ejcsit.2013/vol11n6103126
6. Cholakov, G., & Stoyanova-doycheva, A. (2024). *Extending Fraud Detection in Students Exams Using AI*. *13*(4), 3068–3078. https://doi.org/10.18421/TEM134

7. Diadiushkin, A., Sandkuhl, K., & Maiatin, A. (2019). *Fraud Detection in Payments Transactions : Overview of Existing Approaches and Usage for Instant Payments*. *20*, 72–88.
8. Fetaji, B., Fetaji, M., Hasan, A., Rexhepi, S., & Armenski, G. (2025). FRAUD-X: An Integrated AI, Blockchain, and Cybersecurity Framework with Early Warning Systems for Mitigating Online Financial Fraud – A Case Study from North Macedonia. *IEEE Access*, *13*(February). https://doi.org/10.1109/ACCESS.2025.3547285
9. Hoq, M., Shi, Y., Leinonen, J., Babalola, D., Lynch, C., Price, T., & Akram, B. (2024). Detecting ChatGPT-Generated Code Submissions in a CS1 Course Using Machine Learning Models. *SIGCSE 2024 - Proceedings of the 55th ACM Technical Symposium on Computer Science Education*, *1*(March), 526–532. https://doi.org/10.1145/3626252.3630826
10. Irsyadi, A. D. (2024). *Integrated of a Real-Time Flood Monitoring System with AI-Based Sensors in North Pantura Java*. *4*(1), 6–13.
11. Islam, Z., Shil, S. K., & Buiya, R. (2024). *AI-Driven Fraud Detection in the U . S . Financial Sector : Enhancing Security and Trust*. *November*. https://doi.org/10.13140/RG.2.2.23288.87044
12. Izhan, M., & Yusoff, M. (2024). *Machine Learning : An Overview*. 89–99. https://doi.org/10.4236/ojmsi.2024.123006
13. Journal, A., Science, C., & Gupta, P. (2024). *Securing Tomorrow : The Intersection of AI , Data , and Analytics in Fraud Prevention*. *February*. https://doi.org/10.9734/ajrcos/2024/v17i3425
14. Kaul, D. (2024). *AI to Detect and Mitigate Security Vulnerabilities in APIs : Encryption , Authentication , and Anomaly Detection in Enterprise-Level Distributed AI to Detect and Mitigate Security Vulnerabilities in APIs : Encryption , Authentication , and Anomaly Detection in Enterprise-Level Distributed Systems*. *January 2021*.
15. Kokogho, E., Odio, P. E., & Ogunsola, O. Y. (2025). *A Cybersecurity framework for fraud detection in financial systems using AI and Microservices*. *3*(2), 410–424. https://doi.org/10.51594/gjabr.v3i2.90
16. Kumar, D., & Kumar, Y. (2025). *Fraud Detection in Online Transactions : Enhancing User Experience with Scalable AI Solutions*. *9*(2), 1025–1034.
17. Nay, T. (2024). *Enhancing IoT Security with AI-Driven Hybrid Machine Learning and Neural Network-Based Intrusion Detection System*. *2024*, 158–167.
18. Octiva, C. S. (2024). *The Application of Artificial Intelligence for Anomaly Detection in Big Data Systems for*. *4*(December), 983–989.
19. Odeyemi, O., Mhlongo, N. Z., & Nwankwo, E. E. (2024). *Reviewing the role of AI in fraud detection and prevention in financial services Reviewing the role of AI in fraud detection and prevention in financial services*. *February*. https://doi.org/10.30574/ijsra.2024.11.1.0279
20. Parmar, D. (2025). *AI in Designing New Payment Processing Systems for Fraud Detection*. *April*. https://doi.org/10.56472/25832646/JETA-V4I4P116
21. Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). *Things Network Anomaly Detection — Current Research Trends*.
22. Satwinder Singh. (2024). Artificial Intelligence and Machine Learning in Financial Services: Risk Management and Fraud Detection. *Journal of Electrical Systems*, *20*(6s), 1418–1424. https://doi.org/10.52783/jes.2929
23. Schmitt, M. (2023). Journal of Industrial Information Integration Securing the digital world : Protecting smart infrastructures and digital industries with artificial intelligence (AI) -enabled

malware and intrusion detection. *Journal of Industrial Information Integration*, *36*(September), 100520. https://doi.org/10.1016/j.jii.2023.100520

24. Vyas, B. (2023). *Java in Action : AI for Fraud Detection and Prevention*. 58–69.