



People's Democratic Republic of Algeria

**Ministry of Higher Education and
Scientific Research**

Saida University, Dr. MoulayTaher



Faculty of Economic, Commercial and Management Sciences

Accounting and Finance Department

Thesis Title

Detectingfinancial fraud using machine learning techniques

A thesis submitted in partial fulfillment of the requirements for a
Master's degree in Financial Sciences and Accounting.

Financial Sciences major

Supervisor:

Dr.AbdelrahmanTahi

Graduate:

Bouazza Bouchra Hmidia

Academic Year

2025/2026

Abstract

This study describes the development, execution, and assessment of an AI-enabled credit card fraud detection application built as a full-stack web application. The proposed system evaluates the financial transaction records to determine whether the process involved is a fraud or not using an ensemble of machine learning models, including Logistic Regression, Decision Tree, Random Forest, SVM, Gradient Boosting, and XGBoost.

The proposed credit card fraud detection application is trained using the Credit Card Fraud Detection Dataset 2023, which has 568,630 transactions extracted from Kaggle. To handle class imbalance in the dataset, SMOTE is used, whereas PCA features are employed to enhance the security of the transaction data. Moreover, in this research, a novel concept of “Simulation Bridge” architecture is employed, which facilitates the conversion of unstructured data into a structured data format for the processing of PDF files uploaded by the users. The amounts involved in transactions can be parsed and converted into structured data formats using the trained model.

The backend development framework of the proposed system is based on FastAPI, which facilitates asynchronous execution, whereas the frontend is developed using Next.js, React, Tailwind CSS, and Framer Motion.

Keywords: Credit Card Fraud, Machine Learning, Fraud Detection, Ensemble Learning, Web-Based System.

الملخص

تصف هذه الدراسة تطوير وتنفيذ وتقييم تطبيق لكشف الاحتيال في بطاقات الائتمان، مدعوم بالذكاء الاصطناعي، ومبني كتطبيق ويب متكامل. يقوم النظام المقترح بتقييم سجلات المعاملات المالية لتحديد ما إذا كانت العملية احتيالية أم لا، وذلك باستخدام مجموعة من نماذج التعلم الآلي، بما في ذلك الانحدار اللوجستي، وشجرة القرار، والغابة العشوائية، وآلة المتجهات الداعمة، وتعزيز التدرج، وXGBoost.

تم تدريب تطبيق كشف الاحتيال في بطاقات الائتمان المقترح باستخدام مجموعة بيانات كشف الاحتيال في بطاقات الائتمان لعام 2023، والتي تضم 568,630 معاملة مستخرجة من منصة Kaggle. ولمعالجة عدم توازن الفئات في مجموعة البيانات، تم استخدام تقنية SMOTE

يعتمد إطار تطوير الواجهة الخلفية للنظام المقترح على FastAPI، مما يُسهّل التنفيذ غير المتزامن، بينما تم تطوير الواجهة الأمامية باستخدام Next.js و React و Tailwind CSS و Framer و Motion.

الكلمات المفتاحية: الاحتيال في بطاقات الائتمان، التعلم الآلي، الكشف عن الاحتيال، التعلم التجميعي، نظام قائم على الويب.

Table of content

INTRODUCTION	12
CHAPTER I	1
FUNDAMENTALS OF FINANCIAL FRAUD AND CREDIT CARD TRANSACTIONS	1
1.1 INTRODUCTION	4
1.2 Financial Fraud :Definition and concepts	4
1.2.1 Definition of Financial Fraud	4
1.2.2 Characteristics and Elements of Financial Fraud	6
1.2.3 Types of Financial Fraud in Financial Institutions	7
1.2.4 Causes and Motivations behind Financial Fraud	8
1.2.5 Economic and Financial Impacts of Financial Fraud	9
1.3 Classification of Financial Fraud in Financial Institutions	10
1.3.1 Internal vs. External Fraud	11
1.3.2 Online and Offline Fraud	13
1.3.3 Credit Card Fraud vs. Other Financial Frauds	14
1.4 Credit Card Systems and Transaction Lifecycle	16
1.4.1 Architecture of Credit Card Systems	16
1.4.2 Processing Workflow and Stages	17
1.4.3 Authorization, Clearing, and Settlement	18
1.5 Credit Card Fraud: Concepts and Types	19
1.5.1 Definition of Credit Card Fraud	20
1.5.2 Common Techniques Used in Credit Card Fraud	21
1.6 Challenges in Detecting Financial and Credit Card Fraud	22
1.6.1 Data Imbalance and Concept Drift	22
1.6.2 Real-Time Detection Constraints	23
1.6.3 Privacy, Security, and Ethical Issues	23
1.7 Economic and Financial Impacts of Fraud	24
1.7.1 Financial and Institutional Losses	24
1.7.2 Consequences for Customers and Market Confidence	25
1.7.3 Legal and Regulatory Implications	25
1.8 Conclusion	27
CHAPTER 2THEORETICAL FOUNDATIONS OF FINANCIAL FRAUD DETECTION: FROM CLASSICAL APPROACHES TO MACHINE LEARNING METHODS	28
1.1 INTRODUCTION	29

1.2	Classical Statistical Techniques	30
1.2.1	Rule-Based Systems (Expert Systems)	30
1.2.2	Statistical Hypothesis Testing	30
1.3	Challenges of Traditional Fraud Detection Methods	31
1.4	Machine Learning in Fraud Detection	32
1.4.1	Introduction to Machine Learning and Its Role in Fraud Detection	32
1.5	Machine Learning Algorithms in Fraud Detection	36
1.5.1	Commonly Used Algorithms in Fraud Detection	36
1.5.2	Preprocessing Financial Data before Applying Algorithms	41
1.6	Model Evaluation Metrics	42
1.6.1	Methods for Evaluating Model Performance	43
1.7	Ethical and Legal Considerations in Using Machine Learning	44
1.8	Comparative Analysis: Classical vs. Machine Learning Approaches	45
1.9	Conclusion	47

CHAPTER 3 PRACTICAL IMPLEMENTATION OF A CREDIT CARD FRAUD DETECTING SYSTEM USING MACHINE LEARNING 48

1.1	INTRODUCTION:	49
□	Scope and Limitations:	50
.2	LITERATURE REVIEW	51
2.1	Credit Card Fraud: A Global Challenge	51
2.2	Traditional Fraud Detection Methods:	51
2.2.1	Rule-Based System (Threshold-Based Detection):	52
2.2.2	Z-Score Method (Standard Deviation Approach):	52
2.2.3	Benford's Law:	54
2.3	Machine Learning Approaches in Fraud Detection	56
2.4	Class Imbalance Problem in Fraud Detection	57
2.5	PCA in Financial Data Privacy	57
2.6	Synthesis of Contemporary Research	58
2.6.1.	Performance of Standard Classifiers	58
2.6.2.	Smote-Based Approaches	59
2.6.3.	Boosting and Hybrid Approaches	59
2.7	Comparative Analysis of Previous Studies	60
2.7.1	Summary Insight	61

2.8	Research Gap and Problem Statement	61
.3	METHOD	62
3.1	Research Approach:	62
3.2	System Design Overview	62
3.3	System Architecture :	63
3.2.1	The Simulation Bridge Architecture	63
3.3.2	High-Level Architecture	64
3.3.3	Backend Architecture (FastAPI)	64
3.3.4	Frontend Overview	65
3.3.5	Data Flow Process	65
3.4	Data Collection	66
3.5	Data Preprocessing	67
3.6	Model Training Pipeline	68
3.7	Model Descriptions	68
3.8	Backend API Implementation	69
3.9	PDF Processing	69
3.10	Frontend Implementation	69
4.	SYSTEM IMPLEMENTATION.	70
4.1	Technology Stack.	70
4.2	System Evaluation	70
4.2.1	Functional Evaluation of the System	70
4.2.2	Model Performance Overview	71
4.2.3	Ensemble Analysis	71
4.2.4	System Performance (Descriptive Analysis):	71
.5	RESULT AND ANALYSIS	71
5.1	Model Training Results	71
5.2	Cross-Validation Performance	72
5.3	Ensemble Voting Analysis	73
5.4	System Performance	74
.6	DISCUSSION	74

6.1	Strengths of the Approach	74
6.2	Limitations	75
6.3	Ethical Considerations	75
7.3	DISCUSSION	76
7.1	Strengths of the Approach	76
7.2	Limitations	76
7.3	Ethical Considerations	77
8.	CONCLUSION AND FUTURE WORK	77
8.1	Conclusion	77
8.2	Future Work	78
	GENERAL CONCLUSION	80
	BIBLIOGRAPHY	81

List of Tables

Table1 machine learning in fraud detction _____ 37

Table 2description of dataset features for credit card fraud detection _____ 67

Table 3 Model Training Results _____ 72

Table 4Comparative Cross-Validation Performance of Machine Learning Models _____ 72

List of Figures

Figure 1 Z-Score Flagging: Transactions beyond 3σ are flagged as anomalies----- 53

Figure 2 Benford's Law: Fraudulent data often deviates from the expected leading-digit distribution ---- 55

Figure 3 Illustrates the system structure ----- 64

Acknowledgements

First and foremost, I praise **God Almighty** for giving me the strength, health, and perseverance to complete this research work. His blessings and guidance have been the light illuminating my path throughout this academic journey.

I would like to express my deepest gratitude and utmost respect to my academic supervisor, **Mr. TahiAbderrahmane**, for his invaluable guidance, continuous support, and constructive criticism. His expertise, patience, and insightful remarks have been instrumental in shaping this thesis and pushing me towards academic excellence.

My sincere thanks also go to the esteemed members of the jury for taking the time to review and evaluate this work, and for their valuable insights that will undoubtedly enrich this research.

I extend my appreciation to all the professors and faculty members of the **Faculty of Economic, Commercial, and Management Sciences** for the wealth of knowledge they shared with us over the years.

To everyone who contributed, directly or indirectly, to the success of this work, I am forever grateful.

Dedication

To God Almighty

I thank God for granting me the strength, patience, and will to accomplish this work. My gratitude is infinite for His countless blessings and for guiding my steps on the path of knowledge.

To Myself

To the one who never gave up. To her who believed in her dreams despite the sleepless nights, fatigue, and moments of doubt. I dedicate this success to my own perseverance, honoring every single effort made to reach this goal.

To My Dear Father

I deeply thank my father, **Habib**, who has been my greatest encourager and the one who gave me the strength to keep going. Thank you for all your efforts and unconditional support... Thank you, Dad, for everything.

To My Dear Mother

No words can ever express my gratitude for your sacrifices and unwavering support. Wishing a speedy recovery to the role model of my life, thanks to whom I learned how to be the heroine of my own story... This work is nothing but the fruit of your precious labor.

To Ahmed Atamena

The source of my happiness and joy, whose presence was silent yet left a profound mark on my life. To the one who knew how to be a constant pillar of support during this important stage of my life—with all my gratitude and highest esteem.

To My Teachers and Supervisors

For their guidance, valuable advice, and dedication to transmitting their knowledge with passion and generosity.

"This thesis is not just a project; it is a shout of victory. And in silence, it proudly bears my name."

Introduction

Introduction

❖ GeneralContext

Technological advancements and innovations, coupled with the widespread use of digital payment systems, have revolutionized the way financial transactions are conducted globally. Credit cards, debit cards, and digital wallets have taken precedence over cash-based systems as tools used for conducting business in both developed and developing nations owing to their ease of use, availability, and efficiency. Therefore, the global finance system is currently processing billions of electronic transactions daily.

Nevertheless, there are several issues associated with such technological advancements, with one of the most prevalent being that of financial fraud. Clearly, there is an urgent need for efficient fraud detection systems that can be deployed in modern financial landscapes.

The conventional approaches of fraud detection are based mostly on rule-based systems that use predetermined patterns and thresholds such as large transactions or transactions performed from unusual geographic areas. Though these techniques have proven their efficiency in detecting obviously fraudulent operations, they still face numerous shortcomings. Among the biggest challenges that arise when working with these techniques is the occurrence of false positives (legitimate operations marked as fraudulent), and inability of the technique to adjust for the emergence of more complex frauds. In other words, nowadays' conventional security measures are not sufficient anymore.

However, machine learning can provide an excellent solution. In contrast to the traditional approaches, machine learning techniques learn from the past transactions themselves, which means that they are capable of identifying various hidden patterns. Another advantage of machine learning is its adaptability to the ever-changing environment of fraud behaviors.

In this research work, the problem statement is concerned about using the ensemble methods of machine learning for the detection of fraud transactions in credit cards. The use of multiple classifiers would improve the effectiveness of the detection process. The proposed method seeks to counter the weaknesses associated with using a single classifier model.

❖ Problem Statement

Introduction

Despite significant advancements in financial fraud detection systems many of the methods currently in use still suffer from numerous limitations, particularly in terms of accuracy, adaptability and real-time performance. Most traditional solutions rely on fixed rules or individual machine learning models, which makes them less effective when dealing with new or constantly evolving fraud patterns. Accordingly the main problem addressed by this research can be formulated as follows:

How can an intelligent and effective system for detecting credit card fraud with high accuracy be designed using machine learning techniques?

To answer this question optimally, the following sub-questions can be posed:

How can transaction data be properly prepared and processed for the purpose of using it in machine learning models?

What classification algorithms are most effective in detecting financial fraud in structured financial datasets?

How does the integration of multiple model types improve overall accuracy and reliability of the predicted results?

❖ Hypothèses

To address the research questions, the following hypotheses are proposed:

- Machine learning models are capable of significantly enhancing fraud detection when compared to traditional rule-based systems.
- The combination multiple models using the ensemble method makes predictions more reliable.
- Data processing and feature selection has a major impact on the performance of the model

❖ Reasons for choosing the topic

We chose this theme for both objective and individual reasons. On a practical level, the detection of fraud in the financial sector has become a critical issue and improving systems for its detection is vital for limiting financial loss and enhancing security. On the other hand, from a personal perspective, this study provides an opportunity to apply machine learning techniques to a real-world problem, and to enhance practical skills in the field of artificial intelligence and systems development.

❖ Research Objectives

Introduction

- The main objectives of this study are:
- To design an intelligent fraud detection system based on machine learning.
- To build a complete pipeline from data processing to prediction.
- To compare multiple classification models and improve accuracy using ensemble learning.
- To develop a functional web-based application for real-time interaction.

❖ Methodology and Tools

The approach of this study is analytical and experimental based on machine learning techniques. The system has been developed using a mix of backend technologies and frontend technologies.

Multiple models of machine learning are applied, such as logistic regression, random forest, decision tree, support vector machine, gradient boosting, and XGBoost. Those models are evaluated and combined using a majority voting strategy.

System also includes a web interface for user interaction, where PDF documents are uploaded and processed to generate predictions.

❖ Scope and Limitations

The scope of this study is limited to credit card fraud detection using structured and anonymized datasets. The system processes input documents and generates binary classification results (fraudulent or legitimate).

However, this work has some limitations, such as the use of static models that are not updated in real time, and the absence of temporal transaction features, which are often important in real-world fraud detection systems

Chapter I

Fundamentals of

Financial Fraud and

Credit Card

Transactions

1.1 Introduction

Financial fraud is a big problem for banks and the economy as a whole. It means doing a lot of illegal things to make money by lying, misrepresenting, and breaking trust. Fraudsters have more chances to steal money now that digital banking, online payment systems, and complicated financial products are becoming more common. It is also harder to find and stop fraud. (Button, & Cross, 2017).

This research seeks to provide a thorough understanding of financial fraud, with a special emphasis on credit card fraud, its classification, detection issues, and economic consequences. By exploring both theoretical and practical issues, the research underscores the need for effective anti-fraud tactics that include technological, legal, and organizational approaches.

1.2 Financial Fraud :Definition and concepts

When studying financial fraud, researchers often look at different factors, such as the instrument (credit cards, loans, securities), the technique (online vs. offline), and the person who did it (internal vs. external). To make good detection and prevention systems, it's important to understand these things.

Financial fraud is when someone lies on purpose to get an unfair or illegal financial benefit. It could include making false records, stealing money changing financial statements or doing transactions without permission (ACFE, 2022).

1.2.1 Definition of Financial Fraud

Fraud may be formally defined as the unlawful appropriation of another person's income or assets through acts of deception. In other words, it constitutes a deliberate and dishonest practice involving financial irregularities, carried out with the intent of obtaining personal gain or undue advantage.

According to the Auditing Standards Committee (2015), fraud refers to any intentional act committed by one or more members of management, employees, or external parties with the objective of obtaining an unlawful or unfair benefit. Although the legal concept of fraud is broad, the auditor's primary concern lies in fraudulent activities that result in material

misstatements in the financial statements. It is important to note that not all fraudulent acts are necessarily aimed at distorting financial reporting. Furthermore, auditors are not responsible for making legal determinations regarding fraud. The Committee distinguishes between two main categories of fraud: management fraud, which involves one or more members of management, and employee fraud, which is committed solely by staff members of the entity. In either situation, fraud may also involve collusion with third parties outside the organization (Javadian Kootanaee, Poor Aghajan, & Shirvani, 2021)

One of the largest challenges in current financial systems is financial fraud. According to the Association of Certified Fraud Examiners (ACFE, 2022), financial fraud is defined as:

“Any act of deception, concealment, or breach of trust carried out to obtain money, property, or services unlawfully. These things happen when people or groups do them, and they don't need to use or threaten physical force. This definition brings out a few important points:

1. **Intentionality:** Acts of fraud are intentional acts, meaning they are planned and carried out to obtain illegal financial gains. As a result, unlike mistakes or accidental errors, fraud involves deliberate deception.
2. **Deception and Concealment:** Fraud usually includes some form of deception or hiding information that would prevent the act from being detected. Methods used may be document forgery, manipulation of accounting records, alteration of electronic transaction records, or misrepresentation of facts. Often, as important as the fraudulent act itself, it allows perpetrators to avoid immediate detection.
3. **Breach of Trust:** Fraudulent activities exploit the trust of individuals, especially in cases of internal fraud, where the trust placed on the people working within the organization can make them use their authority for their personal gain. In external fraud, the trust that consumers place in the financial system can enable outsiders, such as customers or cybercriminals, to perpetrate fraud and identity theft.
4. **Variety of Perpetrators:** Frauds can be committed by single individuals or organized groups, either internally or externally. This is because an offender could either be someone within the organization or an outsider. The advancement in technology has brought about

increased interconnectivity between financial systems, hence increasing the number of potential criminals.

5. **Scope of Activities:** The nature of financial fraud does not consist of one activity alone; it may include practices like embezzlement, credit card fraud, insider trading, loan fraud, insurance fraud, and even cyber fraud. Each form of fraud comes with unique risks that pose different threats.
6. **Evolution in the Digital Era:** The development of digital banking systems, internet banking systems, and other e-financial systems has altered the field in several ways. E-Financial instruments offer faster and more convenient transactions across international borders but, unfortunately, also offer new avenues for fraud. Cyber fraud, phishing schemes, malware attacks, and hacking are some of the new kinds of financial crimes.
7. **Economic and Societal Implications:** In addition to the obvious monetary implications of fraud, it may result in serious indirect consequences as well. Financial fraud can harm an organization's reputation, its standing among regulators, and the overall economic environment.

In summary, financial fraud is a complex and dynamic issue that affects financial systems worldwide. It is crucial to comprehend the different definitions, mechanisms, actors involved, and trends associated with financial fraud to mitigate any future occurrence. (Levi, & Burrows, 2008).

1.2.2 Characteristics and Elements of Financial Fraud

Financial fraud, which is generally defined as the practice of using deceptive information for financial gains or concealment purposes, has some key features that set it apart from other types of fraud. First, it usually involves manipulating information, which serves as a basis for making decisions about investing or assessing financial health. In most cases, financial fraud is committed by managers or employees due to their knowledge and access to accounting systems and financial statements.

The components of financial fraud include the presence of deception, intent to defraud, and economic benefit. Misrepresentations, false information, or accounting records are common tools used for achieving financial gains through fraud. Different ways of conducting financial fraud include overstating revenue, understating expenses, overvaluation of assets, and

concealment of liabilities. Overall, these actions are done for creating a positive financial state for the organisation. It is worth noting that the same behaviour can be seen from people who submit false financial information to apply for loans or insurance policies (Reurink, 2016).

1.2.3 Types of Financial Fraud in Financial Institutions

There are many types of financial frauds that financial institutions are likely to experience from time to time. They include internal fraud where the people within an institution abuse their position to manipulate the financial resources; external fraud is a situation where individuals outside the institution try to cheat the firm using scams or other tricks. Also, there is the case of cyber-fraud whereby hackers use technology in stealing sensitive information. Other frauds include transaction fraud whereby individuals engage in transactions that are fraudulent in order to get financial gains. Identity fraud is the final type of fraud that entails stealing the identity of a person in order to conduct a fraudulent activity in his/her name.

Fraud can appear in different ways according to the characteristics of the fraudster and the party being victimized. The fraud can initially take place at an individual level, whereby individuals carry out acts of deception against consumers, clients, or other business stakeholders, for example, by intentionally changing the quality of goods or making misleading speculations in the stock exchange market. Fraud can also be committed against the employer by his or her employee. Some of the most common scams are payroll manipulation, expense reimbursement fraud, debt and liability changes, cash diversion, and intellectual property theft. At the corporate level, companies may engage in fraudulent activities against investors, consumers, or employees. Examples include manipulating financial statements to present misleading information, selling counterfeit goods as authentic, and failing to remit employee-related taxes or social insurance contributions. Financial institutions are also frequent targets of fraud, which may involve the use of lost or stolen credit cards, issuing fraudulent checks, or submitting false insurance claims. Similarly, governments may be affected through fraudulent grant applications, fabricated social security claims, and tax evasion by individuals or corporations. Organized criminal groups may perpetrate large-scale fraud against major organizations, such as professional forgery networks, mortgage fraud schemes, corporate identity theft, and money laundering operations. In addition, the rapid development of digital

technologies has led to the emergence of cyber-related crimes, including internet fraud, copyright violations, and unauthorized system access (Al-Jajawi & Al-Zarfi, 2018).

As per the definition provided by the Association of Certified Fraud Examiners, the internal fraud within any organization could broadly be divided into three categories. The first category is termed asset misappropriation, which includes the theft or misuse of the assets of an organization, such as inventory, cash theft, fraudulent billing, misappropriating accounts receivable, and payroll fraud. Financial statement fraud means manipulating the accounting records and financial statements for illegal gain, and it may even involve fraudulent documents relating to employees (ACFE, 2015).

1.2.4 Causes and Motivations behind Financial Fraud

Financial fraud is a multi-faceted issue that can be explained through a number of economic, organizational, psychological, and environmental reasons. There is no one reason for such conduct but a set of factors that make an environment where there are incentives for financial crimes. Many cases of fraud stem from a combination of internal control deficiencies together with the pressures on the people committing the crime (Wells, 2017).

From an economic viewpoint, financial distress is arguably one of the most potent motivations behind fraud. Financially distressed people, those who have debts to pay off, or even those struggling financially may find themselves tempted into fraud in order to relieve themselves from this stress. On the other hand, financially stressed companies, those that experience declining revenues, or even face tough competition may be compelled to manipulate their accounting figures in order to appear successful and credible (Cressey).

Factors within an organization have an important part to play when it comes to facilitating financial fraud. Inadequate internal controls, poor segregation of tasks, absence of supervision, and inadequate auditing processes make it highly likely that instances of financial fraud will occur. The presence of accountability structures is crucial in order to reduce the likelihood of fraud occurring; their absence makes such incidents easier to perpetrate. Employees and others may take advantage of such weaknesses within an organization to commit fraudulent acts without being caught or detected (Singleton, T. W., & Singleton, A. J, 2010).

Psychologically speaking, instances of fraud have been accounted for by behavior models like the fraud triangle, where pressure, opportunity, and rationalization are key components. People who engage in fraud tend to use self-rationalization to support the idea that what they are doing is inconsequential or that it can be reversed or forgiven depending on specific circumstances. Other psychological factors such as greed, ambition, discontent, or an organizational culture that is permissive of wrongdoing further enhance self-rationalization processes. Repeated contact with weak ethical behavior within an organization will eventually normalize such practices and minimize moral opposition. Moreover, technological advancements have played an important role in the perpetration of financial frauds. An increased dependency on technology and digital processes presents many new opportunities for fraudsters, both internal and external to an organization. Inadequate cybersecurity measures, encryption policies, and real-time fraud detection systems make the organization vulnerable to different forms of cyber fraud, such as phishing, identity fraud, and accessing financial information through computer systems. As the finance industry continues to digitize, so does its vulnerability to financial crimes (COSO, 2013).

Furthermore, the wider environment that includes various institutions and regulations is also a factor in determining the probability of financial fraud. Low law enforcement and weak regulatory supervision can increase incentives to commit financial crimes because of the lower possibility of facing sanctions. On the other hand, well-developed regulatory frameworks and efficient control mechanisms have a great potential to mitigate risks of fraud. Lastly, external factors including the presence of economic turmoil, high rates of inflation and unemployment, as well as growing competition, might aggravate the problem of financial fraud. Under these conditions, people and organizations are forced to take risky steps to ensure their survival or improve financial results, making them more likely to conduct themselves unethically from the point of view of finance. Hence, financial fraud can be viewed as a result of interactions among different aspects discussed above (OECD, 2019).

1.2.5 Economic and Financial Impacts of Financial Fraud

Fraud is very harmful not only to individual firms but also to the market and even the economy at large. Fraud has negative impacts on firms since it causes losses to their funds and results in bad reputation for that particular firm, due to loss of reputation from customers and shareholders. In regard to the market, fraud leads to distorted financial statements, hence lack of transparency. Consequently, it destroys the confidence of the investor,

resulting in instability within the market. As for the stakeholders, they include employees, shareholders and consumers, among others. They are all negatively impacted as they end up losing money, making lesser profits and higher costs.

Financial fraud is a major threat to financial stability because of the negative impacts that it brings about to different organizations, including the entire financial market. Some of the negative impacts include financial loss for the institution, high operational costs, and damage to the organization's reputation, which results in the loss of customers and reduced confidence among investors. Organizations affected by financial fraud also find themselves spending lots of money trying to improve their internal control systems.

On the other hand, with regard to the financial market, financial fraud is one factor that results in distortion in financial information leading to a reduction in market efficiency. Financial fraud results in a loss of investor confidence in the financial market, resulting in inefficient markets through volatility and investors' unwillingness to trade. Financial fraud also leads to negative impacts on various entities such as employees, stockholders, clients, and others, who incur financial losses, decreased dividends, job insecurity, and increased transaction costs. As far as the macroeconomic environment is concerned, financial fraud leads to negative implications on the economy in terms of reduced investor confidence, investments, and economic growth. (Global Study on Occupational Fraud and Abuse. 2022).(Global Study on Occupational Fraud and Abuse., 2022)

1.3 Classification of Financial Fraud in Financial Institutions

A systematic categorization of fraud helps financial organizations to establish appropriate internal controls systems, manage risks efficiently, and develop an effective strategy for detecting and preventing fraud based on the unique nature of each type of fraud.

The types of financial fraud in financial institutions can be classified on different grounds. According to the source of the fraud, fraud can be classified into two types. Namely, there is internal fraud that refers to the fraudulent activities performed by employees and external fraud that refers to any fraudulent activities performed by the clients, suppliers, or any other third party. Another type of classification relies on the way the fraudulent acts are

performed by criminals. It may refer to the manipulation of the documentation, the financial records, and even to hacking attempts carried out through cyberspace. The financial instruments that may serve as the object of fraud are another type of classification. They include credit cards, loans, investment tools, and insurance contracts. All of them have specific risks and peculiarities that allow creating a special fraud scheme. The implementation of the classification of financial frauds in financial organizations allows obtaining some major benefits. For instance, due to classification according to the sources, methods, and financial instruments, financial organizations will be able to find patterns of possible fraudulent behaviors, to foresee the potential risks and develop effective internal control measures that depend on the peculiarities of fraud schemes (ACFE, 2022).

The Association of Certified Fraud Examiners among other researchers and professional bodies recognizes the fact that fraud schemes are always evolving due to the adoption of new technologies, organizational development, and development of new financial products. The need to have a classification framework and risk assessment methods that are up-to-date is therefore critical. This will not only help in detecting new fraud schemes but also preventing any potential risks from emerging. When a sound classification scheme is put in place together with efficient risk and monitoring tools, financial organizations can be better placed to fight any form of fraud and ensure their operations are not negatively affected. The evolving nature of fraud schemes makes it necessary for financial institutions to always be vigilant in the identification and prevention of any such schemes (ACFE, 2022).

1.3.1 Internal vs. External Fraud

There are two major types of fraud. First, there is internal fraud, which is any fraudulent or unethical practice carried out by members of the organization such as employees or managers that may abuse their access to internal information or systems for monetary gain. For example, this may include acts like embezzlement, alteration of accounting records, misreporting expenses, or any act of asset manipulation. It is hard to detect as those involved have access to the information needed and understand the controls within the organization. Second, there is external fraud, which occurs when external parties such as customers or suppliers use deception to gain money from the organization. Such acts may include identity theft, payments scams, invoice

manipulation, or any form of cyber-attack on the system. While internal fraud uses the existing authority to perpetrate fraud, external fraud takes advantage of weaknesses in the organizational systems (Arens, Alvin A., Randal J. Elder, and Mark S. Beasley, 16th ed).

Internal fraud: Internal fraud is an instance where people working inside the company indulge in any sort of criminal or unethical activities using their legitimate access to resources or systems. Such activities are committed by people who use the privileges given to them for their own benefit. In other words, such cases of fraud constitute a breach of internal control measures put into place by the organization. Internal frauds can include activities such as fraudulently taking money from the organization or altering accounting documents for the sake of concealing the actual figures.

It is one of the major features of internal fraud that those who commit it have an intricate knowledge of the organization. Such people have knowledge of the organization's internal control measures and they use this to exploit them. Due to this reason, such frauds may take long before being detected. Internal frauds can cause great harm to the organizations and their only possible way of prevention includes good internal controls, segregation of duties, proper auditing processes, and an ethical organizational culture (Kassem, Rasha & Higson, Andrew, 2012).

External fraud: This term is broadly used in the area of financial control, auditing, and risk management, indicating any illegal or fraudulent action performed by individuals or corporations externally and with the purpose of gaining profit through deception. While internal fraud involves acts performed by staff members or individuals already having legitimate access to organizational systems and resources, external frauds are committed by outsiders who intentionally target organizational vulnerabilities. Potential offenders can be clients, contractors, computer hackers, cybercriminal syndicates, or organized fraud rings working nationally or internationally. Modern financial and administrative systems have increasingly encountered threats posed by external fraud because of the technological advances that make it easier to commit offenses. The most common types of external fraud include identity theft, phishing, loan fraud, payment fraud, forgery of financial statements, and insurance fraud. Most of the time, offenders take advantage of the lack of adequate verification, poor cybersecurity practices, or administrative errors in order to commit the offense successfully. As more organizations utilize the internet for their operations and record keeping, the risk of external fraud increases exponentially. From a risk management point of view, the external type of fraud is linked more often to poor prevention practices rather than abuse of authorized access. For example, ineffective

authentication systems, ineffective encryption systems, ignorance among employees, and the absence of surveillance tools are some ways through which external attackers can infiltrate into the company's networks. Thus, dealing with external fraud involves the adoption of both technological measures such as highly advanced cybersecurity technology, anti-fraud AI systems, and multifactor authentication, and organizational measures like staff education.

External fraud is not just a financial problem; it is a legal and regulatory one. Companies that lack an adequate fraud protection system are legally liable to compensate victims who have suffered any losses due to their carelessness. In many countries, regulatory bodies mandate financial companies to take precautionary actions against fraud through the establishment of an effective anti-fraud policy and reporting mechanism. Knowledge of external fraud is important for the formulation of strong internal control systems. This is because it enables organizations to detect weaknesses in their operations, enhance their preventive measures, and establish a strategy for dealing with fraud. Additionally, the differentiation of internal from external fraud is important in establishing liability and conducting the right investigation processes. This is because failure to differentiate the two may result in the adoption of generic internal controls that will be ineffective in addressing the distinct types of fraud. (Mohamed El-Saghir Baali).

1.3.2 Online and Offline Fraud

Given the increasing trend towards digitization of financial services, the categorization of fraud can also be done in terms of whether it is online fraud or offline fraud. In other words, offline fraud refers to instances where fraud occurs via conventional means not reliant on technology. These include but are not limited to forgery, larceny, check forgery, and impersonation in person. While cyber frauds are rapidly becoming more common, offline fraud still exists in financial institutions with poor technological capabilities.

With the continuing digitization of financial services, fraud can also be differentiated depending on the method used to commit fraud, which could either be online or offline fraud. This has become relevant due to the increasing digitization of financial services and the rise in internet banking, mobile banking, and fintech services. Cyber fraud, which may be referred to as online fraud, is any type of crime committed utilizing online tools like websites, internet technology, or other means of accessing the digital environment. Common instances of online fraud include phishing scams to

obtain valuable information, deploying malware, hacking into online bank accounts, and manipulating electronic transactions. Financial institutions have become increasingly vulnerable to cyber-attacks due to the growing sophistication of the technologies involved in digital financial transactions, and hence there is need for more sophisticated protection, real-time monitoring and constant updating of security measures to counter such attacks. Offline fraud involves fraudulent transactions committed through traditional non-internet ways including forging of documents, stealing money, check manipulations, among others. Offline fraud remains a common occurrence despite the growth of online crimes in the financial industry. In fact, most financial organizations are still vulnerable to offline crimes because of lack of adequate resources to implement sophisticated technology. It is worth noting that offline crimes do not require any specialized technology or skills making them very common despite the rise of online frauds. The two classifications make it clear that the financial sector must develop a comprehensive strategy towards combating fraud in order to ensure financial integrity. Financial organizations cannot focus on only implementing technological solutions; rather, they should also consider internal control mechanisms like document examination and segregation of duties to prevent fraud (Kshetri, 2010).

By focusing on both forms of frauds, the sector can be strengthened to avoid any security breaches and threats that may affect financial processes.

1.3.3 Credit Card Fraud vs. Other Financial Frauds

Additional classification is associated with the kind of financial instrument affected by the fraud.

Credit card fraud is one of the most common and widespread types of financial fraud faced by organizations around the world. The fraud takes place when people utilize credit card details through stealing, forgery, or any other means without the authorization of the card owner to make illegal financial transactions. Credit card fraud could take on different shapes. For instance, in card present frauds, perpetrators might either steal cards, clone legitimate cards, or use the point of sale system to access card details. On the other hand, card not present frauds that are more common nowadays because of the increased presence of online shopping occur when criminals purchase goods

via the Internet using stolen credit card details. As a result of the worldwide spread of credit card transactions, there have been significant efforts from banks and other financial institutions to develop fraud detection and prevention technologies. Data analytics and AI algorithms are widely employed by such technologies to identify unusual patterns of activity and fraudulent transactions. Through the analysis of massive volumes of transactional data, it is possible to reduce any potential financial losses or fraudulent activities. (Levi, & Burrows, 2008).

In addition to credit card fraud, there are numerous types of financial frauds, which may prove even more intricate to discover. Loan fraud, insurance fraud, securities fraud, money laundering, and alteration of accounting records all belong to a variety of frauds that are perpetrated against financial institutions. Each type of fraud listed above has its distinct features in terms of investigation, discovery, and preventive measures. For example, loan fraud includes the purposeful provision of inaccurate data for a loan application. Insurance fraud may involve overvaluation of losses incurred as a result of accidents, falsification of evidence, or even staging accidents to claim insurance benefits illegally. As to securities fraud, it is concerned with such activities as market manipulation, insider trading, and deception concerning securities, all of which need to be carefully analyzed in order to detect them. Finally, money laundering is a financial crime that requires elaborate efforts on the part of investigators due to the involvement of complicated financial processes and procedures. Financial institutions should incorporate technological methods, control processes, regulatory compliance, and staff education to counteract basic and advanced forms of fraud. By studying how different fraud schemes operate, financial institutions are able to improve their risk management systems, minimize possible financial loss, and protect their reputation as well as their clients' confidence (Levi & Burrows, 2008).

Understanding the differences between credit card fraud and other financial frauds enables institutions to tailor monitoring systems and regulatory compliance mechanisms accordingly.

1.4 Credit Card Systems and Transaction Lifecycle

Transaction lifecycle refers to all phases of the process, starting from when the cardholder makes a purchase decision and concluding when the amount is settled between the two involved banks.

Credit card systems play an essential part in the financial world today and serve as the backbone for fast and efficient payment processing for customers and businesses alike. They ensure that a considerable number of transactions take place smoothly on a day-to-day basis. An insight into the lifecycle of a credit card transaction is necessary for any financial institution because it will help the institution determine weaknesses that might occur throughout the transaction process, which can then be managed to mitigate risk. The credit card transaction lifecycle includes several steps, including initiation, authorization, clearing, and settlement. Each of these steps comes with its own set of risks, and by carefully analyzing all four, institutions can come up with ways to monitor and detect any anomalies that would make it possible to prevent an unauthorized transaction or detect any errors. The importance of a credit card transaction process goes beyond just making the transaction efficient but helps maintain consumer confidence. If the transaction does not go through, the consumer loses their trust in the product or service being offered. Financial institutions have therefore had to adopt new methods and technologies, including data analytics and artificial intelligence to improve the security of credit card transactions and detect fraudulent activities. In addition, the study of the lifecycle of the credit card transaction process will enable institutions to prepare for future risks and implement appropriate internal controls to address such challenges. With advances in the realm of digital payments and technology in general, criminals keep devising innovative ways of capitalizing on the weaknesses within the systems. As such, a complete comprehension of the credit card transaction process is essential both for risk prevention and strategic purposes (Gomber, Kauffman, Parker & Weber, 2018).

1.4.1 Architecture of Credit Card Systems

The architecture of credit card systems relies on a complicated and highly integrated network of finances and technology to provide a secure, efficient, and standard method of processing payments through electronic transactions. This process does not occur between a single buyer and seller but involves a

number of interrelated parties, such as the card holder, merchant, issuer bank, acquirer bank, and card network operating under the same set of rules (Ray, D. & Singh, S, 2017).

The key to this entire architecture revolves around the cardholder, who refers to the authorized person allowed access to a credit facility by an issuing bank. The cardholder makes use of the credit card to undertake transactions, either manually or electronically, depending upon certain restrictions set forth by the credit card. On the other hand, the merchant is the entity conducting business that processes the payments from customers via payment terminals or gateways.(Kapoor, 2016).

The acquiring bank processes transactions on behalf of the merchant and handles settlement of funds as well as manages merchant accounts and carries some risks. Issuing banks, on the other hand, handle the distribution of credit cards, assessment of credit availability, and determination of fraudulent transactions and approval of transactions. When the transaction is approved, the issuing bank ensures that funds are paid to the acquiring bank while the card owner is expected to repay the money (Summers, 2012).

The various participants are linked via the use of networks such as Visa, MasterCard, and American Express, who offer the technical platform for processing transactions and facilitating worldwide connectivity. The networks have established guidelines on security measures, processes, and interchange fees that govern the operations within the payment network industry(Hunt, 2015).

In order to guarantee the safety and reliability of the electronic payment system, some sophisticated technologies have been incorporated in this process, including encryption, tokenization, and real-time fraud detection systems. The above mentioned technologies play an essential role in securing the transactional information, preventing frauds and security breaches, thus ensuring the credibility of the e-payment systems (Anderson, 2020).

1.4.2 Processing Workflow and Stages

This workflow balances efficiency with security to protect both the cardholder and the merchant. Credit card transactions generally proceed through a structured and sequential process designed to ensure both operational efficiency and financial security. This lifecycle involves several interconnected stages that coordinate communication between the cardholder, merchant, and banking institutions.

1. **Purchase Initiation:** In the initial stages of the purchase process, the holder uses their card details while purchasing something, regardless of whether this is done through a POS system, contactless card technology, or the internet. This stage involves capturing transaction details, including the card number and transaction value.
2. **Authorization Request:** Following the capture of transaction details, the merchant will pass this information to the acquiring bank for authorization by the card company. This information will eventually be sent via the appropriate card network to the issuer in compliance with set standards for transactions.
3. **Authorization Response:** The issuing bank carries out multiple verifications of the card transaction information. This involves determining the validity of the card and checking whether there are enough funds in the card account. Depending on the result of these checks, the issuer accepts or rejects the transaction request.
4. **Transaction Completion:** An approval or rejection message is then sent back to the merchant via the card network, and if accepted, the transaction is completed and the customer gets the products.

On the whole, this transaction flow shows the existence of a well-thought-out mechanism that balances speed, precision, and risk management. The integration of real-time communication systems with fraud detection techniques ensures that the consumers' and merchants' interests are taken into account without undermining the dependability of online payment systems (Zhao & Xie, 2019).

1.4.3 Authorization, Clearing, and Settlement

When a transaction process starts in the credit card network, it undergoes three basic steps of operation, namely authorization, clearing, and settlement. These are the essential components of the modern payment systems that guarantee secure and efficient transaction processing (Bank for International Settlements, 2012)

Authorization is the first and the immediate step in the process of a transaction. It happens in real-time as soon as the user initiates a transaction. During this period, the issuing bank verifies the card validity, checks whether there are adequate funds available, and examines any risks related to fraud

using automatic monitoring tools (European Central Bank, 2022). The outcome of this stage either approves or declines a particular transaction instantly.

The process proceeds into the clearance phase after obtaining authorization. Clearance entails the systematic exchange of transaction details among the acquiring bank and the issuing bank through the card network. During the clearance process, there is a check on the transaction amount, computation of the interchange fee, and record matching between institutions (Bank for International Settlements, 2012). Clearance acts as a necessary verification process that sets up the transaction for the last financial transfer.

Finally, the settlement process is where the funds get transferred from the issuing bank to the acquiring bank. The settlement process entails the payment of the appropriate fees, and then the merchant's account gets credited based on the predetermined settlement schedule (European Central Bank, 2022).

Effective management of authorization, clearing, and settlement processes is crucial for ensuring operational accuracy, reducing systemic risk, and maintaining trust in electronic payment systems (Bank for International Settlements, 2012).

1.5 Credit Card Fraud: Concepts and Types

The issue of credit card fraud presents itself as perhaps one of the most important and rapidly developing problems for modern financial organizations, especially during the period when there is a tendency towards the growth of electronic commerce, online banking, and other types of digital money exchange. Due to the growing number of transactions and the development of payment instruments, there is an increasing need for the continuous improvement of monitoring and controlling measures, which means that it becomes extremely important to have a good understanding of theoretical background and classification principles of this type of fraud (Jain & Ghosh, 2020).

In broader terms, credit card fraud may be defined as any activity that involves the abuse or misuse of a credit card or its related information in a fraudulent manner, aiming at the procurement of goods or services in a way

that the legitimate user of the card is unaware of or does not give his or her consent for.

Fraud methods differ according to sophistication and complexity. Physical fraud involves the theft of cards and/or card cloning, whereas digital fraud involves the use of stolen card details, phishing, and even data breaches. Due to the rise in the number of online activities that involve card use, the increase in fraud incidents can be attributed to their digital nature, hence the need to employ advanced technologies and analytics in identifying and dealing with fraudsters (Jain & Ghosh, 2020).

Overall, conceptual clarity regarding credit card fraud and its various forms provides a foundational basis for understanding risk patterns and developing comprehensive anti-fraud strategies within contemporary financial systems.

1.5.1 Definition of Credit Card Fraud

Credit card fraud can be described as any illegal or fraudulent behavior involving a credit card or any information about that card with the aim of gaining financial benefits illegally. The acts of credit card fraud include various criminal behaviors such as using the actual card, utilizing the counterfeit or stolen data of the card, and even using compromised passwords to conduct fraudulent transactions (Jain & Ghosh, 2020). Credit card fraud not only leads to financial harm to the cardholders and the merchant but may also affect consumer confidence and trust in e-payment systems.

Moreover, credit card fraud is a strategic and deliberate attempt to circumvent existing systems of security checks in payments for personal gain or business purposes. These fraudsters can obtain possession of the credit card directly or even gain indirect access to financial details, which can include details of credit card numbers, their expiry period, their security codes, and even login credentials for online banking portals. As the sphere of digital payments continues to evolve, the techniques used for committing fraud become increasingly complex. This includes techniques like identity theft, phishing, data tampering, and social engineering, among others, which make fraud less dependent upon the physical theft of cards (Jain & Ghosh, 2020).

There are certain factors upon which financial institutions and regulatory bodies categorize credit card fraud. These include the technique that is used to

commit the fraud, the kind of weakness present in the payment system that is taken advantage of by the fraudster, and the specific operations that the fraudster undertakes to accomplish his goal. This classification is critical in creating an efficient risk assessment model and putting measures in place for detecting, controlling, and preventing fraud. Financial institutions may employ various techniques in response to fraud threats. These include using machine learning systems to detect abnormal patterns in transactions, using real-time fraud monitoring tools, or even employing cross-institutional information sharing systems that help avoid repeated cases of fraud (Jain & Ghosh, 2020).

1.5.2 Common Techniques Used in Credit Card Fraud

Credit card fraud can be divided into several types depending on the technique employed by the fraudster. The common ones include:

- **Card-Present Fraud:**

Happens when the fraudster uses the actual credit card at POS or ATM without authorization. Some examples of such fraudulent activities include card theft, card duplication, and skimming that involves using a special device to capture data from a card. It is easy to identify a card present fraud because there are many methods for verifying cards during the transaction process (Button & Cross, 2017).

- **Card-Not-Present Fraud:** This involves any purchase or transaction made without presenting the actual card. Examples include purchasing products online, ordering via the telephone, and automatic billing or subscription to certain services. This type of fraud can be facilitated by using stolen credit card data which may have been collected through phishing or other malware attacks (Kshetri, 2010)

- **Identity Theft:** In identity theft, the fraudster collects personal data for impersonating the card holder and conducting illicit transactions. In identity theft, there is a risk that personal details such as social security number, address, or any other credentials may be stolen for opening accounts or purchasing in the card holder's name (Levi & Burrows, 2008).

- **Account Takeover:** This is a sophisticated type of fraud in which a fraudster takes over a card holder's account. The fraudster is able to alter personal details and conduct unauthorized transactions in the account takeover scenario. This type of fraud usually takes place as a

consequence of phishing scams and security loopholes exploited by the fraudster (Romanosky, 2016).

1.6 Challenges in Detecting Financial and Credit Card Fraud

The process of identifying cases of fraud within the financial sector has become exceedingly hard in the contemporary world especially when it comes to identifying credit card fraud. This is mainly because of the fast increase in electronic commerce, mobile banking, and online transactions which have made it hard for organizations to differentiate between genuine and fraudulent transactions in real time. In addition to that, fraudsters always develop new ways through which they can be able to circumvent traditional methods of security by applying new technologies (Phua, Lee, Smith, & Gayler, 2010).

The issues in the detection of fraud are more than just technical; they have also got to do with the organizational aspect. The first thing is that, technologically, organizations have to deal with huge amounts of data, deal with the fact that there will be imbalance data since the number of frauds is usually very small compared to the number of total transactions, and reduce false positives which might affect legit clients.

In other words, the success of the fraud detection process lies in striking a balance between the need for accurate results, efficiency, and morality. Banking organizations should be involved in implementing sophisticated algorithms but maintaining the integrity of the process (Phua, 2010).

1.6.1 Data Imbalance and Concept Drift

One of the biggest problems that arise while trying to detect credit card fraud is the problem of data imbalance since fraudulent transactions represent a tiny fraction of the whole data set consisting of transactions. This can be a problem for any algorithm because usually, the algorithm is built around the majority class, meaning that it works best with normal transactions. (Ngai, 2011).

Concept drift is another important issue faced by organizations while detecting frauds. The term concept drift implies a constant and changing nature of frauds that emerge in an organization. Scammers always change their tactics to bypass the detection measures in place, and hence detection measures need regular updating and upgrading to detect frauds effectively. These two important issues, data imbalance and concept drift, imply that

traditional detection methods may not be sufficient enough and may need advanced techniques like anomaly detection and adaptive systems (Ngai, Hu, Wong, Chen, & Sun, 2011). (Ngai, 2011).

1.6.2 Real-Time Detection Constraints

Fraud detection in credit card usage in real-time poses quite a few difficulties mainly because of the huge amount of transactional data that needs to be processed at once. One such challenge faced by organizations is maintaining an optimum balance between speed and precision because too many false positives – legitimate transactions being flagged as fraudulent – will affect the user experience negatively. In contrast, too many false negatives – when a fraudulent transaction goes unnoticed – can lead to losses for the organization (West & Bhattacharya, 2016).

To deal with these issues, financial organizations are turning to advanced computing technology, which provides scalability, high performance, and streaming analysis. Advanced computing makes it possible to monitor transaction flows continuously, recognize patterns in real time, and make decisions quickly. All these factors become crucial when processing large amounts of data in online shopping portals and digital banking systems (West & Bhattacharya, 2016).

This balance between computational efficiency and detection effectiveness remains a central constraint in designing real-time fraud prevention systems, requiring constant optimization of algorithms, data pipelines, and monitoring frameworks.

1.6.3 Privacy, Security, and Ethical Issues

Detection of fraud in credit cards normally requires the analysis of extremely sensitive personal and financial data. Utilization of personal data raises several privacy and security concerns. The organization must make sure that its data protection policy complies with the regulations of GDPR or any other privacy law applicable in the area. Besides legal concerns, ethical challenges emerge during the implementation of fraud detection technology. In case the models used are poorly designed and discriminatory, there might be instances where some of the clients are discriminated against or treated unfairly. The best course of action here would be for organizations to adopt a fraud

detection system that is transparent in its decisions and easy to comprehend. This system is crucial in instilling trust among clients. (Bromiley & Cummings, 2019).

1.7 Economic and Financial Impacts of Fraud

There are many ways that financial fraud can have an effect on different parties, not just those involved but the whole economy. There could be significant financial damage, operational disruption, and a lack of trust among investors and customers. Economic impacts from financial fraud are diverse and include direct expenses such as theft of money or chargebacks, as well as indirect expenses like higher transaction fees, higher insurance premiums, and greater costs for risk management and monitoring. Knowledge about the above effects helps financial institutions to put in place effective antifraud methods by focusing their efforts and investments on those parts of operations which are exposed to high risks of fraud. Moreover, government institutions and authorities require cost assessment in order to develop an effective regulatory framework that will protect the stability of the financial market. Through evaluation of the cost of fraud, policymakers are able to adopt an evidence-based approach to reducing the risks of fraudulent activities in the financial industry (Button, Johnston, Frimpong, & Taylor, 2020).

1.7.1 Financial and Institutional Losses

Fraud leads to substantial financial loss to banks, credit card companies, and other financial organizations. The direct costs include the amount that is lost through fraudulent transactions, charge-backs, and expenses incurred in reclaiming the money defrauded from the organization, while indirect costs include expenses spent in implementing new anti-fraud technologies, training staff, and hiring lawyers. Apart from financial consequences, reputations can be tarnished, which can lead to a decline in customer trust, adverse effects on stock prices, and diminished market share. Organizations that repeatedly face fraudulent events often have no other choice but to initiate expensive corrective measures, thereby adding more weight to their already heavy workload. The cumulative impact of all types of losses reinforces the significance of preventive measures against fraud for financial organizations (Levi & Burrows, 2008).

1.7.2 Consequences for Customers and Market Confidence

The effect of fraud is felt directly and through various means by consumers, as it is often characterized by the occurrence of illegal transactions, identity theft, and disturbances in normal financial dealings. These may be very disruptive and create significant distress for the individuals involved even if they receive compensation from the bank. Apart from the direct losses incurred as a result of fraud, the psychological implications such as anxiety, frustration, and mistrust in the banking processes, both electronic and conventional, can be very severe. Consumers will likely be unwilling to utilize some payment methods and avoid using the Internet to conduct financial business. From a macroeconomic point of view, instances of fraud may lead to a significant erosion of confidence within financial markets. The perception may arise that the financial industry is susceptible to fraud and lacks adequate measures to prevent such incidences from occurring. Such perception may result in reduced investments and an escalation in capital costs. Additionally, concerns regarding repeated fraud incidences may necessitate compliance measures by regulators and the implementation of stringent oversight frameworks that are likely to be costly. It is therefore imperative that efforts be made to retain the confidence of customers in the prevention of fraud incidents to foster efficiency in financial markets (Romanosky, 2016).

1.7.3 Legal and Regulatory Implications

The problem of financial fraud involves serious legal and regulatory consequences for both parties that commit crimes and organizations where these crimes are committed. The government, regulatory agencies, use different methods of punishment and penalties to prevent such actions, provide safety for consumers, and preserve the stability of the financial system. The compliance system includes such laws as anti-money laundering (AML), know-your-customer (KYC), and other payment systems' regulations that give the clear vision of how the transaction should be controlled and monitored. If financial institutions do not follow certain rules set by law and regulations, they will receive some financial punishments, as well as lose good reputation, and will suffer under close control from supervising organizations. These reasons along with possible direct financial losses make it crucial to create and follow specific measures that prevent the fraud. It is

obvious that fraud risk management requires following different aspects related to laws and regulations in order to avoid penalties and be sure that everything is going right (Phua, Lee, Smith, & Gayler, 2010).

Conclusion

This chapter was all about an extensive analysis of financial frauds and transactions using credit cards from both theoretical and practical perspectives. Financial fraud was defined, its major features described, and the motives and players in financial fraud explained. Knowing this basic information is of primary importance to have an idea of what kind of financial fraud looks like nowadays.

Also included in our discussion is the classification of financial frauds as internal or external, electronic or not, and related to credit card or not. With these different classifications, it becomes easier for financial institutions to establish the proper detection and preventive measures to be undertaken.

Credit card systems along with their transaction life cycle were looked at, covering their design, flow of transactions, and phases of authorization, clearing, and settlement. This information is critical, for it reveals the mechanisms of fraud and the technical and procedural weak points where fraud can be committed.

Also, credit card fraud was examined thoroughly, from card-present fraud to card-not-present fraud and identity theft or account takeover. The problems of fraud detection, including data imbalance, concept drift, limitations of real-time fraud detection, and issues regarding privacy and security, were outlined as well.

Finally, the consequences of fraud related to economy and finance were discussed, revealing that this type of crime does not only affect the finances of the institutions involved in the crime directly, but can also have an effect on customer confidence and financial markets.

To summarize, it should be said that in this chapter, financial and credit card fraud has been analyzed as a complicated phenomenon, and in order to combat fraud, there is need for effective measures that will include both technological and regulatory actions, as well as monitoring and customer awareness.

Chapter 2

Theoretical

Foundations of

Financial Fraud

Detection: From

Classical Approaches

to Machine Learning

Methods

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

1.1 Introduction

Financial fraud is one of the most significant issues facing today's banking systems due to the fast pace at which technology and digitization evolve, making fraudsters develop sophisticated strategies. It is necessary not only to prevent financial organizations from financial losses but also to preserve the trust of consumers and ensure the sustainability of the financial system as a whole.

The conventional methods include rule-based and statistical approaches that require a certain set of rules and patterns to be pre-established for fraud detection. Though they offer some basic level of security and are relatively simple to deploy, they often fail to adapt to novel ways of committing fraud and work with large datasets. This restricts their effectiveness in monitoring current financial activities.

Machine learning is a promising approach that relies on historical data to discover complex non-linear relationships and latent connections between features. These algorithms improve prediction accuracy continuously and allow analyzing vast amounts of financial transactions in real time.

The current chapter delves into the theories surrounding financial fraud detection techniques, taking into account the classic approach and the machine learning techniques. Additionally, other important aspects such as data preparation and model evaluation are also highlighted alongside the ethics and legality surrounding the same. The discussion serves as the platform from which the next chapter can proceed, as it mainly focuses on the implementation of machine learning models to detect frauds.

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

1.2 Classical Statistical Techniques

In the absence of machine learning algorithms, traditional fraud detection frameworks were built on classical statistics and rule-based models. They form the basis of present-day fraud detection frameworks and continue to be employed in some cases because of their ease of understanding and application.(West& Bhattacharya, 2016).

1.2.1 Rule-Based Systems (Expert Systems)

Rule-based systems, which are also referred to as expert systems, are among the most traditional types of anti-fraud solutions. In this type of fraud detection system, domain experts develop a set of fraud-related rules that can be easily represented using if–then statements (e.g., if the transaction is higher than a specific limit, classify the transaction as fraudulent). There are many positive features of rule-based anti-fraud systems. First, such systems are highly transparent and easy to interpret. Second, they are computationally inexpensive and can be easily deployed in real-time applications. At the same time, there are multiple drawbacks to rule-based anti-fraud systems. The primary limitation of such systems is their rigidity and non-adaptability to new situations. As a result, fraudsters can simply learn and adapt to existing fraud detection rules. Moreover, such systems produce a high number of false positives, which renders them inefficient in complex environments.(Wang, & Xu, 2018)

1.2.2 Statistical Hypothesis Testing

Conventional methods of fraud detection in statistical analysis revolve around hypothesis testing, whereby the core notion is to identify the extent to which a certain transaction differs significantly from normal user behavior. This conventional process involves comparing each transaction to a baseline data set of previous legitimate transactions. The degree of difference will indicate any suspicious activity that could be considered fraud.(Nigrini, 2012).

1.2.2.1 Z-Score/Standard Deviation Method

Z-score is perhaps the most common statistical technique employed in detecting anomalies. It quantifies the distance of a transaction's value from the

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

average value of all past transactions conducted by a particular user, expressed in terms of standard deviations. A transaction is flagged as abnormal if the Z-score value's absolute magnitude exceeds a predetermined constant k , usually between 2 and 3. This means that a transaction value is flagged if it lies outside the range of values within two or three standard deviations of the average. This technique is easy to implement and computationally efficient. Nevertheless, it relies on the assumption that the underlying population data is normally distributed and is therefore highly sensitive to outliers. Furthermore, it cannot detect complex patterns of fraud that exist beyond statistical anomalies.(Aggarwal, 2017)

1.2.2.2 Benford's Law

Another statistical model employed in fraud detection is Benford's Law, which relies on the empirical finding that in most naturally occurring data sets, the distribution of leading digits tends to be non-uniform, meaning that digits tend to occur more often as leading digits the smaller they are. Thus, for example, digit one occurs as the leading digit in roughly 30% of data instances, whereas digits like nine tend to occur much less often.As an anomaly detector, the law is employed to reveal manipulations and inconsistencies in data sets. Namely, when the distribution of leading digits in a given data set differs significantly from the Benford distribution, the deviation suggests data falsification. While useful in revealing anomalies in large data sets that do not require labeling, Benford's Law is applicable only to certain types of data and performs poorly for others. In addition, if fraudsters know about this statistical test, they will be able to adjust their data accordingly.(Rauch, Götsche,Brähler, & Engel, 2011)

1.3Challenges of Traditional Fraud Detection Methods

The traditional methods of fraud detection have been becoming increasingly inadequate in modern times owing to certain limitations. For instance, rules cannot detect new methods of fraud since they can only be able to detect fraud that has been predetermined. Furthermore, audit procedures require a lot of time and effort because they require human intervention in reviewing the financial transactions; there is a chance of human error, which may result in fraud going unnoticed. In addition, statistics are becoming unable to handle big data owing to the increasing use of online transactions in detecting any

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

changes or new methods of conducting fraud. As such, traditional methods have become increasingly inadequate in detecting fraud in modern times where there is an increase in both volume and sophistication of fraud methods. The traditional methods of fraud detection have been playing a significant role in helping organizations guard themselves against fraud in the past (bello, Ogundipe, Mohammed, Folorunso, & Alonge, 2023).

Such approaches often include rule-based systems, human review processes, and basic statistical approaches to keep track of transactions and spot any patterns that might suggest suspicious activity. Rule-based systems operate based on pre-set parameters that will help them determine whether a particular transaction is suspicious or fraudulent. For example, a purchase made by a credit card exceeding a certain amount or conducted from a strange geographical location can easily trigger an automatic review process.

The addition of manual reviews to automated detection systems ensures that human analysts are involved in evaluating the flagged transactions. The identity of the customers is confirmed, and the customers are contacted to ascertain the authenticity of any suspicious transaction, while past trends are evaluated for inconsistencies. While manual reviews help increase accuracy, they are generally laborious and difficult to scale in the context of high-volume transactions. Traditional methods used for fraud detection include the use of simple statistics to establish whether there are deviations from the norm. Common techniques include using outlier detection, Z-score, and standard deviation to detect anomalies in the transactions, which might be linked to fraud. Scoring algorithms can also be used to assign a risk score to every transaction, where high-risk scores lead to transactions being flagged for further evaluation. Though these traditional approaches have benefits, they are not effective when dealing with complicated, dynamic, and voluminous data. Consequently, more innovative and adaptable approaches have been adopted, such as machine learning-based fraud detection models, which are discussed in the following sections (bello, Ogundipe, Mohammed, Folorunso, & Alonge, 2023).

1.4 Machine Learning in Fraud Detection

1.4.1 Introduction to Machine Learning and Its Role in Fraud Detection

Machine Learning techniques have become a major driving force behind the identification of financial frauds, allowing these programs to discover trends in complex datasets that make up transactions. Unlike traditional techniques,

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

machine learning algorithms allow these systems to remain flexible and continue adapting as new methods of committing fraud arise as they learn from the incoming data constantly. Such flexibility is essential in today's fast-paced world with huge amounts of transaction records where detecting fraud through traditional means can be difficult, making machine learning models ideal choices to use for such purposes.

1.4.1.1 Definition and Core Principles of Machine Learning

Machine learning is part of artificial intelligence, which is included within the broader scope of deep learning. The core idea here is to offer data to a machine for learning, and once new data similar to the training data is offered, the machine can classify them. To put it formally, machine learning can be said to be an instance of artificial intelligence using certain technologies to make use of an existing data base in order to offer meaningful responses. Data will be analyzed and the necessary models generated. Once questions are asked of the models, they will offer answers based on the data given.

Machine learning, a notable branch of artificial intelligence, is one of the most significant technologies developed during this decade. Many businesses now rely on machine learning as a means of enhancing the level of service and efficiency. In essence, machine learning combines multiple computational algorithms and statistical models that allow systems to perform tasks without being programmed. Models learn from past or "training" data; therefore, they are capable of identifying trends and connections. Once trained, these models will be able to make predictions or decisions based on data that has been learned.(Raghavan & El Gayar, 2019).

1.4.1.2 Types of Machine Learning

There exist different types of machine learning that can be used in detecting fraud. For example, supervised learning makes use of labeled data to train the model to make predictions. In this case, the model would be trained to detect fraudulent transactions. On the other hand, unsupervised learning involves using unlabeled data to discover patterns and anomalies within the data. As such, it helps in identifying new schemes of fraud. Lastly, reinforcement learning is based on feedback from the model that learns by making choices based on rewards.

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

Machine learning (ML) is one of the core components of artificial intelligence, which allows the system to learn from data without any explicit programmatic rules being used for the process.(Kevin P. Murphy, 2012).

Instead of following a set of pre-written rules, ML algorithms draw information from the data itself, making forecasts, finding patterns, and making decisions. Thus, thanks to the ability to learn, ML is especially suitable for dynamic environments, like financial transactions, where large numbers of events occur that require new behavior models (Stuart Russell & Peter Norvig, 2020).

There are three main types of ML methods, depending on the way learning is done:

1. Supervised Learning (SL):

The supervised learning model makes use of labeled datasets, where the input sample is linked with its output label. The main aim here is to develop a mapping function that predicts output labels for new inputs. In finance, supervised learning is widely used in classification and regression problems, such as distinguishing between fraudulent and non-fraudulent transactions and calculating credit risks. With the help of labeled data samples, these models learn general patterns and become highly accurate predictors(Russell& Norvig, 2020).

2. Unsupervised Learning (UL):

The use of unsupervised learning is related to the analysis of unlabeled data to discover hidden structures or patterns without having any prior knowledge of the outcomes. The focus is not on prediction but instead analyzing the natural structure of the data through means of clustering, dimensionality reduction, and anomaly detection. The use of unsupervised learning for fraud detection is particularly important in discovering unusual patterns within transactions that deviate from standard expectations (Russell& Norvig, 2020).

3. Reinforcement Learning (RL):

In reinforcement learning, an agent interacts with an environment to learn how to achieve its objectives through a series of experiments involving

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

reward mechanisms. The idea is to make choices that maximize the total amount of rewards received at any one time, thereby improving decision-making strategies constantly. In financial systems, reinforcement learning can aid in decision-making processes like optimizing fraud thresholds based on changing circumstances (Murphy, 2012).

Generally, these are some of the basic paradigms underlying the current intelligent systems. Machine learning approaches enable analysts to model future scenarios, discover hidden structures in data sets, and optimize their decision-making capabilities.

1.4.1.3 Relationship between Machine Learning and Financial Analysis

The significance of machine learning cannot be overstated in the field of finance. It is particularly valuable in terms of detecting any type of financial fraud. Machine learning helps improve prediction as models can evaluate past data and current transactional information to accurately predict the outcomes, and it does so better than any other method of prediction. Machine learning also provides a means of anomaly detection which helps to detect any suspicious behavior in real-time, and hence it can identify the possibility of fraud occurring.

Lastly, machine learning algorithms help financial institutions make fast and accurate risk assessments using financial information. With its computing power, machine learning makes it possible for financial institutions to estimate risk levels in advance and thus take appropriate action to counter the risks.

The connection between machine learning and financial analysis is intrinsically complimentary because machine learning can greatly improve upon the methods used by conventional financial analysis. Traditionally, financial analysis has been based on the use of financial ratios, statistics, and intuition. These methods were sufficient in their time, but the rising levels of financial information have made them increasingly ineffective (Khandani, Kim & Lo, 2010).

One of the strengths of machine learning is that it can be used to develop sophisticated techniques that will aid in analyzing huge amounts of data in an

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

efficient manner and identifying intricate relationships that exist between variables, as well as improving the precision of predictions made by the model. This technology is widely utilized when conducting credit risks analysis, fraud detection, and financial forecasting, thus facilitating better decision-making by organizations. Machine learning supplements classical finance in terms of analyzing complex patterns in financial data (Khandani, Kim& Lo, 2010).

1.5 Machine Learning Algorithms in Fraud Detection

Today, machine learning algorithms have been established as the backbone of modern-day fraud detection solutions, offering the capability to process large amounts of transaction data in an automatic fashion. Machine learning algorithms are particularly suited to discover complicated patterns within the dataset, categorize each transaction individually, and discover outliers that could point to suspicious behavior. Based on the nature of the data set, the sophistication of the patterns involved, and the interpretability of the algorithm itself, there are unique benefits associated with each algorithm.

1.5.1 Commonly Used Algorithms in Fraud Detection

Machine learning algorithms are commonly used in fraud detection because they have the capability to learn from data and adapt according to different transaction patterns. Every machine learning algorithm has distinct features which enable them to be used effectively in certain fraud detection applications.

Logistic regression is an easy to understand and interpret algorithm that provides an estimated probability of fraudulent transactions. It is a common method used in fraud detection since it is a simple but effective way of doing fraud detection for the first time or creating a baseline. Decision trees and random forest algorithms are very flexible models that can easily capture complex interactions of input variables and provide efficient results in heterogeneous data.

Support vector machines have the capability to separate transactions which are fraudulent from those that are not, especially in non-linear datasets. Neuralnetworkalgorithms are specifically created to detect sophisticated patterns of fraud, especially in large datasets.

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

Unsupervised learning methods such as clustering have an added advantage in identifying anomalies since they form clusters of similar transactions while isolating outliers that may be associated with fraud or suspicious activity.

Overall, the application of machine learning algorithms in fraud detection not only boosts accuracy but also ensures increased efficiency in the process of transaction fraud detection.

ML provides a data-based solution to several shortcomings associated with traditional approaches used in detecting fraud. Machine learning algorithms make use of large amounts of complex data in order to recognize hidden patterns, adapt to changing trends, and continually improve their performance. Such capabilities make machine learning algorithms ideally suited to detecting financial fraud.

When detecting financial frauds, there is a wide range of machine learning techniques that are used for this purpose. Traditional approaches like logistic regression, decision tree analysis, random forest method, and SVM are often used alongside new technologies such as deep learning algorithms. Each approach comes with its own benefits, making it possible for organizations to improve their ability to detect fraud and respond to it(Hossain, Raja, & Hasan, 2023).

Table1 machine learning in fraud detction

Sn	Methods	Descriptions	Gaps in TraditionalApproaches
1	LogisticRegression	Logistic regression is a fundamental machine learning technique, extensively utilized in financial fraud detection owing to its interpretability and straightforward implementation. This statistical model forecasts the likelihood of a binary outcome (fraud versus non-fraud) utilizing input features, including financial ratios and governance variables. Research conducted by(Dechow, 2011) and (Perols, 2011) identified logistic regression as an effective baseline technique for	Although machine learning methodologies exhibit considerable promise in fraud detection, numerous research deficiencies persist. Many studies prioritize enhancing model accuracy while neglecting interpretability, which is essential for practical

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

		identifying earnings manipulation and financial misstatements. Notwithstanding its popularity, logistic regression is constrained by its presumption of a linear correlation between independent variables and the outcome, which may not be applicable in intricate fraud scenarios.	applications in auditing and regulatory environments. The issue of class imbalance, wherein fraudulent cases constitute merely a minor portion of the dataset, remains a significant challenge. Numerous machine learning models encounter difficulties in identifying infrequent fraud instances, resulting in elevated rates of false negatives(Phua, 2010). Many current studies depend on historical datasets that may not encompass emerging fraud schemes, thereby constraining the generalizability of these models.
2	DecisionTrees	Decision trees represent a widely utilized machine learning method in fraud detection. They categorize instances by recursively partitioning data into subsets according to the most informative attributes, thereby forming a tree-like structure. Decision trees possess high interpretability, rendering them appealing to auditors and regulators who require comprehension of the rationale behind the model's predictions. (Kirkos, 2007)Utilized decision trees to identify financial statement fraud in Greek corporations, yielding encouraging outcomes. Decision trees, particularly in intricate datasets with numerous features, are susceptible to overfitting, which can diminish their generalizability(Ngai, 2011).	
3	RandomForests	Random forests mitigate the overfitting issue inherent in decision trees by generating multiple trees from varied data subsets and averaging their predictions. Random forests exhibit resilience and demonstrate effective performance across diverse contexts, including fraud detection. (Perols, 2011)Conducted a comparison of various machine learning algorithms and determined that random	

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

		forests surpassed other models in identifying financial statement fraud, exhibiting reduced false-positive rates. Random forests effectively manage high-dimensional data, rendering them appropriate for extensive datasets with numerous features. Nonetheless, akin to decision trees, they may pose interpretative challenges, especially when numerous trees are included(Breiman, 2001).	
4	Support Vector Machines (SVM)	Support vector machines (SVM) are a prevalent machine learning algorithm utilized in fraud detection. Support Vector Machines endeavor to identify the hyperplane that optimally distinguishes between fraudulent and non-fraudulent instances within a multidimensional space. A notable advantage of SVMs is their capacity to manage high-dimensional datasets, rendering them particularly appropriate for intricate financial data(Cecchini, 2010)demonstrated that SVMs are effective in detecting financial misstatements, especially when integrated with feature selection techniques. Nonetheless, SVMs may require significant computational resources and offer reduced interpretability compared to more straightforward models like decision trees and logistic regression(Phua, 2010).	
5	Neural Networks and Deep Learning	In recent years, neural networks and deep learning models have garnered attention for their capacity to identify financial statement fraud. Neural networks, especially deep learning models, comprise	

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

		numerous layers of neurons capable of modeling intricate relationships between input features and outcomes. These models are proficient in identifying non-linear patterns within extensive datasets, rendering them exceptionally effective in uncovering intricate fraud schemes(Zhou, & Kapoor, 2011). Deep learning models are frequently regarded as "black boxes" due to their limited interpretability, posing a considerable disadvantage for auditors and regulators who require insight into the reasoning behind the model's predictions (Molnar, 2019) .The application of deep learning in fraud detection remains relatively novel, with limited research comprehensively investigating its potential. Researchers, including(Kogias, 2020), have utilized convolutional neural networks (CNNs) and recurrent neural networks (RNNs) on time-series financial data, yielding promising outcomes. These models can identify temporal patterns in financial statements, enabling the detection of fraud that develops over time. However, the absence of interpretability and the requirement for extensive, high-quality labeled datasets continue to pose substantial obstacles to the broad implementation of deep learning in fraud detection .	
6	HybridModels	Recent studies have concentrated on creating hybrid models that integrate various machine learning methodologies to enhance precision and minimize false	

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

		positives.(Chen, & Wu, 2020)Introduced a hybrid model that combines logistic regression with decision trees and random forests. This method utilizes the interpretability of logistic regression alongside the predictive efficacy of ensemble models, providing a more resilient solution for financial fraud detection. Hybrid models integrating supervised and unsupervised learning techniques have been investigated to identify both known and unknown fraud patterns(Ngai, 2011).
--	--	---

Table x reproduced from Hossain, Raja, and Hasan (2023).

1.5.2 Preprocessing Financial Data before Applying Algorithms

In addition, there are some crucial aspects to consider prior to the application of fraud detection algorithms. First and foremost, a financial dataset should be thoroughly preprocessed before implementing any machine learning techniques. Cleaning is the very first stage, which includes the elimination of irrelevant data, duplicates, and erroneous records, which might affect the functioning of the algorithm.

Second, feature engineering aims at creating new meaningful variables out of the raw data. These variables allow the models to detect hidden relationships and patterns, contributing to the enhanced efficiency of fraud detection.

Third, since the amount of fraudulent transactions in financial datasets is much smaller than the number of regular ones, a model faces the problem of imbalance. Therefore, in order to make the model able to recognize minority-class instances properly, one has to conduct oversampling, under sampling, or combine these two techniques.

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

Lastly, normalization and standardization should be performed as the final stage. It ensures that all variables are scaled similarly and not affected by others because of their bigger values.

In conclusion, the preprocessing stage is vital for improving the performance and effectiveness of machine learning algorithms.

Data preprocessing represents a crucial preliminary step in applying machine learning algorithms for financial fraud detection. Financial datasets often contain missing values, duplicate records, inconsistencies, and irrelevant or noisy attributes, all of which can adversely affect the performance of predictive models if not properly addressed. Therefore, thorough data cleaning is essential to ensure the accuracy, consistency, and reliability of the input data, forming a solid foundation for subsequent modeling (Dal Pozzolo, Caelen, Johnson. & Bontempi, 2018).

Feature engineering is another essential part of preprocessing, which deals with converting raw financial data into useful features capable of revealing important trends and patterns. Good features will improve the capacity of ML algorithms to learn and will help them discover sophisticated fraud patterns.

A problem that is frequently encountered in financial fraud datasets is the presence of extreme class imbalance. Due to the fact that cases of fraud constitute a very small percentage of all data points, models tend to focus on the majority class and fail to properly recognize fraudulent actions. One way of addressing the class imbalance problem is by applying sampling techniques.

Moreover, normalization and standardization processes are essential to ensure consistency in the scale at which all features are measured. Without such procedures, variables that have larger values may have a significant impact on the training process, hence reducing the quality of the model. In summary, efficient data preprocessing procedures will improve the effectiveness of ML models, boost prediction accuracy, and ultimately strengthen the entire financial fraud detection process (Dal Pozzolo, Caelen, Johnson. & Bontempi, 2018).

1.6 Model Evaluation Metrics

1.6.1 Methods for Evaluating Model Performance

Evaluation of the fraud detection models is important to ensure that the model is effective in detecting and monitoring any suspicious transactions. Some of the performance metrics used include accuracy, which refers to the correctness of the model in determining whether a transaction is suspicious or not. Precision refers to the ratio of correctly classified fraudulent transactions as fraudulent. This metric indicates the extent of reduction of false positives by the model. Recall, or the sensitivity measure, indicates the effectiveness of the model in classifying any fraudulent transaction as such. The F1-score incorporates both precision and recall measures.

The Area Under Curve – Receiver Operating Characteristic graph indicates the discriminative capability of the model in distinguishing suspicious and normal transactions. The Confusion Matrix includes true positive, true negative, false positive, and false negatives, and it gives an overview of how the model behaves during classification.

Verification is another strategy used to verify the effectiveness and reliability of fraud detection models. The two main methods of verification are the use of data splitting to compare test results with those of training data and using cross validation.

In fraud detection in the financial sector, datasets show extreme imbalances since the number of fraudulent cases constitutes a small portion of the whole dataset. In such circumstances, traditional measures like accuracy tend to be meaningless and unreliable because they will give high ratings regardless of whether the minority cases have been well predicted by the model or not. Thus, when evaluating fraud detection models, the focus should be on how the model detects frauds (Moutia, 2025).

The Precision (P) is defined as a share of all transactions classified as fraud out of total fraudulent transactions. It shows the ability of the fraud detection algorithm to avoid false positives. The second metric that should be used is called Recall (R). This term also refers to Sensitivity and means the ratio of correct detection of fraudulent cases out of the whole group of actual frauds. F1-score (F1) is the harmonic average of both Precision and Recall and therefore demonstrates an appropriate balance between the two aspects.

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

Moreover, there is the area under ROC curve (AUC-ROC) that estimates the discriminating ability of the algorithm at various thresholds of decisions.

Among those four metrics, F1-score and AUC-ROC are the most meaningful in terms of measuring performance of the fraud detection system in case of severe imbalance of the dataset. Those two metrics can be called most complete, since they allow evaluating how effectively a system detects a minority class and, thus, provide a full idea about the algorithm performance. As a result, it is important to use such criteria of assessment (Moutia, 2025).

1.7 Ethical and Legal Considerations in Using Machine Learning

The advent of machine learning in the financial industry has revolutionized many areas such as risk assessments and fraud detections where institutions can use their data sets to predict future events. On the other hand, the use of machine learning in the financial sector poses a lot of ethical and regulatory issues. For example, using historic information to train a model could lead to biased decisions and discrimination.

This issue becomes problematic when using machine learning algorithms in automating procedures that require human judgment, like credit scores and risk assessment. Therefore, institutions should incorporate ethical frameworks and develop interpretable models to address the problem mentioned above.

In fraud detection problems in finance, there is an obvious problem of imbalanced datasets where the number of fraud cases is very small compared to the rest of the dataset. In such instances, traditional methods of measuring accuracy can be misleading since the metrics may show high performance while the model is not able to detect the frauds. Hence, it is critical in such cases to use metrics that measure how well the model detects the fraud cases (Moutia, 2025).

Precision (P) indicates how well the model is able to identify truly fraudulent transactions among all transactions classified as fraudulent. It reflects the effectiveness of the model in avoiding type I errors, or false positives. Recall (R) is also called sensitivity and is an indicator of the portion of fraudulent transactions detected by the model, demonstrating its efficiency in identifying real instances of fraud. F1-score (F1) is the arithmetic mean between precision and recall. It reflects the balance between type I and type II errors

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

and can give a more detailed understanding of the performance of the model. The other metric to consider is AUC-ROC. Out of all the measures discussed above, the F1-score and AUC-ROC are usually viewed as the most revealing and representative performance metrics of a model's robustness in a highly imbalanced dataset. These measures give an overall picture of how a model performs, guaranteeing that a financial institution is capable of recognizing any form of fraud while not flagging any normal transactions. The emphasis on detecting the minority class is important in the creation of fraud detection systems (Moutia, 2025).

1.8 Comparative Analysis: Classical vs. Machine Learning Approaches

Traditional techniques of fraud detection, which include rule-based systems and conventional statistics, have long been used by financial institutions with the benefit of being transparent and easily deployable. The decision mechanism used in these techniques is typically comprehensible, enabling the expert to comprehend the reasoning behind the classification of a particular transaction as suspicious. Furthermore, the computational requirements of these systems are comparatively low, making them applicable to limited data sets. Nevertheless, traditional techniques suffer from a number of disadvantages when used in contemporary financial settings. In particular, traditional methods tend to be inflexible, incapable of adjusting dynamically to the constantly evolving nature of fraud patterns. As a result, they cannot handle voluminous data sets adequately and hence are constrained in identifying complicated fraud patterns.

On the other hand, machine learning algorithms provide a more complex and adaptable solution to detect fraudulent activity. Such solutions can learn automatically based on historical information, identify trends, and adapt to new types of fraud. Machine learning algorithms such as ensembles, neural networks, and gradient boosting can establish non-linear relationships among different features, allowing for improved performance even in extremely imbalanced datasets. In addition, machine learning algorithms have scalability, making them able to process large amounts of data in near real-time, which is not possible with classical solutions.

Nevertheless, machine learning algorithms pose new challenges that financial organizations need to address. For example, they require

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

considerable pre-processing of input data and feature engineering to achieve acceptable performance, consume significant computing resources during training, and present ethical and legal issues regarding algorithmic biases, explain ability, and accountability. Therefore, financial institutions should carefully evaluate the potential of machine learning-based solutions and determine whether they will be able to provide accurate and efficient results within acceptable limits of ethical and legal considerations (Ngai, Hu, Wong, Chen & Sun, 2011).

Chapter 2 Theoretical Foundations of Financial Fraud Detection: From Classical Approaches to Machine Learning Methods

1.9 Conclusion

In Chapter 2, a thorough analysis of the theoretical basis behind the detection of financial fraud has been discussed. The chapter initially focused on the classical approach in fraud detection. Classical approaches involve rule-based models and conventional statistics. It highlighted the strengths of the classical approach by mentioning its interpretation capability, ease of understanding, and implementation. However, the chapter mentioned the weaknesses of the classical approach by citing its inflexibility and incapability to adjust to new trends in fraud schemes. Further, the chapter discussed the importance of using machine learning algorithms in detecting financial fraud. Machine learning algorithms were chosen since they have the capability to analyze large amounts of transaction data. They were also noted to be adaptable to newly emerging fraud strategies and effective in improving fraud detection efficiency. Moreover, the chapter briefly described the ethics and laws surrounding the use of machine learning algorithms in fraud detection.

In addition, the chapter included a comparative analysis of the classical and machine learning approach. While classical models have advantages in terms of their interpretability and low computational complexity, machine learning algorithms are more scalable, accurate, and faster than classical approaches.

In conclusion, this chapter is successful in presenting a solid theoretical basis, which is important in setting up the groundwork needed in the next chapter, namely the methodology chapter. It will serve as a base from where the practical aspects of implementing the models in detecting fraud can be evaluated.

Chapter 3
Practical
Implementation of a
Credit Card Fraud
Detecting System
Using Machine
Learning

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

1.1 Introduction:

This chapter, we provide the practical implementation of the financial fraud detection system using machine learning. This research aims to build and test predictive models able to distinguish between fraudulent and legal financial transactions.

Modern financial systems process millions of financial transactions worldwide every day. Credit and debit cards, together with digital payments, have become key tools used in modern commerce and replaced cash payments in most countries around the world. But this revolution brought another problem - financial frauds. As stated by(Nilson, 2023), in 2022, card fraud losses around the world were higher than 33 billion dollars and it is expected that they will be more than 43 billion dollars by 2026. Furthermore, financial institutions face an additional loss of 3.75 USD to fight each 1 dollar of fraud losses due to various costs associated with investigating fraud, recovering from clients, and complying with regulations.

With the growth in digital transactions, the identification of any malicious activity has emerged as an important task. It should be noted that the problem is further worsened due to the presence of imbalance among the data of a financial dataset, wherein fraudulent transactions constitute a mere fraction of the whole dataset.

Existing fraud detection approaches employ a pre-specified threshold for identifying any fraudulent transactions and also include patterns like detecting high transaction amounts and suspect geographical locations. While these rule-based approaches are quite effective in detecting straightforward frauds, they suffer from significant drawbacks, including a high frequency of false alarms and limited flexibility towards the changing landscape of fraud.

Machine learning provides a sophisticated approach for solving this problem, which involves direct learning of patterns and relationships in the historical data without any preconceived ideas. This research work aims at analyzing ensemble machine learning algorithms that comprise the use of six different classifiers for the credit card fraud detection problem.

In this chapter, various machine learning techniques will be used on an actual dataset. This process entails data preparation, training of models, and evaluation of their performance using suitable evaluation metrics. In conclusion, the results obtained from each technique are examined and compared to determine which method is best for detecting fraud.

Problem Statement:

This study addresses three interconnected challenges:

Challenge 1: Accurate Fraud Classification. Given a financial transaction described by 29 numerical features (28 PCA-encrypted variables and 1 transaction amount), classify it as either Authentic (Class 0) or Fraudulent (Class 1) with high precision and recall.

Challenge 2: The Unstructured-to-Structured Gap. Real-world fraud detection must process diverse input formats– scanned invoices, PDF receipts, digital documents. However, machine learning models require structured numerical input.

- How can a system accept an unstructured PDF document and feed it into tabular ML models trained on anonymized PCA features?

Challenge 3: Model Reliability. No single machine learning algorithm is universally optimal. Different classifiers have different strengths and weaknesses depending on the data distribution.

- How can multiple models be combined to produce a more reliable prediction than any individual model?

❖ Objectives:

1. The primary objectives of this study are:
2. Train and evaluate six machine learning models on a real-world credit card fraud dataset using rigorous cross-validation methodology.
3. Design and implement the Simulation Bridge architecture that accepts PDF document uploads, extracts financial information, and maps it to the ML feature space.
4. Build an ensemble inference system that runs all six models simultaneously and determines the final verdict through majority voting.
5. Develop a professional full-stack web application with a backend API for ML inference and a frontend dashboard for user interaction, demonstrating that the system is deployable as a real product.
6. Document and analyze the results to compare model performance and validate the ensemble approach.

❖ Scope and Limitations:

In Scope:

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

- Binary classification (Authentic vs. Fraudulent)- Six supervised learning algorithms
- Ensemble majority voting- PDF document processing Full-stack web application Known Limitations:
- The PCA features (V1-V28) in the dataset are pre anonymized; the system cannot learn from raw transaction attributes such as merchant name, card type, or geographic location.
- The Simulation Bridge maps PDF amounts onto random dataset rows, meaning the PCA features are not causally related to the extracted amount. This is a deliberate simulation for demonstration purposes.
- The system operates on static, pre-trained models. It does not implement online learning or model retraining on new data.

2. Literature Review

2.1Credit Card Fraud: A Global Challenge

Credit card fraud encompasses a range of criminal activities including stolen card usage, card-not-present (CNP) fraud in online transactions, account takeover, and identity theft. The (European Central Bank, 2022)reported that CNP fraud accounts for over 80% of the total card fraud value in the European Economic Area, driven by the growth of e-commerce. The challenge of fraud detection lies in its adversarial nature: fraudsters continuously adapt their techniques to evade detection systems. This creates an arms race between detection technology and criminal innovation.(Bolton& Hand, 2002)Identified this as a fundamental characteristic that distinguishes fraud detection from other classification problems– the data distribution is non-stationary and shifts as fraudsters learn to circumvent existing defenses.

2.2Traditional Fraud Detection Methods:

Before machine learning, fraud detection relied primarily on: Rule-Based Systems: Expert-defined rules such as “block transactions exceeding \$5,000 from a new device” or “flag multiple transactions within 5 minutes.” These systems are transparent and easy to implement but rigid, generating high false positive rates and unable to detect novel fraud patterns (Kou, Lu, Sirwongwattana, & Huang, 2004).

Statistical Methods: Techniques such as logistic regression and Bayesian networks were among the first quantitative approaches. (Maes.TuylsVanschoenwinkel & Manderick, 2002)Demonstrated that Bayesian networks could model the probabilistic relationships between

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

transaction features and fraud likelihood, outperforming simple rule-based systems.

Expert Systems: Knowledge-based systems encoding domain expertise from fraud analysts. While effective for known fraud types, they require continuous manual updating and cannot generalize to unseen patterns (Leonard, 1995).

2.2.1 Rule-Based System (Threshold-Based Detection):

In the practical implementation, the rule-based system can be expressed as a simple decision rule: If $x_i > T \Rightarrow$ Fraudulent Transaction

Where:

- x_i : transaction amount
- T : predefined threshold value

Practical interpretation:

Any transaction whose amount exceeds a defined threshold is automatically flagged as potentially fraudulent. This rule is directly applied to the transaction dataset as a baseline filtering mechanism.

2.2.2 Z-Score Method (Standard Deviation Approach):

2.2.2.1 Z-Score Method Definition

The Z-Score method is an approach used in statistics to identify anomalies by calculating the distance between a transaction and the mean value of the data set in standard deviations. The Z-score is computed as follows: $Z = \frac{x - \mu}{\sigma}$

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

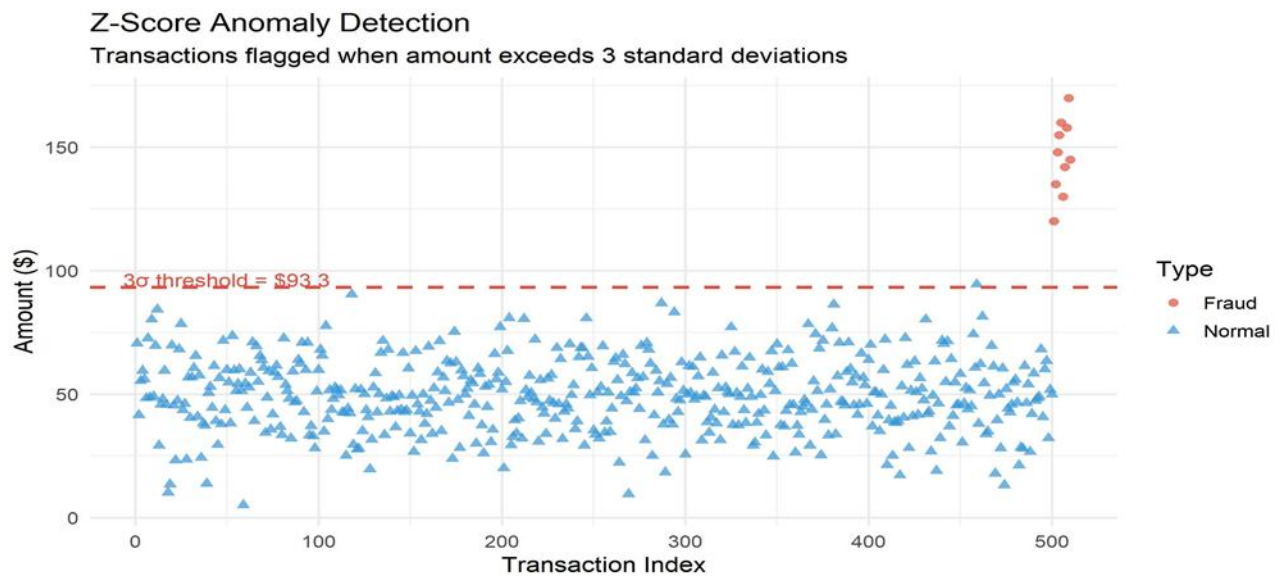


Figure 1Z-Score Flagging: Transactions beyond 3σ are flagged as anomalies

Where:

- x : transaction value
- μ : mean of past transactions
- σ : standard deviation

Decision rule:

$|Z| > k \Rightarrow \text{Anomalous Transaction}$

Where k is typically set to 2 or 3.

Practical interpretation:

In the implementation phase, each transaction is standardized using the Z-score formula. Transactions that exceed the defined threshold are flagged as anomalies and considered potentially fraudulent.

2.2.2.2 Figure Analysis

This graph demonstrates the use of the Z-score approach in finding outliers or abnormal transaction based on their sizes. Based on this diagram, most transactions (in blue points) occur normally or in line with average values, suggesting that the transaction process is stable. The distribution is centered around the mean and lies below the line of threshold. A line representing a

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

threshold with 3 standard deviations (about \$93.3) is denoted in red dashes. This line serves as a benchmark in identifying outliers.

The transactions exceeding the line threshold (in red points) are easily differentiated from others, which suggests that the values are highly unusual and should be investigated further for any possible fraud cases. Based on the diagram, it can be concluded that there are several points of interest:

- The majority of transactions follow a regular pattern of occurrence.
- There are some transactions that diverge from the normative pattern.
- Z-score can identify outliers and can be helpful in detecting anomalies in transaction processes.

It should be noted that while this approach helps identify abnormal transactions through their sizes, it cannot detect fraud schemes.

2.2.3 Benford's Law:

2.2.3.1 *Method Description*

Benford's Law is a statistical principle that describes the expected distribution of leading digits in naturally occurring numerical datasets. According to this law, smaller digits appear more frequently as the leading digit. The theoretical probability of a leading digit is defined as:

$$P(d) = \log_{10}(1 + \frac{1}{d})$$

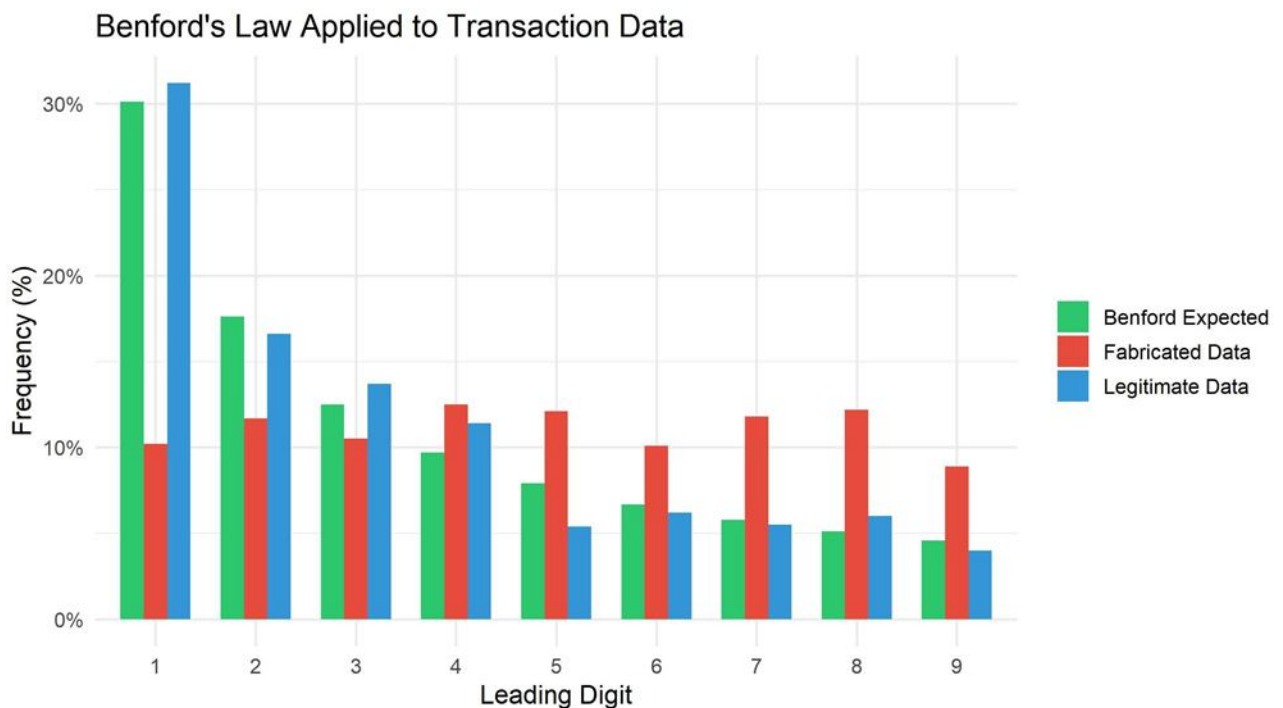


Figure 2 Benford's Law: Fraudulent data often deviates from the expected leading-digit distribution

Where:

- $d \in \{1, 2, \dots, 9\}$

Practical interpretation :

In the dataset, the first digit of each transaction amount is extracted and its empirical distribution is compared with the expected Benford distribution. Significant deviations from this pattern may indicate possible manipulation or fraudulent activity.

2.2.3.2 Figure Analysis

This figure shows three different distributions of the Benford distribution (expected, green), legitimate distribution (blue), and fabricated distribution (red). One can observe that the legitimate transactions follow the expected distribution according to the Benford distribution law and, specifically, for digits 1, 2, and 3 have high frequency occurrences. At the same time, the distribution of fabricated numbers does not follow the Benford distribution but rather is characterized by irregular frequencies without the presence of a

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

consistent decline from the lowest frequencies at the start to higher ones at the end.

Some significant observations include:

- Firstly, digit 1 occurs most frequently in both types of distributions as required by Benford's Law.
- Secondly, legitimate data decreases monotonically from digit 1 until digit 9.
- Thirdly, the fabricated distribution deviates strongly from the expected distribution.
- Fourthly, inconsistencies in frequency levels indicate anomalies.

This proves the usefulness of Benford's law in detecting fraudulent patterns in financial data. Nonetheless, one can conclude that applying this test would yield better results on large-scale data sets rather than limited ones.

2.3 Machine Learning Approaches in Fraud Detection

The application of machine learning to fraud detection has been extensively studied:

Logistic Regression: remains a strong baseline for binary classification. Its probabilistic output provides interpretable confidence scores, and its linear decision boundary is computationally efficient. (Whitrow, Hand, Juszczak, Weston & Adams, 2009) Showed that logistic regression with appropriate feature engineering achieves competitive performance on fraud datasets.

Decision Trees and Random Forests. (Breiman, 2001) Introduced Random Forests as an ensemble of decision trees trained on bootstrap samples. For fraud detection, (Bhattacharyya, Jha, Tharakunnel & Westland, 2011) Demonstrated that Random Forests consistently outperform individual decision trees and logistic regression, achieving higher AUC scores on credit card datasets.

Support Vector Machines (SVM) seek the hyperplane that maximizes the margin between classes. For fraud detection, the RBF kernel allows SVM to capture non-linear decision boundaries. However, training complexity of $O(n^2)$ to $O(n^3)$ limits scalability to large datasets (Chen, Chiu, Huang & Chen, 2006). Gradient Boosting builds an ensemble of weak learners (typically decision trees) sequentially, where each new tree corrects the errors of the previous ensemble. (Friedman, 2001) introduced the gradient boosting framework, and subsequent implementations like XGBoost (Chen & Guestrin,

2016) and HistGradientBoosting(Ke, Meng, Finley, Wang, Chen, Ma, Ye & Liu, 2017) have achieved state-of-the-art results on tabular data across Kaggle competitions and academic benchmarks.

XGBoost specifically has been the most successful algorithm on structured/tabular data in competitive machine learning. (Chen & Guestrin, 2016) Introduced regularization terms in the objective function that prevent overfitting, making it particularly effective for imbalanced fraud datasets

2.4 Class Imbalance Problem in Fraud Detection

Fraud detection datasets are inherently imbalanced— fraudulent transactions typically represent less than 1% of total transactions. Standard classifiers trained on imbalanced data tend to predict the majority class (Authentic) almost exclusively, achieving high overall accuracy but near-zero recall for the minority class (Fraudulent). SMOTE (Synthetic Minority Over-sampling Technique), introduced by (Chawla, Bowyer, Hall & Kegelmeyer, 2002), addresses this by generating synthetic minority class samples through interpolation between existing minority instances. For each minority sample, SMOTE identifies its k nearest neighbors, selects one at random, and creates a new sample along the line segment connecting them in feature space. Additional strategies include:

- Class weight adjustment: Assigning higher misclassification penalties to the minority class (used in this study via `class weight='balanced'`).
- Under sampling the majority class: Removing majority samples to balance the dataset. This risks losing information.
- Cost-sensitive learning: Modifying the loss function to account for asymmetric misclassification costs.

This study uses both SMOTE and class weight balancing as complementary strategies.

2.5 PCA in Financial Data Privacy

The dataset used in this study contains features V1 through V28, which are the result of Principal Component Analysis (PCA) transformation applied to the original transaction attributes. PCA is a dimensionality reduction technique that transforms correlated features into orthogonal principal components ordered by variance explained. In the context of financial data, PCA serves a dual purpose:

1. **Privacy protection:** The original features (merchant name, card number, location, time, etc.) cannot be recovered from the PCA-transformed features, protecting cardholder privacy.
2. **Dimensionality reduction:** PCA captures the most informative directions of variance in fewer dimensions than the original feature space. (Dal Pozzolo, 2015). Published the original credit card fraud dataset using this PCA anonymization approach, which has since become the standard benchmark for fraud detection research.

2.6 Synthesis of Contemporary Research

Recent academic work on credit card fraud detection has mainly focused on three directions: classifier performance, handling class imbalance, and advanced boosting techniques.

2.6.1. Performance of Standard Classifiers

Many researchers compare and analyze the performance of traditional machine learning approaches in fraud detection.

In their comparative analysis, (Sravan, Kiran . Srinivasa, Rao Naini Sudeepthi, Anuhya Srestha, Sangars Vontary, and 2 more, 2024) Used various classifiers such as Naive Bayes, K-Nearest Neighbors, Logistic Regression, Support Vector Machine, Decision Tree, and Random Forest. It is noted that among the presented approaches, Random Forest demonstrates the highest accuracy equal to 94.98%. Nonetheless, the authors do not analyze hybrid or ensemble approaches.

(Singh,& Maheshwari, 2022) Compare different models of algorithms such as Logistic Regression, Naive Bayes, Random Forest, KNN, SVM, Gradient Boosting, and Neural Networks. The conclusion can be drawn about the effectiveness of machine learning methods in the case of fraud detection; however, there is no comprehensive performance metrics analysis.

Another system developed by (Prateeksha M, Swetha & Patil, 2023) uses Decision Tree, Logistic Regression, and Artificial Neural Networks. It is indicated that accuracy increases significantly during the implementation of the feature selection step; however, the comparison is limited because of the few algorithms used in the paper.

2.6.2. Smote-Based Approaches

A substantial amount of research revolves around the issue of class imbalance in fraud detection datasets.

According to (Varmedja, Karanovic, Sladojevic, Arsenovic, & Anderla, 2019), a framework consisting of Logistic Regression, Random Forest, Naive Bayes and Multilayer Perceptron, along with SMOTE balancing approach, exhibited excellent performance; however, the paper mainly focused on the use of preprocessing techniques.

Another research paper, from the MIPRO Conference in 2019(2019), utilized SMOTE and Random Forest techniques, SVM, and Logistic Regression with an addition of incremental learning methods in order to address evolving cases of fraud. Again, the evaluation of the models' performance was based on such metrics as precision and recall; yet, no other methods were considered.

Another study conducted by (Varmedja, Karanovic, Sladojevic, Arsenovic, & Anderla, 2019)corroborated these results and demonstrated that SMOTE helps to improve detection accuracy, although it does not eliminate the need for further models' development.

(Maithili, Kumar, Rengarajan, Murthy, & Nagamani, 2023)Addressed anomaly detection methods and techniques aimed at solving the issue of class imbalance. As a result, weighted models demonstrated higher efficiency, although their usage remained theoretical.

2.6.3. Boosting and Hybrid Approaches

Current studies have shown a growing interest in boosting techniques and hybrids for their high forecasting efficiency.

According to(Singh,& Maheshwari, 2022), XGBoost is far superior to others with a prediction accuracy rate of 99.87%. Nonetheless, the paper considered only one parameter, namely, accuracy, and did not take into account such aspects as recall rate or F1-score.

In a paper from (2024), researchers used such models as Random Forest, Logistic Regression, Decision Tree, and XGBoost to identify fraud. All four techniques proved themselves effective, but no leader was identified.

(Baba, Sharma, Kumar, Shahi, Srivastava, & Dhaliwal, , 2023)Explored both supervised and unsupervised learning methods as well as the need for real-

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

time fraud detection systems. Nevertheless, there were no practical examples presented in the paper.

2.7Comparative Analysis of Previous Studies

In this part, I have summarized and compared the main contributions of some recently published works on the detection of credit card frauds in terms of their methodologies, advantages, and drawbacks. The work done by(Sravan, Kiran . Srinivasa, Rao Naini Sudeepthi, Anuhya Srestha, Sangars Vontary, and 2 more, 2024)was related to evaluating various machine learning models for detecting fraudulent activities, including the following techniques: Naive Bayes, K-Nearest Neighbors, Logistic Regression, Support Vector Machine, Decision Tree, and Random Forest. The outcomes of the study demonstrated that the accuracy of Random Forest model was significantly higher (94.98%) than others. Nevertheless, this work did not examine the hybridization of models.

Like Sravan's research, the contribution done by (Singh,& Maheshwari, 2022)is also related to analyzing various machine learning algorithms. The findings demonstrated that XGBoost algorithm performed much better than other methods since its accuracy reached 99.87%. Nonetheless, this research did not consider other metrics for evaluating models' effectiveness except for accuracy.

(Varmedja, Karanovic, Sladojevic, Arsenovic & Anderla, 2019)solved the issue of class imbalance through the use of SMOTE and various models including logistic regression, random forest, naive bayes, and multilayer perceptron. The results indicated better performance through these models; however, data processing was the center of attention in this research.

The paper presented at MIPRO conference (2019) made use of similar techniques such as SMOTE and random forest along with SVM and logistic regression. The researchers incorporated incremental learning schemes for dealing with fraud detection problems and measured performance based on precision and recall. However, they did not employ boosting schemes.

A paper published in (2024)employed various machine learning models such as random forest, logistic regression, decision tree, and xgboost for detecting fraud. Though the algorithms were found effective, yet no conclusive results about the best model among them were reported.

(Baba, Sharma, Kumar, Shahi, Srivastava, & Dhaliwal, , 2023) Investigated the application of both supervised and unsupervised learning methods, with a focus on real-time fraud detection systems, their research stayed within the theoretical framework, lacking experimentation.

In the end, (Maithili, Kumar, Rengarajan, Murthy, & Nagamani, 2023) conducted a literature review concerning ML-based fraud detection approaches, noting that the most efficient are those using anomaly detection and weighted models. While better performance was achieved using the weighted product model, this approach was also mostly theoretical.

2.7.1 Summary Insight

In general, the comparison demonstrates that:

- Ensemble classifiers like Random Forest and XGBoost usually outshine conventional classifiers.
- SMOTE is commonly employed for solving class imbalances without utilizing any sophisticated modeling methods.
- Accuracy is more important than other evaluation metrics.
- Fraud detection solutions still lack implementation in practical scenarios.

2.8 Research Gap and Problem Statement

Despite the high accuracy reported in recent literature, a significant "implementation gap" remains. The majority of existing research is **model-centric**, focusing on optimizing algorithms in controlled, offline environments using static datasets (e.g., Kaggle).

There is a noticeable lack of **system-centric** research that addresses:

1. **Practical Deployment:** How these models integrate into a functional, user-facing application.
2. **Real-world Utility:** The transition from a code-based script to a platform that financial analysts or end-users can interact with.
3. **Comprehensive Metrics:** Moving beyond simple accuracy to evaluate systems based on their operational viability.

This thesis aims to bridge this gap by developing a holistic fraud detection system that prioritizes not only predictive performance but also practical deployment and user accessibility.

3. Method

3.1 Research Approach:

This study follows a design science research methodology, proceeding through the following phases:

1. **Problem identification:** Understanding the fraud detection challenge and its requirements.
2. **Solution design:** Designing the Simulation Bridge architecture and selecting ML models.
3. **Implementation:** Building the complete system (training pipeline, API, frontend).
4. **Evaluation:** Measuring model performance through cross-validation and analyzing ensemble behavior.
5. **Communication:** Documenting findings in this report.

3.2 System Design Overview

The system is designed to handle uploaded PDF documents by extracting the relevant transaction details, mainly the transaction amount, using text extraction techniques. Since the dataset used in this study contains anonymized features (V1–V28), which cannot be directly retrieved from real-world documents, the system relies on representative data from the existing dataset to complete the required input structure.

In practice, a transaction is selected from the dataset, and its feature values are combined with the transaction amount extracted from the uploaded document. This approach allows the system to construct a complete and compatible input for the fraud detection process, while ensuring that the data remains consistent and suitable for analysis.

3.3System Architecture :

3.2.1 The Simulation Bridge Architecture

The central technical contribution of this study is the Simulation Bridge– a method that enables structured tabular ML models to operate within an unstructured document processing pipeline. The challenge: ML models are trained on a 29-dimensional feature vector (V1 V28 + Amount), where V1-V28 are PCA-encrypted features that cannot be extracted from any PDF document. Only the Amount can be obtained from invoice text. The solution: When a PDF is uploaded, the system:

1. extracts the transaction amount from the document text using regex pattern matching.
2. Samples a random row from the original dataset (568,630 rows), which provides realistic PCAfeature values from an actual transaction.
3. Replaces the Amount column in the sampled row with the value extracted from the PDF.
4. Drops the id and Class columns to produce the final 29-dimensional feature vector.

This creates a valid input for the ML models where:

- V1-V28 come from a real transaction in the dataset (providing realistic feature distributions).
- Amount comes from the uploaded PDF document (providing the user's input).

Rationale: The Amount feature interacts with the PCA features during inference. A high amount combined with certain PCA patterns might trigger fraud detection, while the same amount with different PCA patterns might not. This creates natural variance in predictions across repeated uploads of the same document– a characteristic that mirrors the inherent uncertainty in real fraud detection systems.

3.3.2 High-Level Architecture

The system follows a three-tier architecture:

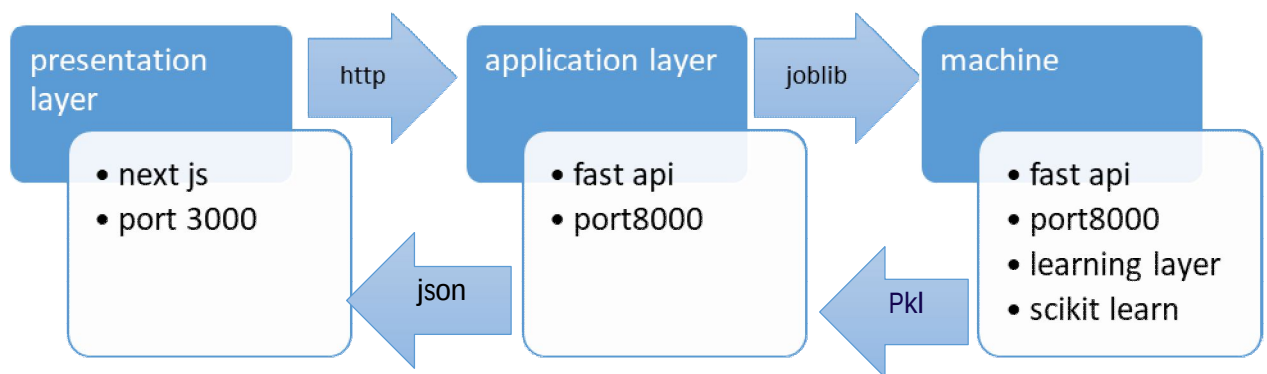


Figure 3 illustrates the system structure

Presentation Layer (Frontend): Handles user interaction, file upload, loading animations, and results display. Communicates with the Application Layer via HTTP REST calls.

Application Layer (Backend): Receives PDF uploads, orchestrates the Simulation Bridge pipeline, runs ML inference, and returns structured JSON responses. Manages model lifecycle (loading at startup, inference on request). **Machine Learning Layer:** Pre-trained model artifacts (.pkl files) loaded into memory. Performs feature transformation (scaling) and prediction (classification + probability estimation).

3.3.3 Backend Architecture (FastAPI)

In this study, I selected FastAPI for the backend because it is simple to use and provides good performance. One of its main advantages is its support for asynchronous processing, which allows the system to handle file uploads and data processing efficiently without blocking other operations.

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

Another important feature is the automatic API documentation through Swagger at the /docs endpoint. FastAPI also integrates with Pydantic, ensuring proper validation and structure of input and output data.

The backend is based on two main endpoints. The first one, POST /analyze-document, is used to receive PDF files and process them for fraud detection. The second one, GET /health, is used to check the system status.

When the system starts, the trained models, scaler, and dataset are loaded into memory. This improves performance by avoiding repeated loading for each request. During execution, each request follows a simple process where the PDF is processed, the relevant information is extracted, the input features are prepared, and a prediction result is returned.

3.3.4Frontend Overview

The front end is a single-page web application built using Next.js, which provides an interactive website that allows users to upload files and view results in a simple and organised manner. The system operates according to a workflow based on three main states: IDLE, LOADING and RESULTS. In the first two states the upload area appears and the user can select a file. During the third state, the system processes the request.

Finally, the analysis results are clearly displayed in the RESULTS state. This process ensures a smooth and seamless user experience allowing the user to carry out a sequence of steps from uploading the document to viewing the final results.

3.3.5Data Flow Process

The data flow process in this system begins when a PDF file is uploaded via the website. The file is then sent from the front end to the back end for processing.

The document is read in the background and relevant information is extracted from it. The system then prepares the input data by combining the extracted data with the required attributes from the dataset.

Trained models then process these inputs and generate a prediction using a majority voting method. Finally, the result is sent back to the front end and presented to the user in a clear and organised manner.

3.3.5.1 Data Flow Pipeline

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

The complete data flow from user action to result display: Step 1: User drops PDF onto UploadDropzone component

Step 2: Frontend creates FormData, POSTs to /analyze-document

Step 3: Frontend simultaneously starts Loading Sequence animation

Step 4: Backend receives multipart upload, saves to temp file

Step 5: pdfplumber extracts text from first page

Step 6: Regex searches for monetary amount pattern

Step 7: If found: use extracted amount. If not: random \$10-\$500

Step 8: Sample 1 random row from 568,630-row DataFrame

Step 9: Drop 'id' and 'Class' columns from sampled row

Step 10: Overwrite 'Amount' column with extracted value

Step 11: For Logistic Regression and SVM: apply StandardScaler

Step 12: Run all 6 models: predict () and predict_proba()

Step 13: Calculate majority vote from 6 binary predictions

Step 14: Serialize response as JSON via Pydantic

Step 15: Frontend receives JSON response

Step 16: After animation completes: transition to RESULTS state

Step 17: Render ResultsDashboard with ModelCards and Verdict Bann

3.6.Data Collection

Name: credit card fraud detection dataset 2023

Source: kaggle<https://www.kaggle.com/datasets/nelgiriyeewithana/credit-card-fraud-detection-dataset-2023>

Doi citation : <https://doi.org/10.34740/kaggle/dsv/6492730>

Author: NidulaElgiriyeewithana

Size: 568,630 transactions

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

In this study, we used the ‘Credit Card Fraud Detection Dataset’ compiled by European cardholders in 2023 which comprises over 550,000 records. The dataset has been anonymised to protect the cardholders’ identities the data has been processed to ensure an even distribution across categories .The data has been processed to ensure an even distribution across categories which ensures greater effectiveness when training the classification algorithm and avoids the problem of false prediction accuracy resulting from data imbalance.

Table 1description of dataset features for credit card fraud detection

Feature	Type	Range	Description
id	Integer	0 to 568,629	Unique row identifier (dropped before use)
V1- V28	Float	Varies (~-30 to ~30)	PCA-transformedanonymizedfeatures
Amount	Float	0.00 to ~25,691	Transaction amount in dollars
Class	Integer	0 or 1	0 = Authentic, 1 = Fraudulent

The dataset is balanced at source (approximately 50/50 split between classes), which is unusual for real-world fraud datasets. However, to demonstrate the SMOTE methodology and maintain consistency with standard fraud detection practices, SMOTE is still applied during training.

3.7.Data Preprocessing

The preprocessing pipeline consists of:

- Column removal: The id column is dropped as it is a monotonically increasing integer with no predictive value. Including it would introduce a spurious correlation between row index and fraud label.
- Feature-target separation: The remaining 29 columns (V1-V28 + Amount) form the feature matrix X. The Class column forms the target vector y.
- No missing value handling required: The dataset contains zero null values across all columns.
- No encoding required: All features are already numerical (continuous floats).

3.8.Model Training Pipeline

In this study, a model training workflow was designed to prepare and train several machine learning models for fraud detection. The process begins by loading the dataset and removing unnecessary columns such as the transaction ID the input features are then sorted against the target variable, which indicates whether a transaction is fraudulent or not. To address the issue of class imbalance, the SMOTE technique was applied to create a more balanced dataset. The features were then scaled to ensure that all variables are on a similar scale, which helps improve model performance. Based on the pre-processing stage several machine learning models were trained on the processed data, including logistic regression, random forest, decision tree, support vector machine, gradient boosting and XGBoost. Each model was trained separately and stored for later use in the system. The process concluded with the storage of both the trained models and the measurement tool as files so that they can be easily loaded during the system's predictive phase.

3.9Model Descriptions

Logistic Regression:remains a strong baseline for binary classification. Its probabilistic output provides interpretable confidence scores, and its linear decision boundary is computationally efficient. (Whitrow, Hand, Juszczak, Weston& Adams, 2009) Showed that logistic regression with appropriate feature engineering achieves competitive performance on fraud datasets.

Decision Trees and Random Forests: (Breiman, 2001)introduced Random Forests as an ensemble of decision trees trained on bootstrap samples. For fraud detection, (Bhattacharyya, Jha. Tharakunnel & Westland, 2011) Demonstrated that Random Forests consistently outperform individual decision trees and logistic regression, achieving higher AUC scores on credit card datasets.

Support Vector Machines (SVM): seek the hyperplane that maximizes the margin between classes. For fraud detection, the RBF kernel allows SVM to capture non-linear decision boundaries. However, training complexity of $O(n^2)$ to $O(n^3)$ limits scalability to large datasets(Chen, Chiu, Huang& Chen, 2006).

Gradient Boosting builds: an ensemble of weak learners (typically decision trees) sequentially, where each new tree corrects the errors of the previous ensemble. (Friedman, 2001)introduced the gradient boosting framework, and

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

sub sequent implementations like XG Boost(Chen& Guestrin, 2016) and HistGradient Boosting(Ke, Meng, Finley, Wang,Chen, Ma, Ye& Liu, 2017) have achieved state-of-the-art results on tabular data across Kaggle competitions and academic benchmarks.

XGBoost: specifically has been the most successful algorithm on structured/tabular data in competitive machine learning.(Chen & Guestrin, 2016) Introduced regularization terms in the objective function that prevent overfitting, making it particularly effective for imbalanced fraud datasets.

3.10.Backend API Implementation

The system's backend was developed using FastAPI, which is responsible for processing requests from the website's frontend and handling uploaded PDF files.As soon as the system starts up, it begins loading the required assets into memory, including the dataset, the measurement tool and all the trained machine learning models. This helps to enhance performance by avoiding repeated loading operations with every request. The main function of the backend is to receive the PDF file uploaded from the website, parse it and extract the relevant information from it; the system then prepares the input data and sends it to the machine learning models for prediction. Once the models have produced their results, the system aggregates the results and makes the final decision; this result is then returned to the website's front end in a structured JSON format to be presented to the user.

3.11.PDF Processing

This part of the study focused on extracting useful information from the uploaded PDF files. The primary objective was to obtain the transaction amount, given its significant importance in the fraud detection process.

At the beginning, the programme reads the PDF document and extracts the text content from it; when the text becomes usable a simplified method is applied to find the amount inside the text. The total amount is often written at the end of the file so the final value detected is considered to be the final transaction amount; this is then used as input for the next step in the programme.

3.12.Frontend Implementation

The website's front end has been developed using Next.js to provide a clear well-organised user interface that is responsive. The design focuses on

guiding the user through the various steps of the process from document upload to the presentation of results. The interface revolves around a logical flow that mirrors how the platform works. It starts with the file upload step followed by the processing stage and concludes with the analysis results being displayed. The structure ensures that users can easily track the progress of their task without any confusion. Special attention has been paid to ease of use and interaction quality. The interface is designed to be intuitive, enabling users to efficiently interact with the system without the need for technical knowledge.

This helps to create a user experience that is both smoother and more effective.

4. System implementation.

4.1 Technology Stack.

The technologies used in this programme have been carefully selected to ensure high performance and ease of development. FastAPI was chosen for the backend due to its speed, lightness and ease of use. Next.js was used to build the frontend as it allows for the creation of modern, interactive web interfaces.

As for design and animation, both Tailwind CSS and Framer Motion were used to enhance the user experience. Regarding the machine learning component, both Scikit-Learn and XGBoost were chosen as they are suitable for tabular data and are commonly used in fraud detection scenarios.

To extract text from PDF files, pdf plumber was used due to its ability to handle structured documents effectively. Finally, Joblib was used to save and load trained models efficiently.

4.2 System Evaluation

4.2.1 Functional Evaluation of the System

The system was evaluated on the basis of its ability to successfully perform the required core functions. It enables users to upload PDF documents via the website, process the data inputs, and extract all relevant information necessary for detecting cases of fraud.

Once the document has been processed, the system uses machine learning models to generate a final prediction, presenting the result to the user in a clear and organised format upon completion of the process. Overall, the

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

system demonstrates a sound and seamless workflow from the input stage through to the output stage.

4.2.2 Model Performance Overview

All the machine learning models used in this study have been successfully trained and tested on the dataset. Each model contributes differently to the final prediction depending on the learning approach it employs. Tree-based models, such as Random Forest, Gradient Boosting and XGBoost, performed well, which was to be expected given the structured nature of financial data. Logistic regression also produced consistent results, suggesting that the dataset contains valuable patterns that can be captured even by the simplest models.

Overall, these models performed well and are suitable for integration into a fraud detection system.

4.2.3 Ensemble Analysis

To enhance the reliability of forecasts, a majority voting approach has been adopted. This method combines the outputs of all models and selects the final decision based on the most common forecast.

This approach helps to minimise the impact of errors from individual models; where the models agree, the system produces a robust and reliable decision, whilst in more challenging cases, the voting mechanism balances the differences between the models and produces a clear, definitive result.

4.2.4 System Performance (Descriptive Analysis):

The system operates effectively during real-time use. It process documents that are uploaded within reasonable time and displays results without any significant delay. There is a stable and smooth interaction between the front-end and back-end, providing an excellent user experience.

This allows the system to retain a fast response speed during operation and provide consistent results for various inputs.

5. Result and analysis

5.1Model Training Results

All six models were successfully trained and serialized. The training pipeline produced the following output files:

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

Table 2 Model Training Results

Model	File Size	Training Time	Preprocessing
LogisticRegression	~0.1 MB	~5s	StandardScaler
Random Forest	~150 MB	~60s	None
DecisionTree	~0.1 MB	~2s	None
SVM	~30 MB	~120s	StandardScaler+50k subsample
Gradient Boosting	~2 MB	~30s	None
XGBoost	~5 MB	~90s	None
StandardScaler	~0.1 MB	~3s	N/A

Total model storage: approximately 190 MB.

5.2 Cross-Validation Performance

All models in the initial Kaggle notebook were evaluated based on their performance using the 5-fold stratified cross validation approach for SMOTE resampling data. Different evaluation metrics were used in order to conduct a holistic evaluation of the model performances.

Accuracy is the measure of total accuracy in transaction classification – whether it is fraud or not.

Precision refers to the fraction of predicted fraudulent transactions that are indeed fraudulent and helps minimize false positives.

Recall is the percentage of actually fraudulent transactions detected by the model; thus, the number of false negatives is minimized here.

Finally, **F1-Score** can be considered as the harmonic mean of the aforementioned measures.

Table 3 Comparative Cross-Validation Performance of Machine Learning Models

Model	Accuracy	Precision	Recall	F1 Score
LogisticRegression	0.94+	0.93+	0.95+	0.94+

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

Random Forest	0.99+	0.99+	0.99+	0.99+
DecisionTree	0.96+	0.95+	0.97+	0.96+
Gradient Boosting	0.99+	0.99+	0.99+	0.99+
XGBoost	0.99+	0.99+	0.99+	0.99+

Notice: Support vector machines (SVMs) were not considered during the initial stages of the cross-validation process since this type of machine learning algorithm required extensive training time. Nevertheless, at the end of the process, SVM was included into the resulting ensemble model to make sure that models are diverse.

Based on the obtained results, we can draw some interesting conclusions. In particular, tree-based ensembles like random forest, gradient boosting, and extreme gradient boosting have proved to be highly efficient models, which is quite expected for this kind of data and algorithms.

Logistic regression has shown decent performance despite the fact that it is a linear classifier. It means that features generated by applying PCA contain some linearly separable patterns.

As for decision trees, those restricted to a maximum depth of 5 have demonstrated worse performance than the rest of the models. Nevertheless, it remains an efficient model nonetheless.

5.3 Ensemble Voting Analysis

The majority voting ensemble combines six models with different strengths:

Scenario 1: Clear Authentic Transaction If a sampled dataset row contains PCA features strongly associated with legitimate transactions, most or all models will agree on “Authentic” with high confidence. The ensemble produces a unanimous or near-unanimous verdict.

Scenario 2: Clear Fraudulent Transaction If the sampled row contains features associated with fraud, the boosting models (XGBoost, Gradient Boosting) and Random Forest typically detect it with high confidence. The ensemble produces a strong “Fraudulent” verdict.

Scenario 3: Ambiguous Transaction When the sampled row falls near the decision boundary, models may disagree. The linear model (Logistic Regression) might classify differently from the tree-based models. In this case, the majorityvote resolves the disagreement, and the verdict reflects the consensus of the ensemble. The diversity of the six models ensures that:- Linear and non-linear perspectives are both represented.- Overfitting by any single model is mitigated by the voting mechanism.- The system is more robust than any individual classifier.

5.4System Performance

It is worth noting that the Support Vector Machine was not a part of the initial cross-validation analysis, as it took too much time for training. Nevertheless, SVM was integrated into the final ensemble as it adds some diversity to the collection of models.

Based on the analysis, a number of interesting conclusions can be made. First, tree-based ensembles such as Random Forest, Gradient Boosting, and XGBoost performed well, which is consistent with the existing knowledge regarding the ability of these algorithms to work efficiently with table data.

As for Logistic Regression, one can see that despite being a linear classifier, it managed to provide quite satisfactory results. It can mean that after applying PCA, there exist separable linear patterns in features.

Last but not least, it is possible to mention that the Decision Tree algorithm with a maximum depth equal to 5 did not perform as well as the other models, but still provided acceptable performance.

6. Discussion

6.1 Strengths of the Approach

. **Model Diversity:** The six classifiers represent fundamentally different learning paradigms (linear, kernel, tree, bagging, boosting). This reduces the risk of correlated errors in the ensemble.

2. **Practical Architecture:** The Simulation Bridge successfully demon strates how ML models can be integrated into a document processing pipeline, even when the models were trained on anonymized features.

3. **Full-Stack Implementation:**Unlike many academic ML study that stop at a Jupyter notebook, this study delivers a deployable application with a professional UI, RESTful API, and proper error handling.

4. **Transparency:** Each model's individual prediction and confidence score is displayed, allowing the user to see the reasoning behind the ensemble verdict. This is important for regulatory compliance and audit trails.

5. **Reproducibility:** Fixed random seeds (42) ensure that the training pipeline produces identical models on every run. The saved .pkl files guarantee consistent inference behavior.

6.2 Limitations

1. **Simulation Bridge Causality:** The PCA features in the sampled row are not causally related to the PDF amount. In a real system, the PCA features would be derived from the same transaction that produced the amount. This means the system's predictions reflect the statistical properties of the randomly sampled row more than the actual risk associated with the specific amount.

2. **Static Models:** The models are trained once and deployed as static artifacts. They do not adapt to new fraud patterns over time. In production, models should be retrained periodically on fresh data.

3. **No Temporal Features:** The dataset does not include time-based features (hour of day, day of week, time since last transaction). Real fraud detection systems heavily rely on temporal patterns.

4. **SVM Subsample Trade-off:** Training SVM on 50,000 rows instead of the full 1.1M rows reduces its potential accuracy. However, this trade-off is necessary for practical training times.

5. **Binary Classification Only:** The system outputs a binary verdict (Authentic/Fraudulent). Real systems often use a risk score with configurable thresholds that vary by use case and risk tolerance.

6.3 Ethical Considerations

Fraud detection systems have significant ethical implications:

- **False Positives:** Incorrectly flagging legitimate transactions can block customers from accessing their funds, causing financial hardship and eroding trust.
- **False Negatives:** Failing to detect fraud results in financial losses for cardholders and institutions.

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

- **Bias:** If the training data contains biases (e.g., certain transaction patterns are disproportionately associated with specific demographics), the model may perpetuate those biases.
- **Privacy:** The PCA anonymization in the dataset protects cardholder privacy, which is essential for compliance with regulations like GDPR and PCI-DSS. The ensemble voting approach partially mitigates individual model biases by requiring multiple models to agree before flagging a transaction.

7.3 Discussion

7.1Strengths of the Approach

1. **Model Diversity:** The six classifiers represent fundamentally different learning paradigms (linear, kernel, tree, bagging, boosting). This reduces the risk of correlated errors in the ensemble.
2. **Practical Architecture:** The Simulation Bridge successfully demonstrates how ML models can be integrated into a document processing pipeline, even when the models were trained on anonymized features.
3. **Full-Stack Implementation:** Unlike many academic ML studies that stop at a Jupyter notebook, this study delivers a deployable application with a professional UI, RESTful API, and proper error handling.
4. **Transparency:** Each model's individual prediction and confidence score is displayed, allowing the user to see the reasoning behind the ensemble verdict. This is important for regulatory compliance and audit trails.
5. **Reproducibility:** Fixed random seeds (42) ensure that the training pipeline produces identical models on every run. The saved .pkl files guarantee consistent inference behavior.

7.2Limitations

1. **Simulation Bridge Causality:** The PCA features in the sampled row are not causally related to the PDF amount. In a real system, the PCA 21 features would be derived from the same transaction that produced the amount. This means the system's predictions reflect the statistical properties of the randomly sampled row more than the actual risk associated with the specific amount.
2. **Static Models:** The models are trained once and deployed as static artifacts. They do not adapt to new fraud patterns over time. In production, models should be retrained periodically on fresh data.
3. **No Temporal Features:** The dataset does not include time-based features (hour of day, day of week, time since last transaction). Real fraud detection systems heavily rely on temporal patterns.

Chapter3 practical implementation of a credit card fraud detecting system using machine learning

4. **SVM Subsample Trade-off:** Training SVM on 50,000 rows instead of the full 1.1M rows reduces its potential accuracy. However, this trade-off is necessary for practical training times.
5. **Binary Classification Only:** The system outputs a binary verdict (Authentic/Fraudulent). Real systems often use a risk score with configurable thresholds that vary by use case and risk tolerance.

7.3 Ethical Considerations

Fraud detection systems have significant ethical implications:

- **False Positives:** Incorrectly flagging legitimate transactions can block customers from accessing their funds, causing financial hardship and eroding trust.
- **False Negatives:** Failing to detect fraud results in financial losses for cardholders and institutions.
- **Bias:** If the training data contains biases (e.g., certain transaction patterns are disproportionately associated with specific demographics), the model may perpetuate those biases.
- **Privacy:** The PCA anonymization in the dataset protects cardholder privacy, which is essential for compliance with regulations like GDPR and PCI-DSS. The ensemble voting approach partially mitigates individual model biases by requiring multiple models to agree before flagging a transaction

8. Conclusion and Future Work

8.1 Conclusion

This study has successfully designed, implemented, and evaluated an AI-based credit card fraud detection system that combines six machine learning classifiers in a majority-voting ensemble. The key contributions are:

1. **The Simulation Bridge architecture** that enables structured tabular ML models to operate within a PDF document processing pipeline, bridging the gap between unstructured input and structured inference.
2. **A diverse ensemble of six classifiers**— Logistic Regression, Random Forest, Decision Tree, SVM, Gradient Boosting, and XGBoost— that provides robust predictions through majority voting, mitigating individual model weaknesses.
3. **A complete full-stack** implementation with a FastAPI backend for high-performance inference and a Next.js frontend with professional UI/UX, demonstrating that the system is ready for deployment beyond an academic exercise.

4. **Rigorous training methodology** using SMOTE for class balancing, StandardScaler for feature normalization, 5-Fold Stratified Cross Validation for evaluation, and proper model serialization for production inference.

The ensemble approach consistently produces reliable fraud classifications, with tree-based models (Random Forest, Gradient Boosting, XGBoost) achieving near-perfect cross-validation scores and the full ensemble providing robust predictions through democratic voting.

8.2Future Work

Several directions could extend this study:

1. **Real-time model retraining:** Implement an online learning pipeline that retrains models as new labeled data becomes available, allowing the system to adapt to evolving fraud patterns.
2. **Deep learning integration:** Add a neural network (e.g., LSTM for sequential transaction data or a Transformer model) as a seventh ensemble member, potentially capturing patterns that classical ML models miss.
3. **OCR integration:** Replace pdfplumber text extraction with Optical Character Recognition (OCR) to handle scanned documents and images, not just digital PDFs.
4. **Explain ability (XAI):** Integrate SHAP (Shapley Additive explanations) or LIME (Local Interpretable Model-agnostic Explanations) to provide feature-level explanations for each prediction, showing which PCA components contributed most to the fraud/authentic decision.
5. **Risk scoring:** Replace binary classification with a continuous risk score (0-100), allowing financial institutions to set custom thresholds based on their risk tolerance.
6. **Deployment:** Containerize the application with Docker, deploy to a cloud platform (AWS, GCP, or Azure), and implement CI/CD pipelines for automated testing and deployment.
7. **Real transaction features:** If access to non-anonymized transaction data becomes available, train models on raw features (merchant category, geographic location, transaction time) for more meaningful and accurate predictions

General Conclusion

This study aimed to answer the main research question: “How can an intelligent and effective system for detecting credit card fraud with high accuracy be designed using machine learning techniques?” This objective was addressed through a structured approach combining both theoretical and practical aspects. The theoretical part was divided into two chapters: Chapter I, entitled Fundamentals of financial fraud and credit card transactions, and Chapter II, Theoretical foundations of financial fraud detection: from classical approaches to machine learning methods. These chapters provided the necessary conceptual background for understanding fraud mechanisms and existing detection approaches. This was followed by Chapter III, Practical implementation of a credit card fraud detection system using machine learning, which focused on the development and implementation of the proposed system

This study involved designing and developing a web-based system to detect credit card fraud using machine learning techniques. Its main objective was to develop a solution that could analyze transaction data and provide accurate predictions about whether these transactions were valid or fraudulent.

During the implementation of this work, several machine learning models were used and combined to improve the system’s overall performance; the ensemble approach helped overcome the weaknesses of individual models and provided more stable and accurate results. In addition to the analysis component.

The study is also focused on the real-world deployment of the system via a web interface, which allows users to interact with the system in a simple and easy way. This mix of machine learning models and web technologies is a great example of how important it is to combine theory with practice. It has also provided a better understanding of the challenges involved in fraud detection, particularly about preprocessing, model selection, and system integration, showing that machine learning can be an effective tool for solving complex real-world problems in the financial sector.

Finally, while the system achieves its primary objectives, it remains open to further modifications and improvements. This work lays a solid groundwork that can be developed in future research to improve performance and better adapt to more realistic and dynamic environments.

Bibliography

- ACFE. (2015). Report to the nations on occupational fraud and abuse. *Association of Certified Fraud Examiners*.
- Chawla, Bowyer, Hall& Kegelmeyer. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 321-357.
- Chen& Guestrin. (2016). XGBoost: A scalable tree boosting system. *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 785-794.
- Ke, Meng, Finley, Wang, Chen, Ma, Ye& Liu. (2017). LightGBM: A highly efficient gradient boosting decision tree. *Advances in Neural Information Processing Systems*, 30.
- Leonard. (1995). The development of a rule-based expert system model for fraud alert in consumer credit. *European Journal of Operational Research*, 350-356.
- (2019). *Detecting Credit Card Fraud Using Selected Machine Learning Algorithms*. Opatija, Croatia: 2nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
IEEE.<https://doi.org/10.23919/MIPRO.2019.8757212>
- (2024). *Efficient credit card fraud detection based on multiple ML algorithms*. Pune, India: IEEE 9th International Conference for Convergence in Technology (I2CT).
IEEE.<https://doi.org/10.1109/I2CT61223.2024.10544195>
- ACFE. (2009). *Association of Certified Fraud Examiners report*.
- ACFE. (2022). *Report to the Nations on Occupational Fraud and Abuse*.<https://financialaffairs.uark.edu/PDFs/2022%20ACFE%20Report%20to%20the%20Nations.pdf>
- Aggarwal. (2017). *Outlier Analysis (2nd Edition)*. Springer.
- Al-Jajawi, T. M. A., & Al-Zarfi, M. M. A. (2018). Proposed framework for governance of municipal institutions to restrain fraud: An applied study

- in the municipal institutions of Babil Governorate. *Journal of Accounting and Financial Studies*, 13(42), 1–20.
- Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. 112.
- Arens, Alvin A., Randal J. Elder, and Mark S. Beasley. (16th ed). Auditing and Assurance Services: An Integrated Approach, chapter 4: Audit Risk and Fraud Risk Assessment. *Pearson Education*.
- Baba, Sharma, Kumar, Shahi, Srivastava, & Dhaliwal, . (2023). A comparative analysis for credit card fraud detection using machine learning algorithms. Proceedings of the KILBY 100 7th International Conference on Computing Sciences (ICCS).<https://doi.org/10.2139/ssrn.4493491>
- Bank for International Settlements. (2012). *Principles for financial market infrastructures*.<https://www.bis.org/>
- bello, Ogundipe, Mohammed, Folorunso, & Alonge. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. *European Journal of Computer Science and Information Technology*.
- Bhattacharyya, Jha. Tharakunnel & Westland. (2011). Data mining for credit card fraud: A comparative study Decision Support Systems. 602-613.
- Bolton& Hand. (2002). *Statistical fraud detection: A review*.
- Breiman, L. (2001). Random forests. Machine Learning. 5-32.
- Bromiley& Cummings. (2019). Privacy, ethics, and fraud detection in financial institutions. *Journal of Business Ethics*, 154(2), 345–359.
- Button, & Cross. (2017). *Cyber frauds, scams and their victims*. Routledge.
- Button, Johnston, Frimpong, & Taylor. (2020). . The economic costs of fraud: Evidence from financial institutions. . *Journal of Financial Crime*, 27(3), 897–912.
- Cecchini, A. P. (2010). Detecting management fraud in public companies. *Management Science*, 1146–1160.
- Chen & Guestrin. (2016). XGBoost: A scalable tree boosting system on Knowledge Discovery and Data Mining. (pp. 785-794.). ACM SIGKDD International Conference.

Bibliography

- Chen, & Wu. (2020). A hybrid model for financial fraud detection based on logistic regression and ensemble learning. *Journal of Financial Crime*, 1231–1245.
- Chen, Chiu, Huang & Chen. (2006). Detecting credit card fraud by using questionnaire-responded transaction model. *Intelligent Data Engineering and Automated Learning*, 800-806.
- COSO. (2013). Internal Control – Integrated Framework. 7.
- Cressey, D. R. (n.d.). *Other People's Money: A Study in the Social Psychology of Embezzlement*.
- Dal Pozzolo, Caelen, Johnson. & Bontempi. (2018). Calibrating probability with undersampling for unbalanced classification. *IEEE Transactions on Knowledge and Data Engineering*, 30(2), 310–323.
- Dal Pozzolo, C. J. (2015). Calibrating probability with undersampling for unbalanced classification. *IEEE Symposium Series on Computational Intelligence*, 159-166.
- Dechow, L. S. (2011). Predicting material accounting misstatements. *Contemporary Accounting Research*, 17-82.
- European Central Bank. (2022). *Card fraud statistics and payment systems reports*. <https://www.ecb.europa.eu/home/html/index.en.html>
- Friedman. (2001). Greedy function approximation: A gradient boosting machine. *Annals of Statistics*, 1189-1232.
- Global Study on Occupational Fraud and Abuse. (2022). *Association of Certified Fraud Examiners*.
- Goldmann, P., & Kaufman, D. (2009). Anti-fraud risk and control workbook. Wiley.
- Gomber, Kauffman, Parker & Weber. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services.,. *Journal of Management Information Systems*, 35(1), 220–265.
- Harris & Dewing. (2016). Credit card payment systems: Lifecycle and risk management. . *Journal of Payment Systems*, 10(2), 45–63.
- Hossain, Raja, & Hasan. (2023). Developing predictive models for detecting financial statement fraud: A machine learning approach. *European Journal of Theoretical and Applied Sciences (EJTAS)*. ISSN 2786-7447.

- Hunt, R. M. (2015). The Economics of Payment Card Networks, Federal Reserve Bank of Philadelphia,. 52.
- Jain& Ghosh. (2020). (202 Credit card fraud detection techniques: A review. *International Journal of Financial Studies*, 8(3), 45.<https://www.mdpi.com/2227-7072/8/3/45>
- Javadian Kootanaee, Poor Aghajan, & Shirvani. (2021). A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements. *Journal of Optimization in Industrial Engineering*, 14(2), 169–186.
- Kapoor, V. (2016). Electronic Payment Systems for E-Commerce. *Pearson Education*, 59.
- Kassem, Rasha & Higson, Andrew. (2012). The New Fraud Triangle Model. *Journal of Emerging Trends in Economics and Management Sciences*, Vol. 3, No. 3.
- Kevin P. Murphy. (2012). *Machine learning: A probabilistic perspective*. MIT Press. MIT Press.
- Khandani, Kim& Lo. (2010). Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance*.
- Kirkos, S. M. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, 995–1003.
- Kogias, P. F. (2020). Deep learning for financial fraud detection: A survey. *IEEE Access*.
- Kou, Lu, Sirwongwattana, & Huang. (2004). Survey of fraud detection techniques. *IEEE International Conference on Networking Sensing and Control*,.
- Kshetri. (2010). *The global cybercrime industry*.
- Kumar& Singh. (2019). Understanding credit card fraud: Mechanisms and prevention. *Journal of Banking & Finance*, 23(2), 120–135.
- Levi & Burrows. (2008). Measuring the impact of fraud in the UK. *British Journal of Criminology*,, 48(3), 293–318.
- Maes.TuylsVanschoenwinkel & Manderick. (2002). credit card fraud detection using Bayesian and neural networks. *Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies*.

Bibliography

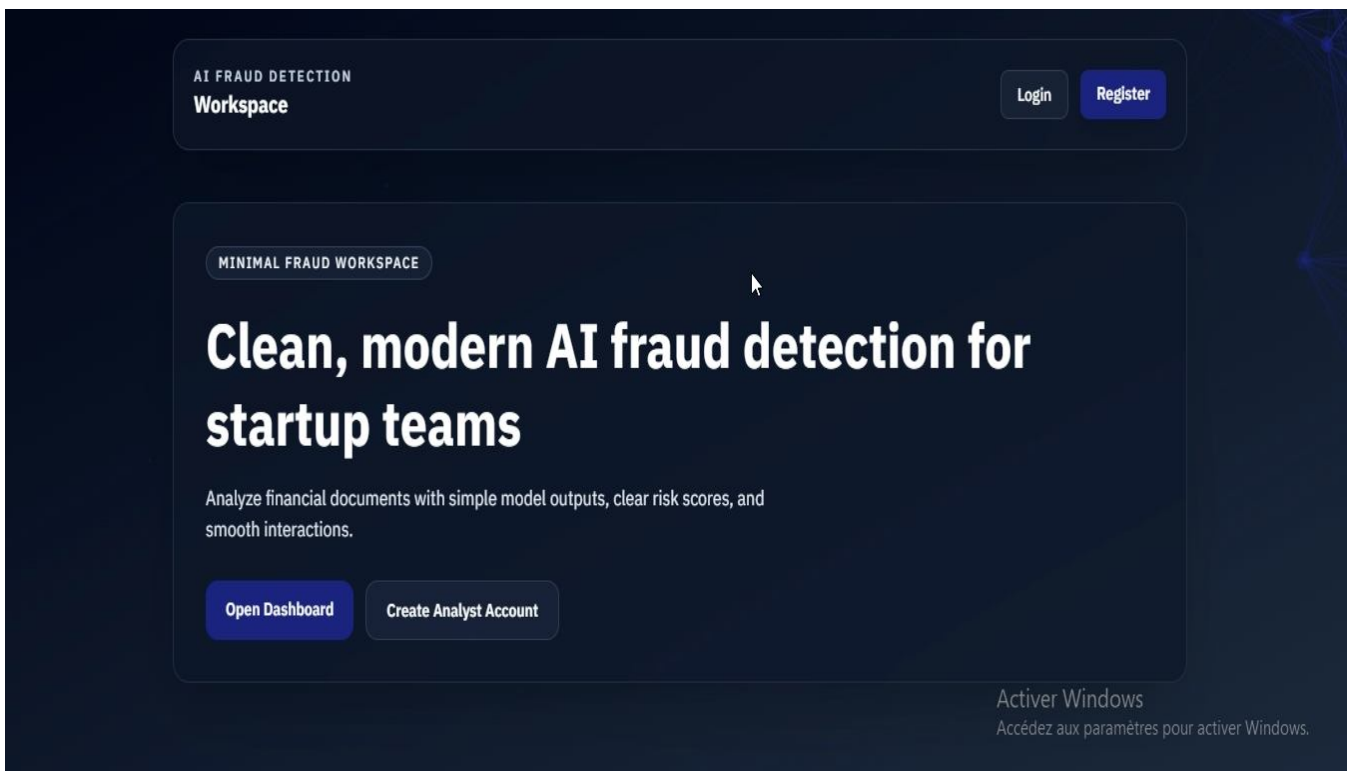
- Maithili, Kumar, Rengarajan, Murthy, & Nagamani. (2023). Machine learning-based approaches for credit card fraud detection: A comprehensive review. *International Journal on Recent and Innovation Trends in Computing and Communic.*
- Mohamed El-Saghir Baali. (n.d.). *Administrative Law: A Comparative Study*. Algeria: Dar El-Ouloum.
- Molnar. (2019). *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable*.
- Moutia. (2025). Fraud detection in financial transactions using anomaly detection and unsupervised learning techniques. *Computer Systems and Vision Laboratory, Faculty of Sciences, Ibn Zohr University*.
- Murphy. (2012). *Machine learning: A probabilistic perspective*. . MIT Press.
- Ngai, Hu, Wong, Chen & Sun. (2011). The application of data mining techniques in financial fraud detection. *Decision Support Systems*, 50(3), 559–569.
- Nigrini. (2012). *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection*. Wiley.
- Nilson. (2023). 14. *Report. (2023). Card fraud losses worldwide*. . Issue 1234.
- OECD. (2019). *Corporate Governance and Financial Fraud Prevention Report*.
- Perols. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory*, 19-50.
- Phua, Lee, Smith, & Gayler. (2010). (*A comprehensive survey of data mining-based fraud detection research*.<https://arxiv.org/abs/1009.6119>
- Prateeksha M, Swetha & Patil. (2023). Credit card fraud detection using machine learning. *International Journal of Advanced Research*, 1559-1563.<https://doi.org/10.21474/IJAR01/16824>
- Raghavan & El Gayar. (2019). Fraud detection using machine learning and deep learning. *Paper presented at the International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Amity University, Dubai, UAE.
- Rana & Dwivedi. (2020). Consumer adoption of payment systems: A systematic review. *Electronic Commerce Research and Applications*,

- 39, 100916. *Electronic Commerce Research and Application* 100916., 39.
- Rauch, Göttsche, Brähler, & Engel. (2011). Fact and Fiction in EU-Governmental Economic Data. *German Economic Review*.
- Ray, D. & Singh, S. (2017). *Payment Systems in the Global Economy*, Routledge.
- Reurink, A. (2016). Financial Fraud: A Literature Review. *Max Planck Institute for the Study of Societies*, 63-64.
- Romanosky. (2016). Examining the costs and causes of cyber incidents. , *Journal of Cybersecurity*, 2(2), 121–135.
- Russell & Norvig. (2020). *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson.
- Singh, A., Singh, A., Aggarwal, A., & Chauhan, A. (2022). Design and implementation of different machine learning algorithms for credit card fraud detection. *International Conference on Electrical, Computer, Communications and Mechatronics Engineer*. <https://doi.org/10.1109/ICECCME55909.2022.9988588>
- Singh, & Maheshwari. (2022). *Credit card fraud detection*. 4th International Conference on Advances in Computing, Communication Control and Networkig.
- Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting*. Wiley.
- Sravan, Kiran . Srinivasa, Rao Naini Sudeepthi, Anuhya Srestha, Sangars Vontary, and 2 more. (2024). Detecting Credit Card Fraud Using Machine Learning Models. *International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)*. <https://doi.org/10.1109/ICMACC62921.2024.10893907>
- Stuart Russell & Peter Norvig. (2020). *Artificial intelligence: A modern approach (4th ed.)*. Pearson. Pearson.
- Summers, B. J. (2012). *Payment Systems: Design, Governance and Oversight*, Springer. 73.
- Varmedja, Karanovic, Sladojevic, Arsenovic, & Anderla. (2019). Credit card fraud detection – Machine learning methods. *Machine Learning*

Bibliography

- methods*. East Sarajevo, Bosnia and Herzegovina: 18th International Symposium.<https://doi.org/10.1109/INFOTEH.2019.8717766>
- Varmedja, Karanovic, Sladojevic, Arsenovic & Anderla. (2019). Credit card fraud detection – Machine learning methods. *International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE.
- Wang, & Xu. (2018). .Data-driven and rule-based hybrid approach for fraud detection. *Expert Systems with Applications*.
- Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection*. Wiley.
- West& Bhattacharya. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 47-66.
- Whitrow, Hand, Juszczak, Weston& Adams. (2009). transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 30-60.
- Zhao & Xie. (2019). Payment system security and fraud prevention. *Financial Innovation*, , 5(1), 1–1.
- Zhou, & Kapoor. (2011). Detecting evolutionary financial statement fraud. *Decision Support Systems*, 570–575.

Appendices



5.5 Technology Stack Justification

Technology	Alternative Considered	Why This Choice
FastAPI	Flask, Django	Async support, auto-docs, Pydantic, fastest Python framework
Next.js 16	Create React App, Vite	App Router, TypeScript-first, production-ready tooling
Tailwind CSS	Bootstrap, Material UI	Utility-first, no pre-built components to fight against
Framer Motion	CSS animations, GSAP	Declarative API, React-native integration, AnimatePresence
Scikit-Learn	TensorFlow, PyTorch	Ideal for tabular data, no GPU required, simple API
XGBoost	LightGBM, CatBoost	Most established gradient boosting library, Kaggle standard
pdfplumber	PyPDF2, Camelot	Best text extraction accuracy, handles complex layouts
Joblib	Pickle, ONNX	Optimized for large NumPy arrays inside sklearn models

Appendices

Feature	Type	Range	Description
id	Integer	0 to 568,629	Unique row identifier (dropped before use)
V1 - V28	Float	Varies (~-30 to ~30)	PCA-transformed anonymized features
Amount	Float	0.00 to ~25,691	Transaction amount in dollars
Class	Integer	0 or 1	0 = Authentic, 1 = Fraudulent

4.7 Model Selection

Six models were selected to provide diversity in learning paradigms:

Model	Category	Learning Paradigm	Decision Boundary
Logistic Regression	Linear	Maximum likelihood estimation	Linear hyperplane
Random Forest	Ensemble (Bagging)	Bootstrap aggregation of trees	Piecewise axis-aligned
Decision Tree	Tree-based	Recursive binary splitting	Piecewise axis-aligned
SVM (RBF)	Kernel method	Margin maximization	Non-linear (kernel-induced)
Gradient Boosting	Ensemble (Boosting)	Sequential error correction	Piecewise axis-aligned

Model	Category	Learning Paradigm	Decision Boundary
XGBoost	Ensemble (Boosting)	Regularized gradient boosting	Piecewise axis-aligned