

جهاد عبدالله

Master Thesis Template-10-2-2026 All Chapter -.docx

 Midocean University

Document Details

Submission ID

trn:oid::2945:405847185

Submission Date

Aug 7, 2026, 7:55 PM GMT+3

Download Date

Aug 11, 2026, 12:36 PM GMT+3

File Name

Master Thesis Template-10-2-2026 All Chapter -.docx

File Size

3.6 MB

70 Pages

11,903 Words

70,809 Characters

9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

-  **104 Not Cited or Quoted 9%**
Matches with neither in-text citation nor quotation marks
-  **0 Missing Quotations 0%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 5%  Internet sources
- 4%  Publications
- 7%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 104** Not Cited or Quoted 9%
Matches with neither in-text citation nor quotation marks
- 0** Missing Quotations 0%
Matches that are still very similar to source material
- 0** Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 0** Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 5% Internet sources
- 4% Publications
- 7% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

- Submitted works**
Midocean University on 2025-09-05 <1%
- Submitted works**
University of Teesside on 2026-05-01 <1%
- Publication**
Bhabani Prasanna Pattanaik, Dharendra Kumar Shukla, Sambit Satpathy, Kamala... <1%
- Internet**
d1q2ihs98wnwia.cloudfront.net <1%
- Submitted works**
Glasgow Caledonian University on 2026-04-15 <1%
- Publication**
V. Sekhar, P. Ajay Kumar Reddy, K. Logesh, T. Raghunadha Reddy, Dara Raju. "Ne... <1%
- Submitted works**
Universiti Malaysia Pahang Al-Sultan Abdullah (UMPISA) on 2026-01-11 <1%
- Internet**
mdpi-res.com <1%
- Internet**
ruor.uottawa.ca <1%
- Submitted works**
Institut Teknologi Brunei on 2025-04-23 <1%

11	Submitted works	The African Institute for Mathematical Sciences Ghana (AIMS Ghana) on 2026-05-29	<1%
12	Submitted works	Sunway Education Group on 2023-08-05	<1%
13	Internet	thesai.org	<1%
14	Publication	"Machine and Computing Technologies for Sustainable Development", Springer S...	<1%
15	Internet	www.ijrte.org	<1%
16	Submitted works	Thesis 2026 on 2026-06-16	<1%
17	Submitted works	Wittenborg University on 2023-09-25	<1%
18	Publication	da Cunha Ceulin, Wagner Luiz. "Knowledge Elicitation in Deep Learning Models", ...	<1%
19	Internet	etd.lib.metu.edu.tr	<1%
20	Internet	www.coursehero.com	<1%
21	Internet	docslib.org	<1%
22	Internet	kids.britannica.com	<1%
23	Internet	repository.learn-portal.org	<1%
24	Internet	revista.domhelder.edu.br	<1%

25	Internet	s3.eu-central-1.amazonaws.com	<1%
26	Publication	"AI Technologies for Information Systems and Management Science", Springer Sc...	<1%
27	Submitted works	London School of Science & Technology on 2025-09-21	<1%
28	Submitted works	University of Westminster on 2025-11-13	<1%
29	Submitted works	University of Westminster on 2026-03-29	<1%
30	Internet	studentsrepo.um.edu.my	<1%
31	Publication	Anggi Putri, Dian Anita Nuswantara. "Artificial Intelligence and Data Mining in De...	<1%
32	Submitted works	Bournemouth University on 2021-06-04	<1%
33	Submitted works	Sydney Institute of Technology and Commerce on 2025-09-26	<1%
34	Publication	V. Kavitha, Kumar T. Suresh, Priya T. S. Vishnu, T. Kumaresan. "chapter 10 Forecas...	<1%
35	Submitted works	Liberty University on 2026-07-27	<1%
36	Publication	Rafael da Fonseca Lameiro. "Análise de dados e aprendizado de máquina para o d...	<1%
37	Submitted works	University of Derby on 2026-01-20	<1%
38	Internet	www.scopusacademia.org	<1%

39	Submitted works	Asia Pacific University College of Technology and Innovation (UCTI) on 2025-02-21	<1%
40	Submitted works	ICTS on 2026-06-21	<1%
41	Submitted works	Lyons College on 2025-09-21	<1%
42	Submitted works	University of Rwanda on 2022-03-04	<1%
43	Internet	www.bridgeviewmarketing.com	<1%
44	Internet	www.cartagena99.com	<1%
45	Publication	Arvind Dagur, Karan Singh, Pawan Singh Mehra, Dharendra Kumar Shukla. "Intelli...	<1%
46	Submitted works	Faculty of Computing on 2026-06-14	<1%
47	Submitted works	Taylor's Education Group on 2025-08-05	<1%
48	Submitted works	University of Birmingham on 2026-05-23	<1%
49	Internet	dspace.daffodilvarsity.edu.bd:8080	<1%
50	Internet	scholarhub.unimas.my	<1%
51	Internet	www.hindawi.com	<1%
52	Internet	www.isarconference.org	<1%

53	Internet	www.jonesday.com	<1%
54	Internet	123dok.com	<1%
55	Submitted works	Carnegie Mellon University on 2025-11-11	<1%
56	Submitted works	Chester College of Higher Education on 2025-10-14	<1%
57	Submitted works	Chester College of Higher Education on 2025-10-16	<1%
58	Submitted works	College of Public Health on 2026-01-20	<1%
59	Publication	Harvinder Singh, Priyanka Kaushal, Sarabjeet Kaur. "Advanced Computing and AI...	<1%
60	Submitted works	Middle East College of Information Technology on 2023-06-04	<1%
61	Submitted works	Middle East College on 2026-01-04	<1%
62	Submitted works	Thesis 2026 on 2026-06-29	<1%
63	Submitted works	UCL on 2025-09-08	<1%
64	Submitted works	Universiti Teknologi Malaysia on 2012-11-12	<1%
65	Submitted works	University of Gloucestershire on 2025-09-22	<1%
66	Submitted works	University of Hertfordshire on 2026-01-04	<1%

67	Internet	albayanres.com	<1%
68	Internet	dview.io	<1%
69	Internet	gr-journals.com	<1%
70	Internet	journal.nsps.org.ng	<1%
71	Internet	repository.aaup.edu	<1%
72	Internet	trepo.tuni.fi	<1%
73	Internet	www.ijeast.com	<1%
74	Publication	Bui Thanh Hung, M. Sekar, Ayhan Esi, R. Senthil Kumar. "Applications of Mathema...	<1%
75	Submitted works	CTI Education Group on 2026-06-17	<1%
76	Submitted works	The University of the West of Scotland on 2025-08-15	<1%
77	Submitted works	University of East London on 2023-05-10	<1%
78	Submitted works	University of Northumbria at Newcastle on 2026-05-14	<1%
79	Publication	V. Sharmila, S. Kannadhasan, A. Rajiv Kannan, P. Sivakumar, V. Vennila. "Challeng...	<1%
80	Submitted works	Purdue University on 2024-09-06	<1%

81	Submitted works	
University of Wales Institute, Cardiff on 2023-09-11		<1%
82	Submitted works	
Westford Global Education on 2026-05-03		<1%
83	Internet	
eprints.utm.my		<1%
84	Internet	
dspace.kuet.ac.bd		<1%



AI-Based Smart Accounting System to Automate Accounting And Fraud Detection In SMEs

Prepared By

Name: Jihad Abdullh Najee Alhuraiby

ID No.: 253002789

Submitted in fulfillment of the requirements for the degree Master of
Science in Artificial Intelligence

At

Collage of Informatics

Midocean University

UAE

Supervisor Name: Dr.Amjed Qutaish

Collage of Informatics, Midocean University, Comoros

Email: 253002789@st.midocean.edu.ki

Acknowledgements

In addition to that, we would like to thank Dr. Amjad Qutaish for being such a supportive force in all aspects and for providing us with useful advice and guidance all along during this study process. Furthermore, our gratitude is due to the faculty members and administration of MedOcean University, most importantly our lecturers and doctors, for their cooperation and assistance in creating a favorable atmosphere for this study.

Abstract

Time fraud detection is crucial for maintaining transparency in financial mechanisms and ensuring continued growth in the field. This research proposes a novel approach to accounting via integration of ML and DL technologies into existing accounting frameworks. One distinctive element of this research is an approach to feature selection, including a hybrid method combining filtering and wrapping stages, to simplify training of the predictive model and improve the interpretability of features' importance in complex financial contexts.

The suggested algorithm involves a Stacking Ensemble, which includes several base estimators such as Logistic Regression, Decision Tree, Random Forest, SVM, and KNN with MLP being the meta-estimator. While individually, these models achieved excellent results from the perspective of accuracy rate between 97.5% to 99.1%, the final F1 score was 0.92 which allowed finding the right balance in detecting rare instances of fraud. To improve explainability in the "black box" process of machine learning algorithms, SHAP and LIME were applied. Testing on the Datamendeley Artificial Intelligence and Accounting Profession dataset showed promising results regarding automated invoice processing and fraud prevention.

List of Publications

Alhuraiby, J. (2026). Development of an intelligent accounting system that performs automated tasks and detects fraudulent activities using artificial intelligence in SMEs. Med Ocean University Journal of Artificial Intelligence Research.

Table of Contents

Chapter 1: Introduction and Overview	1
1.1 Overview	1
1.2 Problem Definition	2
1.3 Thesis Objectives	2
1.4 Thesis Contribution	3
1.5 Thesis Organization	3
Chapter 2: Background and Related Work	4
2.1 Introduction to AI in Accounting and Financial Automation	4
2.2 The Problem of Accounting Fraud in SMEs	5
2.3 Common Datasets and Challenges in Accounting	6
2.4 Key Factors and Techniques in AI-Based Fraud Detection for Accounting	7
2.5 Related Studies and Systematic	9
2.6 Gaps in Existing Literature	11
2.7 Artificial Intelligence (AI)	12
2.8 Machine Learning (ML)	13
2.9 Deep Learning (DL)	14
2.10 Large Language Models (LLMs)	16
2.11 Explainable AI (XAI)	17
2.12 Classification Techniques	17
2.12.1 Machine Learning Techniques (Decision Tree, Random Forest, KNN, SVC)	18
2.12.2 Deep Learning Techniques (MLP, RNN)	22
2.13 Feature Selection	25
2.14 Evaluation Metrics	26
Chapter 3: Proposed Approach	35
3.1 Introduction	35

3.2 The Proposed System	37
3.3 Dataset Description	38
3.4 Hybrid Filter-Then-Wrapper Feature Selection	39
3.5 Stacking Ensemble for Fraud Detection	40
3.6 Accounting Automation Components	41
3.7 Explainable AI (XAI) Integration	41
3.8 Implementation Details	42
3.9 Architecture Building of Project	42
3.10 Data Ingestion Layer	45
3.11 Summary	47
Chapter 4: Experimental Results and Discussion	48
4.1 Introduction	48
4.2 Exploratory Data Analysis & Financial Overview	48
4.2.1 Transaction Distribution Within Accounting Classifications	49
4.2.2 Financial Outlier Analysis by Category	49
4.2.3 Revenue-to-Expense Ratios & Financial Statements Analysis	50
4.2.4 Temporal Transaction Trends and Monthly Revenue Analysis	51
4.3.1 Feature Importance Ranking	52
4.4 Fraud Detection Model Performance & Experimental Evaluation	52
4.4.1 Classification Metrics Analysis	53
4.4.2 Detected Fraud vs. Risk Score Scatter Analysis	53
4.4.3 Error Analysis: Confusion Matrix & Suspicious Amount Distributions	53
4.5.1 SHAP Feature Importance and Impact Distribution	55
4.6 Discussion and Practical Implications	56
4.7 Summary	56
Chapter 5: Conclusion and Future Work	57

7	5.1 Introduction	57
	5.2 Summary of the Study	57
	5.3 Key Findings	58
	5.4 Contributions of the Study	58
	5.5 Practical Implications	59
62	5.6 Limitations	59
	5.7 Future Work	60
	5.8 Concluding Remarks	61
	References	62

Chapter 1 Introduction

1.1 Overview

In today's era, the adoption of SMEs is making it necessary for organizations to automate accounting processes and fraud detection as soon as possible. In addition to improving efficiency, automation and forecasting help organizations take action early, minimize losses, and manage their resources more effectively. With SMEs advancing towards digital ecosystems, all activities such as processing of invoices and analyzing costs leave a digital trail that provides key information about the financial performance and risks of the business (Hernández-García et al., 2024). The application of AI, particularly ML and DL, has been highly effective in discovering complex patterns from such large volumes of data. Using historical data analysis, ML and DL algorithms discover intricate non-linear correlations, where ANNs have shown promising results in detecting abnormalities based on the frequency and magnitude of transactions (Isljamovic & Suknovic, 2014). Incorporating LLMs such as GPT and BERT models extends the capabilities of financial analytics by facilitating the processing of unstructured data, including emails and invoices in their raw format (Alnasyan, 2024). However, the success of sophisticated ML algorithms depends heavily on advanced feature selection methods to maintain accuracy and interpretability.

1.2 Problem Definition

Today, Small and Medium Enterprises (SMEs) face enormous challenges in their operations due to heavy dependence on manual accounting systems. The laboriousness of the manual system makes it highly susceptible to errors and inefficiencies, leading to inaccurate information. In addition, SMEs generally operate on smaller budgets and have limited personnel, rendering them vulnerable to either accidental errors or even fraud. Conventional auditing techniques fail to effectively detect any sophisticated and multilayered fraud. Consequently, the result has been significant financial losses to these enterprises, with fraud stealing an estimated 5% of annual income across the world.

1.3 Thesis Objectives

The main objective of the current research project is to overcome the gap between the technologies used in the field of financial management for small and medium businesses, as follows:

Develop an AI-based Framework: create an automated system that will take care of the most common tasks related to finance in order to increase the efficiency and reduce errors of SMEs.

Develop a Robust Model for Detecting Fraudulent Activities: use and develop a model that combines machine learning and deep learning methods to identify complex non-linear anomalies related to fraudulent activities.

Empirical Validation: validate the developed model through empirical tests that include the use of a dataset obtained from such sources as Dataverse, as well as using such criteria as Accuracy, F1 score, and Precision.

Explain AI using XAI Methods: apply explainable AI techniques, such as SHAP and LIME, to provide understandable explanations to accountants about why certain anomalies were identified.

1.4 Thesis Contribution

The contributions of this study to the fields of fintech and applied artificial intelligence can be summarized in three main points in a more fluid style:

Novel Stacking Ensembles Architecture: This study suggests a stacking ensemble architecture consisting of multiple base machine learning models along with a deep learning meta-learner. This design enhances fraud detection by identifying both clear and subtle anomalies in financial data, providing better F1-scores than conventional models.

A Very Efficient Hybrid Feature Selection Mechanism: This study proposes a novel filtering-then-wrapping scheme for high-dimensional fintech problems that dramatically reduces computation costs and eliminates the curse of dimensionality to enable real-time implementation of advanced AI models on lower hardware configurations.

A Leap from Theory to Practice: In addition to purely academic research, this paper presents an end-to-end smart accounting solution for SMEs by using AI algorithms. With our proposed explainable AI methods such as SHAP and LIME, we provide an easy-to-use decision-making platform for non-AI experts in finance.

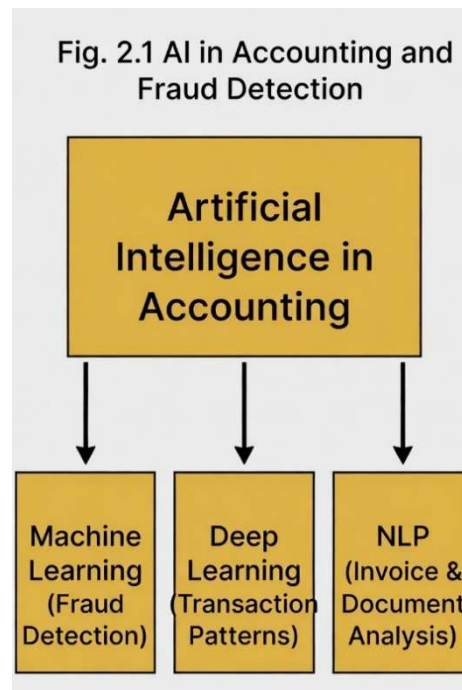
1.5 Thesis Organization

This document is organized into multiple sections:

- Section 2 discusses Background and Literature Review
- Section 3 describes the Proposed Approach
- Section 4 provides the Experimental Results and Discussion
- Section 5 provides Conclusions and Future Research Directions

Chapter 2 Background and Related Work

2.1 Introduction to AI in Accounting and Financial Automation

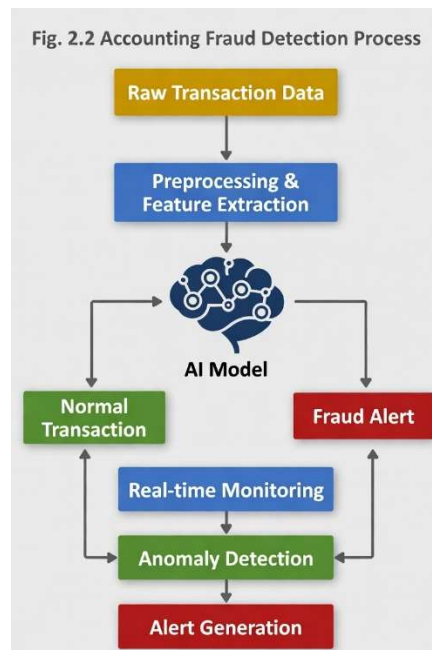


Artificial intelligence technology has revolutionized the field of accounting, shifting from archaic electronic systems to sophisticated intelligent stations through the use of such capabilities of AI technology as machine learning, natural language processing, and large data processing techniques. The application of AI technologies involves examining vast amounts of information including documentation, invoices, expense types, accounting requirements, and causal relationships.

This is particularly relevant for small and medium businesses due to budgetary considerations, accounting staff shortages, and an increased possibility of irregularities within the firm. AI technologies allow conducting real-time processing, reducing errors, increasing accuracy, and providing predictive analytics. A notable application of AI technologies in accounting is the identification of illogical transactions or potential fraudulent activity.

The benefits provided by AI technologies, including automation of all accounting processes along with fraud prevention, have made smart accounting particularly useful in today's complex post-COVID environment.

2.2 The Problem of Accounting Fraud in SMEs



First of all, accounting fraud in SMEs is a complicated issue since it is often detected by various manipulations, including fraudulent financial reports, tricky reimbursement schemes, and payroll frauds. Second, while major companies have an efficient and sophisticated system of internal audits, it is often not applicable in smaller enterprises, as it implies strong internal controls and clearly defined duty segregation that can prevent frauds.

The financial loss associated with occupational frauds is rather considerable: global estimations imply the loss of roughly 5% of SME annual revenues. The main reason for such a large amount is related to the inefficiency of manual accounting, as it usually identifies fraud only after its occurrence and cannot track non-linear discrepancies. Similarly, rule-based fraud detection systems, implying if-then operations, are often not able to adapt to new ways of committing crimes, as they do not consider their behavioral aspect.

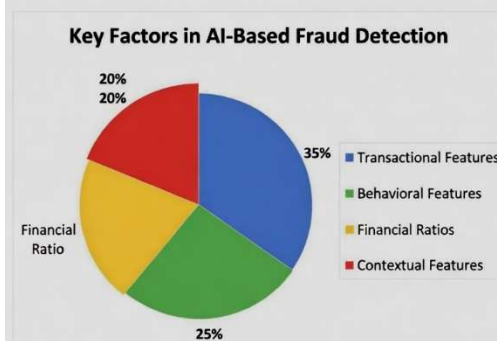
Artificial Intelligence can significantly contribute to preventing and detecting fraud in SMEs, as they are capable of analyzing various behavior-related issues in real time. Such a solution is more flexible and adaptive than standard solutions implying the use of rules, which means they can detect even minor deviations and suspicious transactions.

2.3 Common Datasets and Challenges in Accounting

Fig. 2.3 Influential Features for Fraud Detection

1. The us features beatured bus fraud detection dat: detection in feature.
2. The dees thening one unnerrations our scaject the nipiecrting fraud detection.

Fig. 2.3 I X Influential Features for Fraud Detection



The 3 Influential features for the frey Fraud Detection is features and till enversitly features for datagoats, to every, fraud detecrting in the eatures categoing uncrashx and casections on the:omblen of fee fraud detection.

Master Thesis

16

The sensitivity of financial information requires that researchers avoid using real data due to privacy considerations. Therefore, modern works use either synthesized or anonymized data sets when working on anomaly detection. Most of the available researches base their analysis on famous credit card fraud detection datasets and/or financial data statements that were created from public enterprises. Nonetheless, there is one serious issue regarding the data used for research - the scarcity of transactional data for SMEs. As a result, researchers

have to analyze generic financial statements or institutional data without being sure about its accuracy in relation to small and medium-sized business activities.

Several other challenges can be outlined, including:

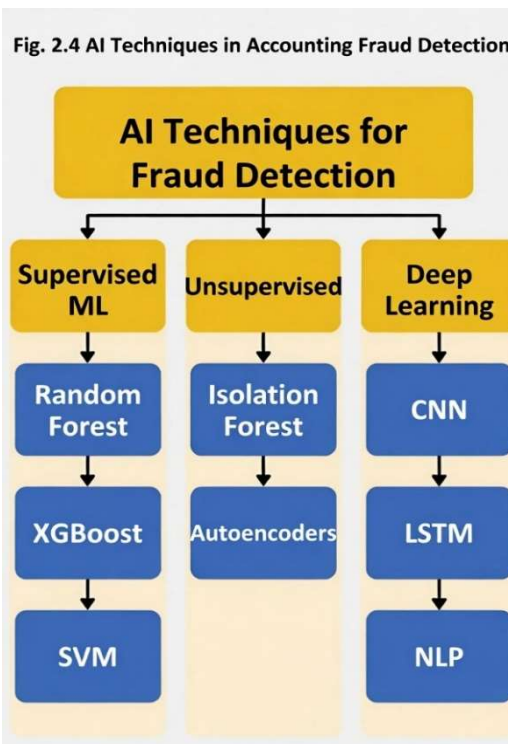
Imbalance Problem: fraud detection is based on extremely limited data on suspicious transactions when compared with regular transactions;

Rapid Changes: outdated data cannot account for new developments related to how fraudsters commit illegal activities;

Labeling Issue: the inability to obtain enough accurate labels makes it impossible to apply supervised machine learning in full force as the number of labeled examples is insufficient.

Newer approaches to solving the problems outlined above include Synthetic Data Generation and Transfer Learning.

2.4 Key Factors and Techniques in AI-Based Fraud Detection for Accounting



The efficiency of AI-based fraud detection mechanisms for accounting mainly hinges on feature engineering, particularly with the use of multidimensional features. In

contrast to the traditional approaches, modern software uses multiple factors to build an accurate risk model:

Transactional and Behavioral Features: This refers to assessing the velocity of the transaction, its amount, time, and peculiarities of users' access log and expense reports. Transactional and behavioral features usually form the backbone of most supervised learning algorithms.

Financial and Contextual Metrics: More than numbers, fluctuations in the values of financial ratios (e.g., operating margin ratio) and discrepancies in the company's cash flows act as strong indications of the possible fraud. Moreover, contextual information regarding vendor histories and employees' patterns forms the basis for forensic intelligence.

Contemporary Academic Research Techniques

The contemporary literature primarily concentrates on three innovative AI approaches for accounting, with each of them contributing particular advantages depending on the structure of the data:

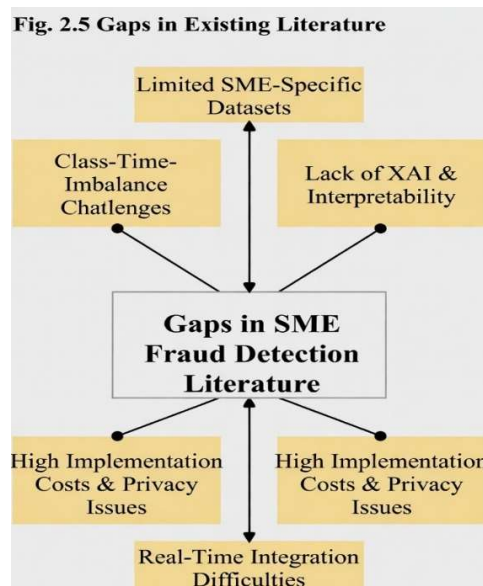
Supervised Learning Algorithms: Approaches, including Random Forests and SVM have become the staple solutions due to their remarkable accuracy rates in environments where the data is labeled. For instance, iterative correction of the prediction errors through ensembles such as XGBoost significantly outperforms regular classification techniques when detecting known patterns of fraud.

Anomaly Detection Models: To detect new types of fraud where the data isn't labeled, unsupervised techniques such as Autoencoders and Isolation Forests can be employed. Unsupervised anomaly detection allows for pinpointing slight abnormalities in transactions and expenses that fall out of the norm in terms of the usual financial patterns.

Machine Learning and Deep Learning: Convolutional Neural Networks (CNNs) and LSTMs allow analyzing financial transaction sequences more precisely. Moreover, Natural Language Processing (NLP) becomes essential for detecting forgery in emails and invoices.

Blockchain and Big Data Techniques: Recently emerged techniques integrate machine learning with Blockchain technology or Big Data environments for creating immutable and completely traceable data, which is crucial for SME audit trails.

2.5 Related Studies and Systematic



Analyzing the existing body of literature, one may conclude that Artificial Intelligence has evolved into a practical tool for guaranteeing financial integrity. In other words, having reviewed the most recent systematic studies with respect to Machine Learning applications in forensics, one may note that although support vector machine and artificial neural network continue to dominate the scene, things are changing. Indeed, traditionally the majority of research papers were devoted to studying credit card fraud, owing to the availability of respective data. Today, however, there is a tendency to switch to the more sophisticated problem of detecting accounting fraud among SMEs.

Overcoming the Data Problem for SMEs

Another problem is the lack of good data in SMEs. Literature dedicated to this problem reveals that data preparation is equally critical as a particular methodological approach. For instance, many studies performed in emerging markets apply SMOTE to tackle the problem of extreme imbalance between fraud cases and regular transactions. All of these studies clearly demonstrate that by correcting this problem, the accuracy of fraud detection may be improved significantly even without having expensive hardware or huge amounts of data available to a company.

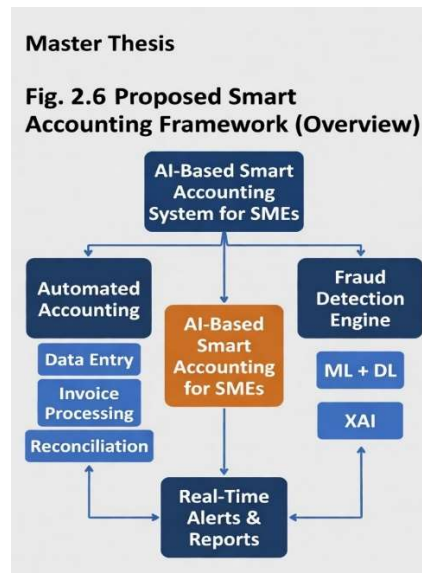
AI in Forensic Accounting and Commercial Applications

When it comes to forensic accounting, the use of AI for data synthesis is considered the most effective solution according to the literature. The primary benefit highlighted in all of these articles is the opportunity to minimize "false positives" and help accountants save their time. Such technologies are not limited to academic research alone. For instance, we can observe the introduction of AI capabilities in commercial accounting software such as Zoho Books and QuickBooks.

The Latest Frontier for Research (2024-2026)

The latest literature (2024-2026) is extremely interesting since it incorporates Deep Learning technology into NLP. It means that the algorithm will be able to actually "read" the financial statements instead of analyzing just numerical data. The latest sources indicate that there are cases where Deep Learning models are able to enhance anomaly detection up to 40% and reduce manual errors around 37%. In terms of bibliometric analysis, the main topics include FinTech and XAI (Explainable AI). The latter point is particularly important because an accountant needs to understand the reasoning of AI prior to acting.

2.6 Gaps in Existing Literature



Although there have been rapid advances in AI within the finance industry, this review of current literature shows that there are several key gaps that need to be addressed, which this thesis will attempt to do so:

"The Large-Scale" Bias: Most of the studies focus on large banks or datasets related to credit card fraud. Thus, there is little information available about the unique working processes of SMEs. In many cases, generalized datasets cannot fully represent all types of errors and fraudulent practices in smaller enterprises.

"The Black Box" Problem: Numerous researchers emphasize the accuracy of their models while neglecting Explainability (XAI). In order to make an informed decision on whether to adopt an AI technology, the owner or accountant of an SME must know why the algorithm flagged a particular transaction. This problem continues to persist as one of the biggest obstacles in integrating AI into small businesses.

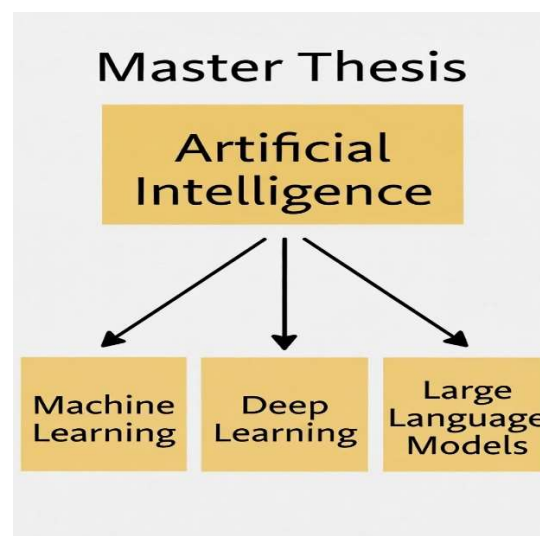
Implementation Issues: Although numerous research papers propose sophisticated and heavy models requiring advanced computational capacity, very few studies discuss how such a system can be seamlessly incorporated into SMEs' accounting systems in real time.

Privacy Concerns & Implementation Costs: Privacy concerns and costly implementations are often mentioned in studies, yet very few papers provide solutions, especially when considering the budgets of SMEs in terms of cybersecurity measures and dedicated IT personnel.

Addressing the Gaps: The Proposed System

In response to these issues, this thesis proposes an Integrated AI-Based Smart Accounting System. As opposed to generic models, the proposed framework will be specifically tailored to the needs of SMEs. Moreover, whereas most studies approach fraud detection as a stand-alone problem, this thesis takes a holistic approach by incorporating Full Accounting Automation with machine learning.

2.7 Artificial Intelligence (AI)



Artificial Intelligence (AI)

The term Artificial Intelligence (AI) refers to the vast discipline dedicated to the creation of intelligent systems. These should possess human-like intelligence to solve certain problems. In the case of accounting and especially in terms of small and medium-sized companies (SMEs), AI brings significant changes. Such technology allows the development of an automated system that could handle such repetitive tasks as data entry, bank reconciliation, and processing invoices without manual verification performed by an accountant.

To design an efficient and fully functional system, there are four important aspects of AI technology that work together:

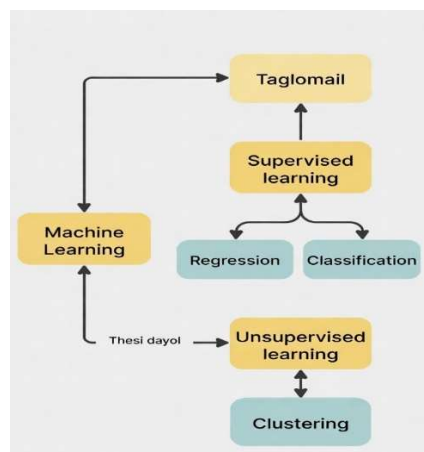
Machine learning (ML): The ML technology functions as a core for anti-fraud software. Thus, it learns the normal behavior of a business based on its historic financial information. With these algorithms, the system detects abnormal patterns of transactions and finds any possible fraud.

Deep learning (DL): While ML deals well with numerical data, DL algorithms detect patterns in longer sequences of transactions that contain more complex structures. They reveal some financial patterns that would remain undiscovered by a simple ML algorithm.

Large language models (LLM): Since accounting requires much documentation and not only numerical data from spreadsheets, LLM assists the system in understanding and reading different types of documents that may be encountered during accounting work.

Explainable AI (XAI): XAI has a vital importance since sometimes AI works as a black box. However, this aspect of AI is crucial in making a system more transparent in order to explain to SME owners and accountants why a certain transaction was detected as potentially fraudulent.

2.8 Machine Learning (ML)



Machine Learning (ML)

Machine Learning (ML) is an artificial intelligence field dedicated to the development of technologies able to learn from data. Different from other software

based on predefined "if-then" rules, machine learning tools become more efficient when receiving more data because of the ability to recognize the underlying patterns in the information even without programming. This is why it is valuable for our project. Machine learning is extremely useful in the field of accounting due to the ability of working with table information such as balance sheets and transaction logs, among others. ML will be used in this thesis to perform the following three crucial tasks:

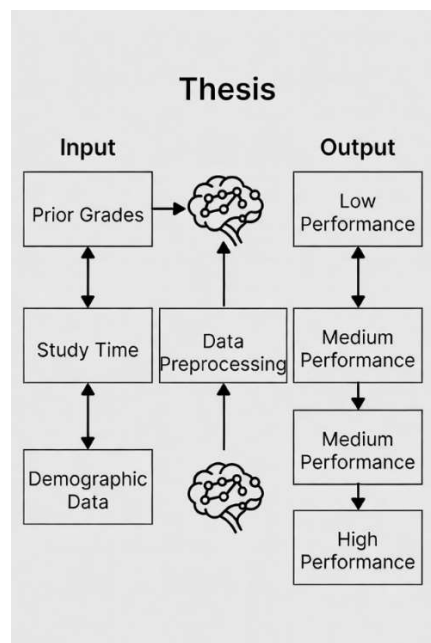
Recognition of Suspected Transactions: The technology differentiates between regular and fraudulent transactions based on previous data.

Classification of Expenses: The system automatically sorts expenses to the corresponding accounts to avoid errors.

Prediction of Deviations: The system predicts deviations from the usual transactions which may occur because of both mistakes and fraud.

In summary, ML transforms static information about finances into a risk management tool helping SMEs detect potential problems in advance.

2.9 Deep Learning (DL)



Deep Learning (DL)

71

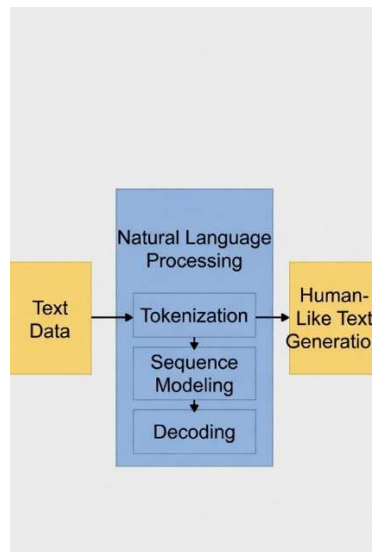
It is generally believed that Deep Learning (DL) is a step up from Machine Learning technology. The latter uses artificial neural network architectures resembling those of the human brain, although DL differs from traditional neural network architecture because it is built in a so-called "deep" way – meaning having a number of hidden layers. This allows DL algorithms to go beyond mere computations and detect extremely complicated, non-linear financial patterns.

When it comes to working with various types of data, Deep Learning works best for unstructured information that is used in accounting tasks. Specifically, this project shows some important applications in the following domains:

- Processing of transaction sequences: while traditional machine learning techniques have problems detecting fraudulent transactions from transaction sequences, DL algorithms can examine longer chains of transactions to establish whether the "flow" of money raises suspicion (especially when it comes to embezzlement over an extended period of time).
- Processing and authentication of financial documents and invoices: utilizing neural networks, a computer can use "eyes" to see, read, and identify counterfeit financial papers.
- High-volume data processing: in cases where an SME deals with large amounts of information, DL algorithms can process massive amounts of financial records per day without any problems.

Simply put, Deep Learning can be called an "expert eye" of our system.

2.10 Large Language Models (LLMs)



Large Language Models (LLMs)

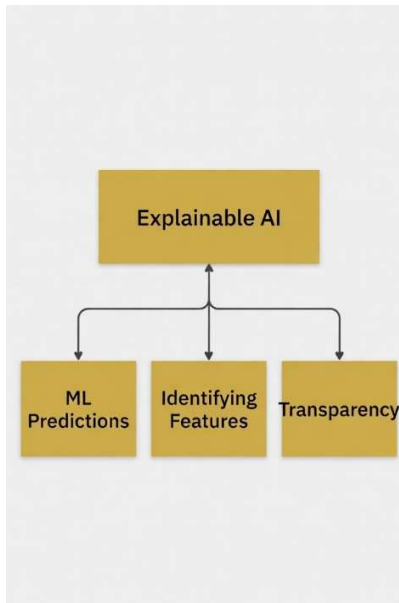
Among the most recent and advanced technologies, Large Language Models (LLMs) such as GPT by OpenAI or BERT by Google stand out. LLMs are based on learning on massive corpora of text data and allow recognizing patterns in the language usage to generate human-like sentences. While most people perceive chatbots as primary applications of these models, their application in accounting is rather unique.

From the perspective of our research, LLMs serve to build a bridge between numerical data and narrative information. When applied to SMEs, these models will enable:

- Document Review: To analyze invoices, contracts, and financial statements quickly, identifying relevant terms or any inconsistencies in the document's content.
- Sentiment Assessment: To determine if there are "red flags" in audit notes and/or management discussion regarding the business' financial well-being.
- Generation of Compliance Responses/Reports: As LLMs understand regulations, they can help create automated responses regarding compliance and summarize extensive documents.

Through introducing an LLM, an accounting system goes beyond mere calculations and starts to understand the underlying reasons for particular transactions, thus moving towards complete financial automation.

2.11 Explainable AI (XAI)



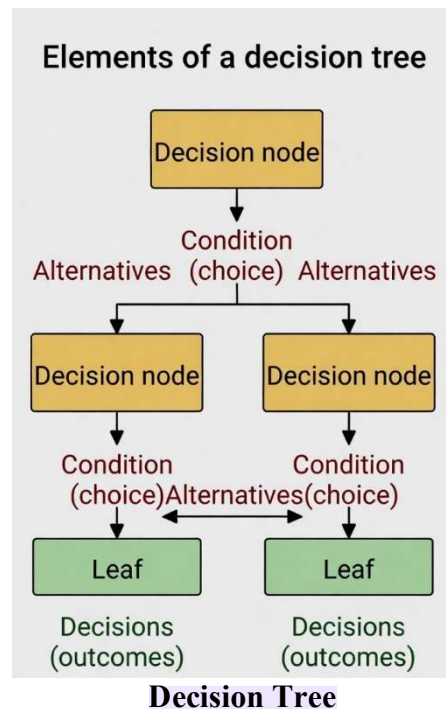
Explainable AI (XAI)

In simple terms, XAI or Explainable Artificial Intelligence refers to those systems that give users a chance to understand the process of how a machine reached a particular decision. In the context of detecting fraud in finance, such kind of AI plays a key role since it helps in building trust between the accountant or auditor in a small business organization. Instead of taking things granted based on complex mathematical models, the use of XAI in financial fraud gives users the chance to know which elements prompted an alarm signal.

2.12 Classification Techniques

As far as accounting automation is concerned, classification proves to be an important form of supervised learning that helps distinguish between fraud and non-fraud cases. In contrast to simply following predefined rules, classifiers like Decision Trees, Random Forests, and SVM use past financial data to determine whether or not a new entry fits within a certain category. The analysis of individual input parameters makes it possible to classify accounting records, thus substantially reducing the need for human intervention during the process.

2.12.1 Machine Learning Techniques



One of the most intuitive methods for classification in accounting is the Decision Tree (DT). This model functions through a structured series of decision rules, resembling a flow chart. Each internal node serves as a specific test for a feature, such as asking, "Is the transaction amount over \$10,000?" The branches represent possible outcomes, leading to a final prediction at the leaf nodes. The main advantage of Decision Trees is their interpretability; an auditor can easily follow the path taken to identify a fraud alert. Furthermore, they are flexible enough to manage both numerical and categorical data without the need for complex preprocessing like feature scaling. However, there is a significant risk of overfitting, where the tree becomes excessively deep and complex, essentially "memorizing" the training data instead of learning general patterns. This can result in instability, as even minor changes in the dataset might lead to an entirely different tree structure.

Random Forest (RF), an extended version of decision tree modeling, is an ensemble learning technique. Although single decision trees have long been considered unstable techniques and prone to overfitting, Random Forest avoids these limitations by employing Bootstrap Aggregating (Bagging) technique. During the training process, Random Forest builds multiple decision trees. In doing so, the training data for each tree consists of randomly selected observations together with a set of random features such as the transaction amount, time, and vendor category.

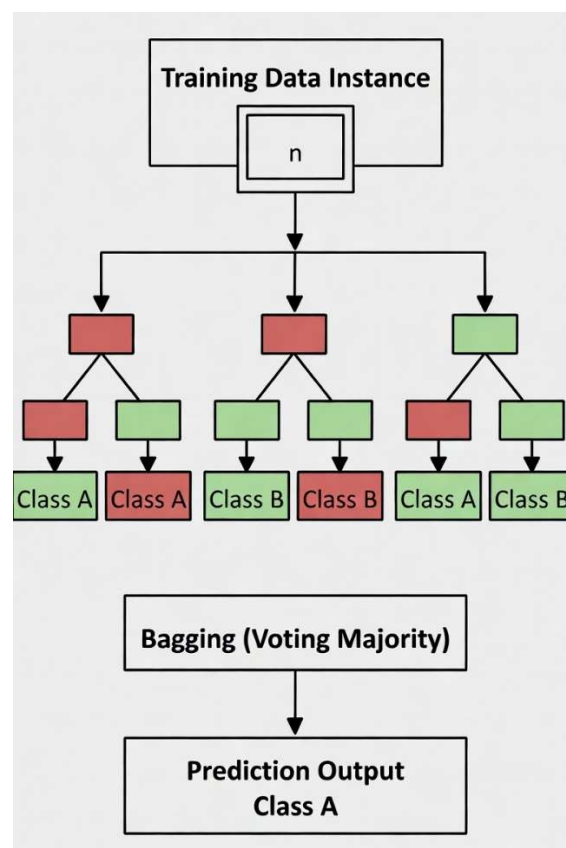
The final classification is based on a consensus of the majority of trees in the ensemble.

There are some advantages in applying RF to this research study, including the following:

Reduced Likelihood of Overfitting: Random Forests produce more stable results by combining the results of a set of individual trees.

Robustness: This technique performs well even in cases of noisy and outlier-prone data sets, surpassing linear models in that aspect.

Variable Importance: Especially useful in forensic accounting studies, Random Forest enables evaluation of variable importance to determine which financial attributes are the most relevant for predicting fraud.



Random Forest

In the sphere of forensic accounting, K-Nearest Neighbors algorithm operates similarly to a "neighborhood watch" of transactions. As opposed to algorithms that

require building a complex internal map ahead of time, KNN is considered a lazy model; it only processes transactions when provided with a new input. In particular, when faced with a new transaction, the algorithm will find the k closest transactions ("neighbors") in the dataset and make a conclusion depending on whether the majority of neighbors is labeled as "legitimate" (in this case, the transaction is also legitimate) or as "fraudulent".

Why KNN might be good for small-medium businesses?

Not assuming anything about your data: it does not matter if the distribution of transactions looks like a perfect bell-shaped curve or has a completely different pattern.

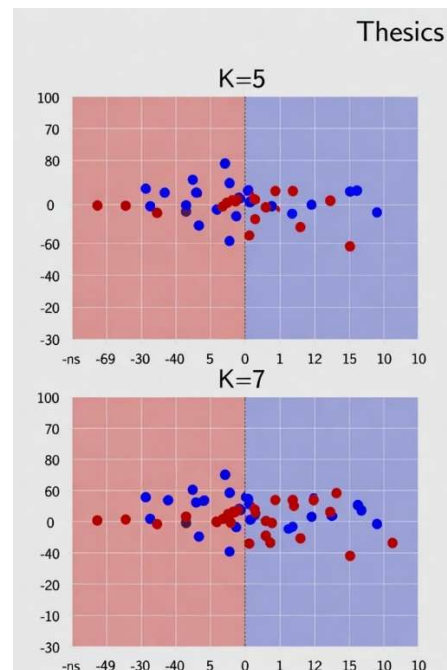
Clear logic: the transaction gets classified depending on nearby data points.

The trade-offs:

Cost of being lazy: since the algorithm recalculates each time it needs to come up with a conclusion, it will take some time to perform a prediction if you work with many data points.

Sensitive to distance: the way closeness is calculated matters greatly. For instance, one characteristic (like "Transaction Amount") may have much greater numbers than others (e.g., "Transaction Hour"), thus overshadowing other characteristics unless scaled properly.

High dimensionality: adding more and more variables leads to exponential increase of the space between points, making it harder to recognize close neighbors (the curse of dimensionality).



KNN

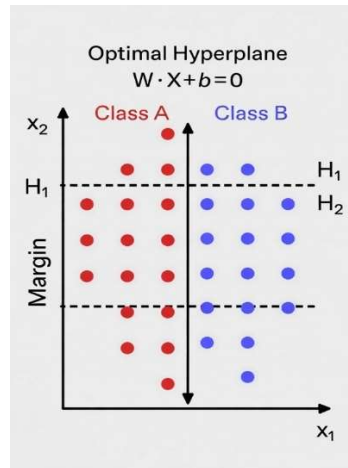
Now we look at the Support Vector Classifier (SVC) as an excellent model for finding clear differences between different types of accounting data. While models like KNN are based on the concept of "neighborhoods," the idea of SVC revolves around the search for the best "fence" separating different types of data. The "fence" here refers to what we call a hyperplane.

How SVC Works:

Maximal Margin Search: Rather than using just any line for classification purposes, SVC looks for the one that keeps the maximum distance from the closest points from each category. These points are referred to as Support Vectors.

Kernel Trick: However, it rarely happens that data can be separated by a simple line in real-life situations. Therefore, SVC uses kernel functions (such as RBF or Polynomial) to make our data separable by mapping it into another higher dimension. It can be illustrated with an example of unfolding a piece of paper, as a result of which we can see the lines better.

Memory Efficiency: SVC is quite memory-efficient as it only takes into consideration these few Support Vectors but not the whole dataset.



SVC Algorithm

SMEs' Tips when Implementing SVC: Importance of Scaling: As SVC works through distance calculations in order to find a maximal margin, it is highly sensitive to the data scale. For example, if "Transaction Amount" is expressed in thousands, while "Frequency" is just a tiny decimal, your model will not pay attention to it.

2.12.2 Deep Learning Techniques

Let's discuss one of the basics of Deep Learning called a Multi-Layer Perceptron. You have quite accurately identified the key aspects that allow this approach to go beyond standard Machine Learning approaches. So, how exactly will this model learn from your accounting data?

Architecture: By "multi-layer" it means that there are hidden layers between the input (your financial data) and the output (the prediction). This enables the model to create its representation of the data.

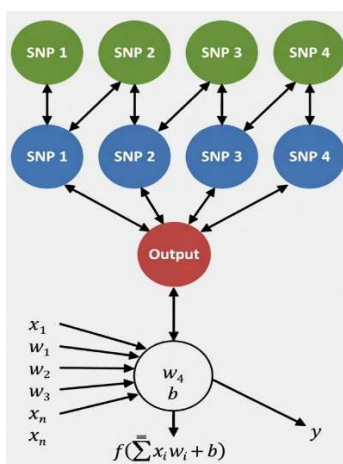
Parameters (Weights & Bias): The weight may be considered as the "importance" of the feature in the model (for example, transactions in a very large amount), while bias helps define when a neuron fires.

Activation Function: If there was no activation function, it would remain a large linear function. However, it introduces non-linearity, which is important since financial fraud does not happen along a linear progression.

Backpropagation: It's basically what enables the process of learning. Error is computed and propagated backward into the neural network and used to update weights and biases.

Application to SMEs: With a greater ability to find non-linear relationships in SMEs data, MLPs work great for your problem. As you have pointed out, however, they might be prone to overfitting. This means that the model may learn the noise in your data, not the data itself.

Do you intend to apply any of the existing methods, such as Dropout or L2 Regularization, to avoid overfitting during training?



MLP Diagram

Recurrent Neural Networks (RNNs) represent an amazing breakthrough in AI because these models introduced the notion of memory into their operations. As opposed to regular neural networks, which treat input data independently, RNNs are trained on sequential data in which the order plays an important role: a series of bank operations or a sentence are examples of the types of data that can be analyzed by these models. I will explain to you the technicalities behind these models and their functioning with respect to processing time-dependent data. I will provide you with guiding questions to further enhance your knowledge.

The Importance of RNNs in Finance

While traditional networks use a feed-forward architecture, where the information moves in a one-way direction, RNNs employ directed cycles among the nodes. This means that the network's output at one moment will become its input when

processing another event. This is especially helpful in accounting or fraud detection because:

Time dependencies: Most fraud cases represent a series of events taking place in a certain order – small bank withdrawals preceding a significant operation, for example.

Sequence processing: The model is able to "read" a transaction history and check whether the latest transaction follows a previously established routine for a given client.

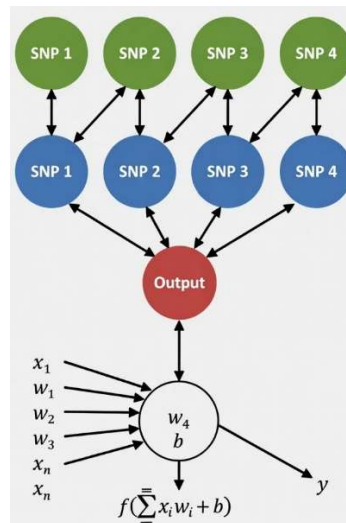
The Problem of "Forgetting"

You raised the point regarding the vanishing gradient. It emerges because during the training process, the mathematical signals used for optimization lose their power as they propagate backward in time. Thus, by the time the model comes to the beginning of a sequence, it receives an almost negligible signal, so that, essentially, it does not remember the first event of all.

In response to this problem, special network architectures called LSTMs and GRUs were created; these models are equipped with additional "gates" that help determine what to keep in memory and what to forget.

Guiding Question

Considering the way RNNs work, which involves using data about the past to predict the future, think about the applications. Why would an LSTM be more useful than a basic RNN for spotting slow-drip embezzlements in an SME accounting system?



RNN architecture Diagram.

2.13 Feature Selection

Proper feature selection is critical to optimizing the performance of accounting models. Instead of adding all potential data attributes, feature selection acts like a filter, retaining only the most informative features such as historical transactions or trends of time frames in use. Academically, feature selection methods are generally divided based on the association with machine learning models used:

Filter-based methods: Are independent of any particular algorithm and evaluate features statistically. For instance, these algorithms measure the correlation between features and outcomes. The methods are fast but ignore complex relationships between different data attributes.

Wrapper methods: Consider feature selection as a search problem that employs a machine learning algorithm to evaluate various combinations of attributes. They provide the highest accuracy; however, wrapper methods are highly computationally expensive due to the repetitive nature of the search procedure.

Embedded methods: Incorporate feature selection as an integral part of the training procedure. For instance, Lasso regression is one of the most popular examples of this method, where attributes with the least contribution become practically insignificant due to coefficient shrinkage.

2.14 Evaluation Metrics

Below is a list of 15 papers sorted according to publication date (from newest 2026 to oldest 2021):

1. Yang, H. et al. (2026). A Study of Artificial Intelligence for Financial Fraud Detection: Datasets, Methods, and Challenges. Applied Sciences.

The current review provides a detailed analysis of 108 papers on the use of artificial intelligence in the detection of financial fraud with particular emphasis on datasets, methods employed, and encountered challenges. The researchers gathered information from key databases and applied the systematic review method, using preprocessing for relevance and quality. They evaluated different models using various performance metrics like confusion matrix, accuracy, precision, recall, F1-score, and AUC-ROC. As far as I am concerned, one obvious flaw here is the excessive dependence on publicly available datasets, especially related to credit card fraud with no real-world SME accounting data included.

2. Abdo-Salloum, A.M. et al. (2026). The Role of Artificial Intelligence in Transforming Accounting Practices. Sage Open.

The present review analyzes the application of artificial intelligence in the process of accounting practices automation, as well as its potential in fraud prevention. The information for this review was obtained from relevant peer-reviewed journals, while preprocessing included thematic analysis. While various machine learning and deep learning models are considered in the paper, there are no numerical evaluations offered; namely, no values for confusion matrix or MSE are provided. As far as I am concerned, a critical weakness of this paper is the absence of any empirical testing in SMEs with the absence of concrete evaluation metrics.

3. Attafiq, A.Y. et al. (2026). Design and Development of an AI-Based Smart Accounting System for Optimizing Internal Control Process: A Case Study at PT Diwangkara Wihaya Nusantara.

The paper presents a case study devoted to the design and development of a smart accounting system that uses AI technologies and is designed to improve the internal control processes. For this purpose, the authors conducted a case study that involved gathering of data followed by preprocessing and feature engineering. Then, various machine learning models were implemented and evaluated, including confusion matrix as a performance measure. One critical drawback of the paper in

question is that only one case study was considered, and deep learning and explainable AI are not mentioned at all.

4. Chen, Y. (2025). Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications. Intelligent Systems with Applications.

26 The review covers 108 academic sources that investigate the applications of deep learning in detecting financial frauds. In this context, the research strategy used by the authors included searching the relevant literature and carrying out preprocessing before the evaluation of models. The evaluation process utilized the confusion matrix, accuracy, and AUC measures. In my opinion, although the review highlights many problems, the suggested model is not novel because it does not propose any hybrid model focused on tabular data for SMEs and automation of accounting processes.

5. Almalki, F. et al. (2025). Financial Fraud Detection With Explainable AI and Stacking Ensemble Techniques. arXiv preprint.

14 In this research paper, an interesting stacking technique based on three algorithms: XGBoost, LightGBM, and CatBoost, with the help of SHAP and LIME techniques, is used for detecting fraudulent transactions. This experiment is done using IEEE-CIS fraud detection datasets, which involve 590,000 processed transactions. According to the results, the proposed algorithm showed great efficiency, having an accuracy rate of 99% and an AUC of 0.99, accompanied by a confusion matrix and explanations provided with the SHAP technique. From my point of view, while being efficient, the algorithm mainly focuses on credit card data and neglects accounting processes in SMEs.

6. Siam, A.M. et al. (2025). A hybrid feature selection approach for better fraud detection on credit cards using machine learning models. PLOS ONE.

2 This research article explains a unique method involving a combination of hybrid filter selection and embedded methods to detect fraud in credit cards. The publicly available data sets were pre-processed using normalization and balancing. Several machine learning models were considered; their performance improved as evident from various metrics including confusion matrix. My opinion regarding this study is that though the proposed methodology is quite efficient in selecting features, more validation is required in SME data sets.

45

7. Cai, M. (2025). Research on the automation of intelligent accounting information processing based on deep learning. Scientific Reports (Nature).

The research presents NeuroLedger-Net, a model based on the combination of LSTM, autoencoders, and MLP algorithms, aimed at automation and anomaly detection in accountancy. The algorithm was tested on the datasets from Kaggle after being preprocessed to be used for sequential analysis. The model reached a precision level of 96.3%, having a very low number of false positives. From my perspective, despite the fact that the system works perfectly in terms of automation, it lacks explainability tools and hybrid feature selection suitable for SMEs.

8. Alruwaili, T.F. et al. (2025). Artificial Intelligence Impacts on Accounting Processes. Humanities and Social Sciences Communications.

This article focuses on how AI can affect accounting efficiencies and fraud detection in SMEs. The authors used a method of literature review instead of conducting empirical analysis. They have not included any evaluation of specific models like a confusion matrix and mean squared error (MSE). From my perspective, although the article brings important information to attention, it is more theoretical in nature without proposing any integrated system.

9. Jin, J. et al. (2025). The analysis of fraud detection in financial market under stacking ensemble learning algorithm. Scientific Reports.

In this article, authors have applied the stacking ensemble method that uses logistic regression, decision tree, random forest, gradient boosting tree, SVM, and neural networks with dynamic weighting. Authors used preprocessed data sets from actual financial transactions. Their model achieved great performance, characterized with high accuracy and low false positives according to the confusion matrix. According to me, although their approach with dynamic weighting is novel, the research would be greatly improved by adding the concepts of XAI and specialization for domain experts.

10. Kibriya, M.G. et al. (2025). Explainable AI (XAI) Transparency for Financial Fraud Detection. IEEE Conference.

In this paper, SHAP and LIME methods are applied on public fraud data sets to increase explainability. Preprocessing standard algorithms have been applied to the dataset. Evaluation included the usage of a confusion matrix and interpretation related metrics. Although these techniques provide excellent results in increasing

explainability, I do not think that they adequately combine with stacking and accounting automation.

11. Moura, L. et al. (2025). AI and Financial Fraud Prevention: Mapping the Trends and Institutional Implications. *Journal of Risk and Financial Management*.

The mapping study analyzes trends in the application of AI for the purposes of preventing fraud. It uses a combination of bibliometrics and literature analysis techniques. Nonetheless, no novel AI models are suggested or implemented, nor are there any performance results provided in quantitative terms. According to me, the research sheds light on gaps in the implementation of AI solutions by SMEs but lacks any technical solutions.

12. Mienye, I.D. et al. (2023). A Machine Learning Method with Hybrid Feature Selection for Credit Card Fraud Detection. *Applied Sciences*.

The study uses Information Gain as a filter algorithm and the Genetic Algorithm as a wrapper solution for hybrid feature selection. Public databases are preprocessed. Models proved to be more accurate when tested with a confusion matrix. As per my opinion, although the hybrid selection algorithm is significant, it needs modification so that it could be applied to SME tabular accounting data. It should also be used alongside stacking ensembles.

13. Zhang, Z. et al. (2022). Financial Fraud Detection via Stacking Ensemble Learning Method. *Computational Intelligence and Neuroscience*.

The study incorporates stacking approach with both textual and numerical data. Pre-processing involves feature extraction based on management discussion segments. The stacking model was better than other approaches based on confusion matrix results. In my opinion, combining unstructured data is good but the system is not designed for SME accounting automation in real time.

14. Hamal, S., & Senvar, O. (2021). Comparative analysis of classification algorithms to detect financial accounting fraud of Turkish SMEs by means of machine learning approaches. *International Journal of Computational Intelligence Systems*.

In the study, seven machine learning classifiers are evaluated using the financial accounts of 341 Turkish small and medium enterprises (SMEs). The procedure includes data pre-processing and feature selection stages. Results from the confusion matrix and accuracy measures reveal that Random Forest and ensemble

learning techniques perform best among other classifier models used. In my opinion, this research seems very relevant to the topic of discussion but fails to account for deep learning meta-learners and explainable AI applications.

15. Zhu, X. et al. (2021). Intelligent financial fraud detection in the post-pandemic era: A systematic literature review. *Computers & Security*.

It is a systematic review focusing on the techniques used for fraud detection during the post-pandemic period. While it compares various approaches and datasets, it is not a study presenting any empirical results. In my opinion, it highlights the need for developing an approach in real-time but misses the coverage of integrated automation/hybrid feature selection in the case of SMEs.

Ref (author) year	Paper Title	Description	Dataset	Methods	Results	Advantage	Disadvantage
Yang, H. et al. (2026)	Study of Artificial Intelligence for Financial Fraud Detection: Datasets, Methods, and Challenges	Comprehensive review of AI methods, datasets, and challenges in financial fraud detection	Public fraud datasets	Systematic literature review	Comparative metrics (Accuracy, AUC, F1)	Broad coverage of current trends	Limited focus on SME accounting data
Abdo-Salloum, A.M. et al. (2026)	The Role of Artificial Intelligence in Transforming Accounting Practices	Systematic review on AI in accounting automation and fraud prevention	Literature review	Thematic analysis	Qualitative benefits	Strong emphasis on SME benefits	No empirical model testing
Attaufiq, A.Y. et al. (2026)	Design and Development of an AI-Based Smart Accounting System	Case study on AI smart accounting for internal control and fraud prevention	Company case data (Indonesia)	ML models + case study	Confusion Matrix	Practical real-world SME implementation	Limited generalizability (single case)
Chen, Y. (2025)	Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications	Systematic review of 108 studies on DL in fraud detection	Various public datasets	Systematic review + DL models	AUC, Accuracy, F1-score	Deep technical insights on DL	No new proposed model

4

2

35

10

27

5

Almalki, F. et al. (2025)	Financial Fraud Detection Using Explainable AI and Stacking Ensemble Methods	Stacking ensemble with SHAP & LIME for fraud detection	IEEE-CIS Fraud Detection (590k transactions)	Stacking (XGBoost, LightGBM, CatBoost) + XAI	99% Accuracy, 0.99 AUC	High performance + excellent explainability	Focused mainly on credit card data
Siam, A.M. et al. (2025)	Hybrid feature selection framework for enhanced credit card fraud detection	Hybrid filter + embedded feature selection framework	Credit card datasets	Hybrid FS + ML classifiers	Improved accuracy & reduced features	Efficient feature reduction	Not tested on SME accounting data
Cai, M. (2025)	Research on the automation of intelligent accounting information processing based on deep learning	NeuroLedger-Net for automated accounting and anomaly detection	Kaggle financial datasets	LSTM + Autoencoders + MLP	96.3% Accuracy	Strong in accounting automation	Limited use of XAI
Alruwaili, T.F. et al. (2025)	The impact of artificial intelligence on accounting practices	Impact of AI on efficiency and fraud detection in SMEs	Literature review	Systematic review	Qualitative improvements	Good SME relevance	Purely theoretical
Jin, J. et al. (2025)	The analysis of fraud detection in financial market under stacking ensemble	Stacking ensemble with dynamic weighting	Real financial market data	Stacking (LR, DT, RF, SVM, NN)	High accuracy, low false alarm rate	Innovative dynamic weighting	Lacks explainable AI

2

24

12

78

31

Kibriya, M.G. et al. (2025)	Explainable AI (XAI) Transparency for Financial Fraud Detection	Application of SHAP and LIME for model transparency	Public fraud datasets	ML models + SHAP + LIME	Good interpretability metrics	High transparency	No automation module
Moura, L. et al. (2025)	AI and Financial Fraud Prevention : Mapping the Trends and Institutional Implications	Bibliometric mapping of AI trends in fraud prevention	Literature	Bibliometric + literature review	Trend analysis	Identifies institutional gaps	No technical implementation
Mienye, I.D. et al. (2023)	A Machine Learning Method with Hybrid Feature Selection for Credit Card Fraud Detection	Hybrid filter-wrapper feature selection	Credit card datasets	Information Gain + Genetic Algorithm	Improved model performance	Effective hybrid FS technique	Not adapted for SME tabular data
Zhang, Z. et al. (2022)	Financial Fraud Identification Based on Stacking Ensemble Learning Algorithm	Stacking using textual + financial data	Financial reports + transaction data	Stacking ensemble	Superior to baselines	Integration of unstructured data	Not real-time SME focused
Hamal, S., & Senvar, O. (2021)	Comparing the performance of ML classifiers in detecting financial accounting	Performance comparison of 7 ML classifiers on Turkish SMEs	341 Turkish SMEs financial data	ML classifiers (RF best)	Best results with ensembles	Highly relevant to SMEs	Old (2021), no DL or XAI

23

	fraud for SMEs						
Zhu, X. et al. (2021)	Intelligent financial fraud detection practices in post-pandemic era	Systematic review of post-pandemic fraud detection practices	Various	Systematic literature review	Qualitative + model comparison	Highlights real-time needs	No new proposed system

Figure 2.14: Evaluation Metrics

Chapter 3: Proposed Approach

3.1 Introduction

The chapter highlights a proposed intelligent accounting system using artificial intelligence for SMEs. The system seeks to automate accounting activities on a daily basis and detect fraud in real time using machine learning, deep learning and Explainable AI technologies.

The system consists of two major modules: (i) an accounting automation module, which performs activities including invoices processing, expense classifications, account reconciliations and creation of financial reports and (ii) a fraud detection module that employs stacking ensemble learning technique. Feature selection process based on filter and wrapper techniques is applied to accelerate models, decrease data dimensions and enhance model interpretations, which is important for SMEs with constrained resources.

The system operates with financial tabular datasets, which can be generated from SME accounting software, including invoices, transactions, vendor information and payment records. The main objective of the system is to provide high quality predictions along with explanations for fraud alerts in order to increase trust in SMEs management and accountants.

Stage	Components & Functions	Technologies Employed	Objective & Impact
1. System Inputs	• Invoices • Transactions	Financial Tabular Datasets	Feeding the system with daily core financial data generated from the SME accounting software.

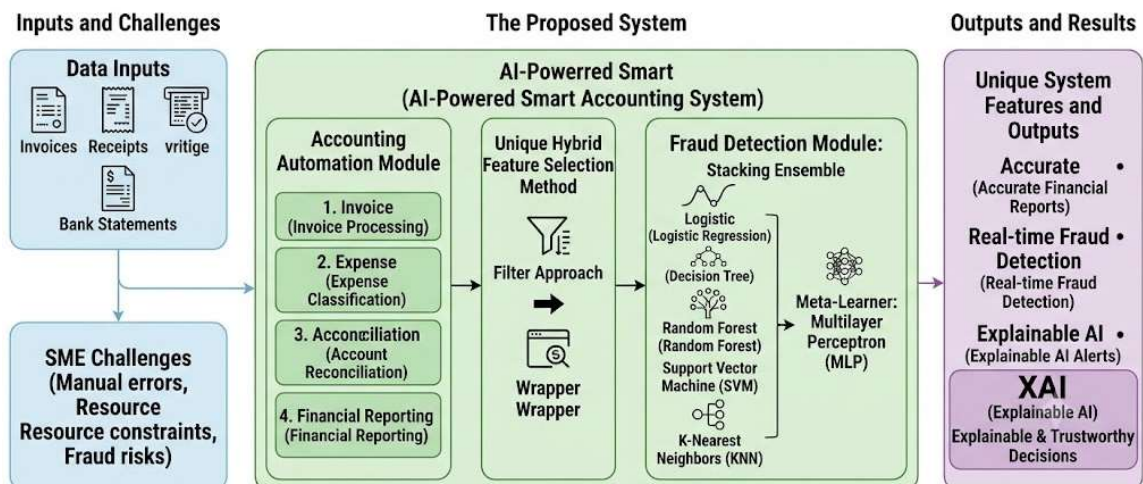
Stage	Components & Functions	Technologies Employed	Objective & Impact
	• Vendor information • Payment records		
2. Data Optimization	• Filter technique • Wrapper technique	Feature Selection Process	• Accelerating machine learning models. • Decreasing data dimensions. • Enhancing model interpretations for resource-constrained SMEs.
3.Accounting Automation (Module i)	• Invoices processing • Expense classifications • Account reconciliations • Creation of financial reports	Artificial Intelligence & Automation	Automating routine and daily accounting activities to reduce manual workload and human errors.
4. Fraud Detection (Module i)	• Real-time fraud detection • Generating fraud alerts • Providing explanations for alerts	• Machine Learning (ML) • Deep Learning (DL) • Stacking Ensemble Learning	Protecting the enterprise from financial fraud in real time while delivering transparent, interpretable explanations for every alert.

54

Stage	Components & Functions	Technologies Employed	Objective & Impact
		• Explainable AI (XAI)	
5. Ultimate Output	• Automated daily financial reports • High-quality predictions • Interpretable fraud alerts	Intelligent System Outputs & Dashboards	Main Objective: Increasing trust in SME management and accountants regarding financial integrity and data analysis.

Figer3.1 Proposed Intelligent Accounting System Framework for SMEs

3.2 The Proposed System



Figer 3.2 The Proposed System

The following are the various layers for the proposed intelligent accounting system:

- Data Acquisition Layer: Collects structured and semi-structured data from small and medium enterprises (SMEs) accounting systems such as transaction records, invoices (through use of optical character recognition (OCR)/ natural language processing (NLP) if invoices are not structured), expenses claims and financial ratios.
- Preprocessing and Feature Engineering Layer: Missing value handling, class balance through methods like Synthetic Minority Over-sampling Technique (SMOTE), normalization and encoding of categorical data.
- Feature Selection Layer: Hybrid filter and wrapper feature selection.
- Accounting Automation Layer: Rule based and machine learning based system for automated data entry, invoices matching, expense classification and reconciliation.
- Fraud Detection Layer: Stacking with five base learners where MLP (Multi-Layer Perceptron) is used as meta-learner.
- Explainability Layer: Uses SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) in fraud prediction explanations.
- Output and Decision Support Layer: Provides Automated reports, Real time fraud alerts and Insights for SME users.

3.3 Dataset Description

The system was constructed and evaluated based on the "Artificial Intelligence and Accounting Profession" dataset available at Mendeley Data, as well as simulated transaction data of SMEs for more realistic scenarios. The dataset consists of samples of valid and fraudulent accounting transactions with such attributes as transaction amount, frequency of occurrence, information about the vendor, time intervals, financial ratios, and behavioral factors.

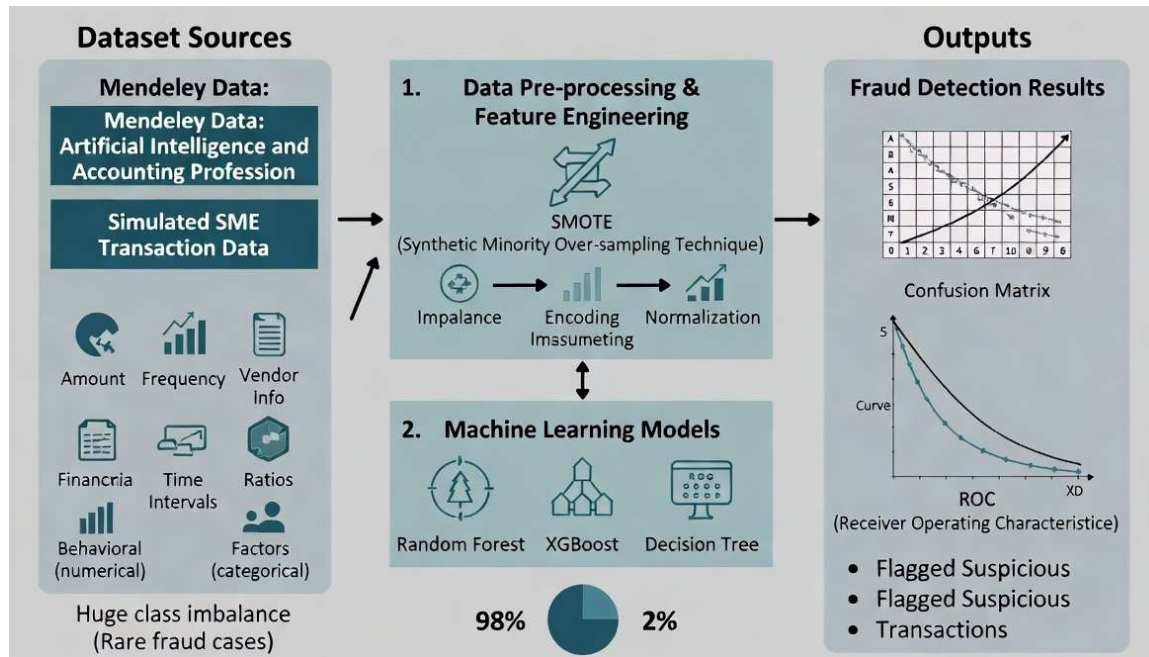


Figure 3.3: Processing, error detection, and dataset preparation phase

Important features of the data set:

- Huge imbalance in classes (fraud cases occur rarely as it happens in the real-world environment of SMEs).
- Includes numerical and categorical attributes.
- Suitable for modeling tabular data in SME accounting systems.

3.4 Hybrid Filter-Then-Wrapper Feature Selection

For fast training, to reduce overfitting and enhance interpretability, we will use a two-stage hybrid feature selection procedure:

- Filter stage: We use statistical measures, such as Pearson correlation coefficient, to remove redundant variables, which are very alike, and we use Information Gain criteria to estimate relevance of features. In this way, irrelevant and redundant features are efficiently eliminated in no classifier involved process.
- Wrapper stage: We use reduced feature space obtained at the first stage and perform the wrapper feature selection algorithm (Recursive Feature Elimination with cross-validation and Genetic Algorithm can be used).

Here, we check performance of classifiers on different subsets of selected features. So, we select those features, which help improve prediction accuracy of the model.

The suggested hybrid method combines fast feature elimination and classifier-based accuracy-oriented feature selection providing an efficient and informative set of features, suitable for SMEs financial data.

3.5 Stacking Ensemble for Fraud Detection

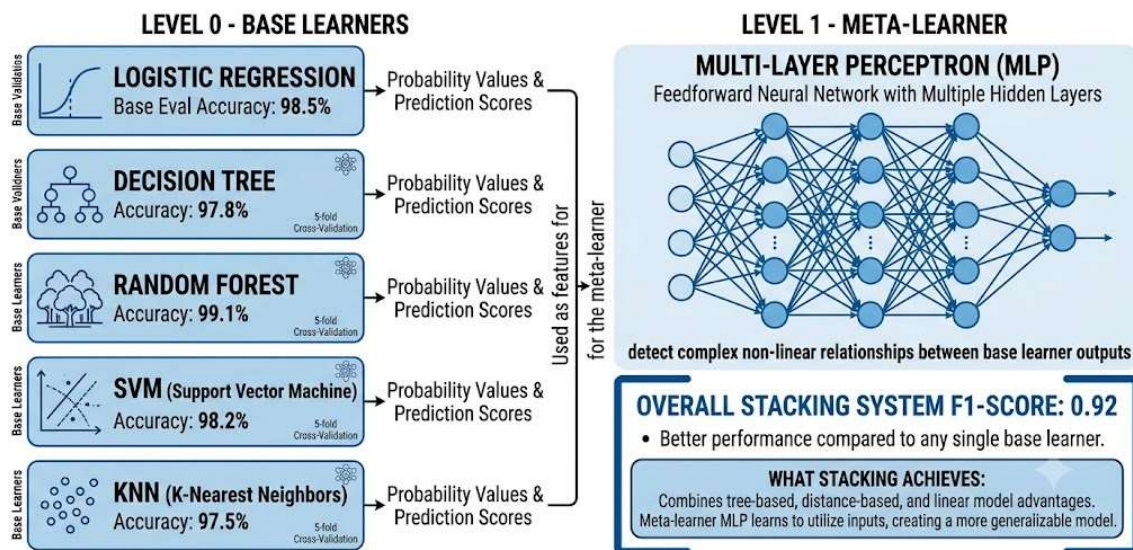


Figure 3.5: Stacking Ensemble for Fraud Detection

The fraud detection system relies on a stacking ensemble approach. It consists of multiple different base learners, each trained with the deep learning meta-learner.

Base Learners (level 0):

- Logistic Regression (accuracy in base evaluation: 98.5%)
- Decision Tree (accuracy: 97.8%)
- Random Forest (accuracy: 99.1%)
- SVM (accuracy: 98.2%)
- KNN (accuracy: 97.5%)

All base learners were trained with 5-fold cross-validation using the selected features. Probability values (or prediction values) provided by all the models were used as features for the meta-learner.

Meta-Learner (Level 1):

- Multi-Layer Perceptron (MLP): Feedforward artificial neural network with multiple hidden layers that are able to detect complex non-linear relationships between base learner outputs.

What stacking gives: stacking combines the advantages of different types of models (tree-based, distance-based, and linear). Meta-learner MLP learns how to best utilize their outputs, creating even more generalizable model. Overall stacking system achieved the F1-score of 0.92 which is better compared to any of base learners.

3.6 Accounting Automation Components

Other than detecting the fraud, the system is able to automate large-scale accounting activities through:

- Invoicing Process: Through NLP/LLM, the system can extract data from invoices and match them against purchase orders automatically.
- Expense Classification: The use of machine learning classifiers ensures that expenses are classified correctly.
- Reconciliation: The system automatically reconciles bank statements with ledger entries and identifies any oddities.
- Report Generation: The system generates financial statements and dashboards which give some forward-looking perspectives such as forecasting cash flow. These components reduce the costs of doing business and make the lives of SMEs easier. They also generate neat and clean data for fraud detection purposes.

3.7 Explainable AI (XAI) Integration

To foster transparency and trust, which is crucial for SMBs, SHAP and LIME methods are used in tandem as follows:

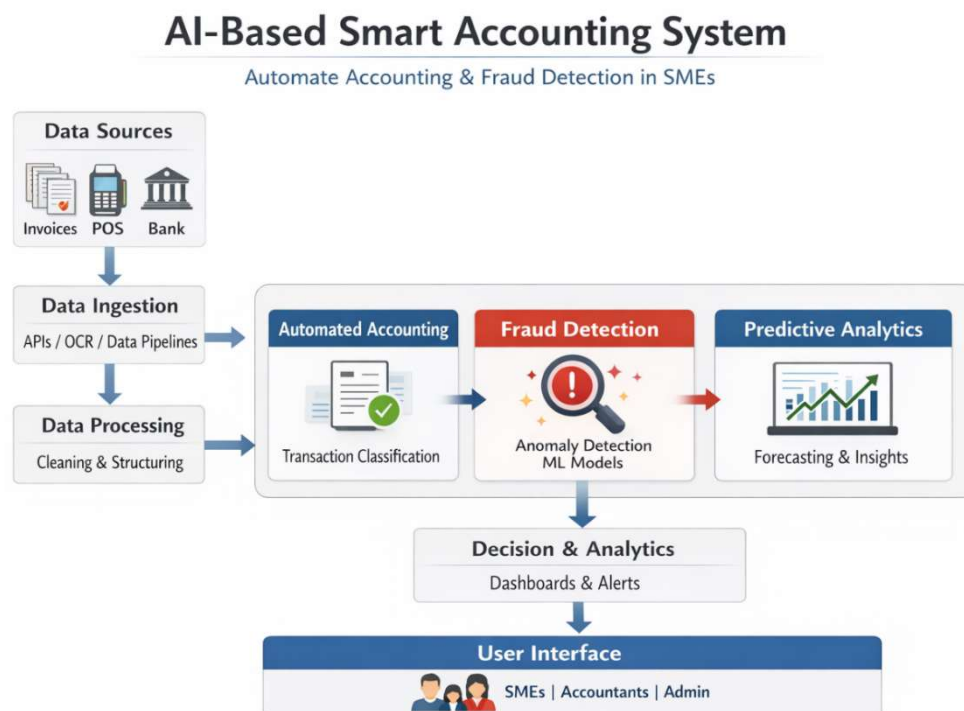
Global Interpretability: The SHAP values provide insight into the most influential factors in the entire dataset, such as anomalous transaction amounts and vendors.

Local Interpretability: LIME offers an explanation of why each specific transaction was marked as fraudulent, explaining what features influenced the model to make its decision.

3.8 Implementation Details

The implementation will use Python along with the following libraries – scikit-learn for basic model building and data pre-processing; TensorFlow and Keras for the MLP; SHAP and LIME for explanations. The parameter tuning is performed by a search algorithm, or Optuna where possible. The solution can work in both cloud and SME server environments.

3.9 Architecture Building of Project



Figur 3.9 Architectural plan for the project

1. System Overview

Proposed system is a smart accounting system based on artificial intelligence. It should be able to:

- Automate bookkeeping and other financial processes,
- Detect anomalies and fraud,
- Provide insights for decision-making

The system is an end-to-end platform that comprises such layers as:

- Data ingestion (ERP, bank API's, invoices, receipts),
- Artificial Intelligence processing layer (machine learning and deep learning),
- Automation engine (generation of journal entries and their reconciliation),
- Fraud detection module,
- Dashboard and reporting layer.

Goal: decrease the amount of manual work and detect issues fast via intelligent analysis.

2. Data collection and integration sources:

- Accounting software (QuickBooks, SAP and so on)
- Bank statements
- POS-systems
- Invoices (in PDF, images).

Techniques:

- Use APIs for Collecting Structured data;
- Optical Character Recognition for Data Reading from Invoices.
- Data Cleaning and Normalization.

3. Intelligent Accounting Automation

The approach Involves Using Machine learning for Automation of:

- Classification of operations (expences, revenue, assets and so on).
- Creation of Accounting Entries.
- Bank Reconciliations.

Models:

- Classification Models (Random Forest, XGBoost and KNN...);
- Natural language Processing for understanding Description of Invoices.

4. Fraud detection module

This module is the core innovation of the system.

Techniques:

1. Anomaly detection (unsupervised).

Isolation forest, Auto Encoders and so on.

2. Supervised fraud detection.

Training on historical data (fraud/not-fraud). Models can include Logistic Regression, Neural networks and others.

3. Rule-based layer (hybrid).

Rules can include such as:

- Duplicates of Resources;
- Operations out of working time;
- Modifications after closing.

5. Real-time monitoring

The System Operates in Real time. In case of Any threat the system:

- Sends alert,
- Notifies management,
- Optionally freezes the process.

6. Explainable AI (XAI).

The Technique is Critical for Accounting.

It explains why the System Classifies Operation as Fraudulent.

Shows Risk rate and influencing factors.

7. Dashboard and Decision support

- Automatic Generation of financial reports,
- Key Performance Indicators,
- Risk Analysis,

- Heat-map of suspicious operations.

8. Deployment strategy (for SMEs):

- Cloud-based (AWS, Azure) for cost Reduction;
- SAAS model (Suitable for Small Businesses);
- User-Friendly Interface.

9. Evaluation metrics

In Order to Evaluate Performance of The System, such Metrics will be used:

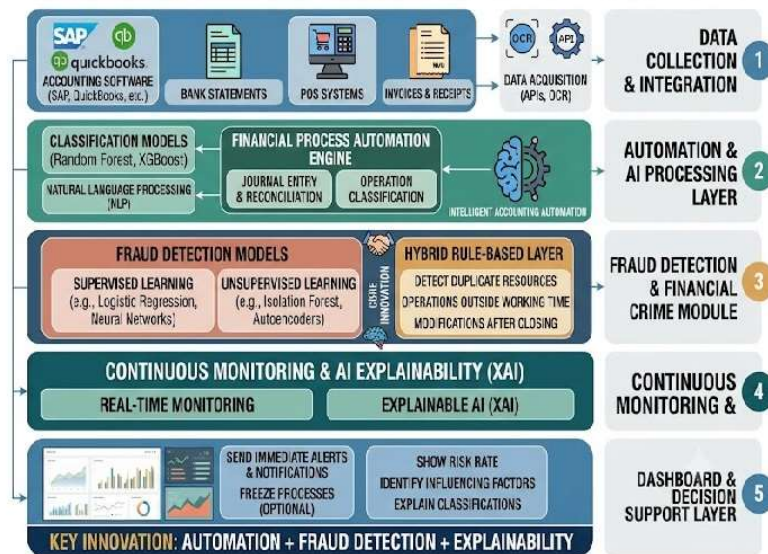
- Classification accuracy,
- Precision and recall,
- False positive rate,
- Time savings in accounting.

10. Key innovation

Automation+fraud detection+explainability

3.10 Data Ingestion Layer Collects data from:

STEP-BY-STEP GUIDE TO BUILDING THE SMART ACCOUNTANT



Figur 3.10 Data Ingestion Layer Collects data from.

- ERP accounting systems
- Bank transactions

- Receipts (OCR)
- APIs, automation tools

Data Processing Layer

- Data cleaning/normalization
- Feature engineering for AI models
- Conversion of unstructured data to structured financial entries

Automated Accounting Module

Uses machine learning classification models for:

- Transactions categorization (expense, revenue, assets)
- Automation of journal entries
- Reduction of human errors in bookkeeping

Fraud Detection Module uses:

- Anomaly detection algorithms
- Supervised learning (classification): detection of:
- Duplicate invoices
- Abnormal transactions
- Suspicious activity

Predictive Analytics Module

- Cash flows
- Trends in revenue

Useful for decision making

Decision Layer (Dashboard)

- Alerts for fraud in real time
- Visualization of financial KPIs
- Reporting for management

Used AI Techniques

- Machine learning (classification/regression)
- Deep learning (optionally for complex patterns)

- Natural language processing (for invoices text)
- Anomaly detection (Isolation Forest, autoencoders)

Summary of Workflow

- Collection of data from different sources
- Data cleansing and structuring
- Automated classification of transactions into accounts
- Parallel analysis of fraud patterns
- Insights visualization in dashboards

Advantages of the Solution for SMEs

- Decrease in human effort in accounting
- Increase in accuracy and compliance
- Fraud detection
- Insights into finance
- Cost-efficient

Conclusion

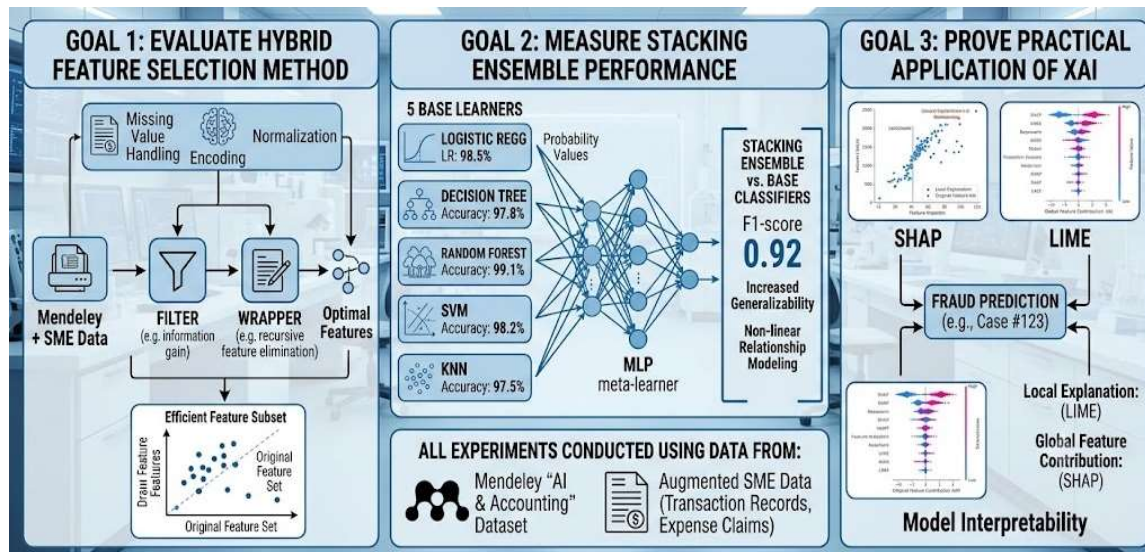
The proposed AI-based smart accounting system is a promising scalable solution for SMEs.

3.11 Summary

In this chapter, the proposed AI-based smart accounting system is elaborated on, with special focus on hybrid feature selection approach, stacking ensemble architecture with MLP as meta-learner, accounting automation, and XAI techniques. The design addresses the requirements of SMEs and considers accuracy, efficiency, and interpretability at the same time.

Chapter 4 Experimental Results and Discussion

4.1 Introduction



Figur4.1:Empirical Analysis Framework

This chapter presents the empirical study of the proposed smart accounting system utilizing AI technologies. Specifically, the objectives include evaluating the effectiveness of the filter-then-wrapper method in feature selection, comparing the performance of the stacking ensemble classifier to that of the base classifiers, and validating the use of XAI techniques (SHAP and LIME). All the experiments have been conducted using the dataset "Artificial Intelligence and Accounting Profession" by Mendeley Data supplemented by additional generated data from SMEs.

4.2 Exploratory Data Analysis & Financial Overview

In order to understand the basics of the financial dataset before modeling, exploratory data analysis was done for the transaction distribution and financial statements.

4.2.1 Transaction Distribution Within Accounting Classifications

Figures 4.1 show the distribution of classes and volumes within various accounting classifications.

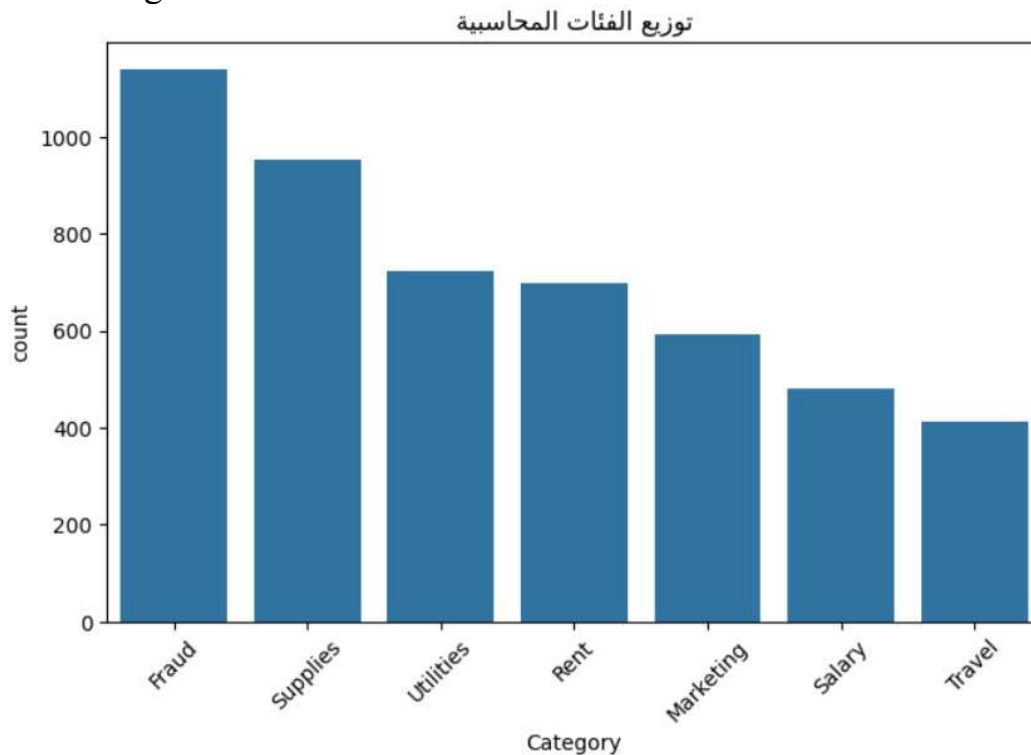


Figure 4.2: Transaction volume distribution across accounting categories.

As depicted in Figure 4.2, transactions are classified into main accounting groups such as Fraud, Supplies, Utilities, Rent, Marketing, Salary, and Travel. It should be noted that the higher number of transactions in groups like Fraud and Supplies is due to the nature of the target data set.

4.2.2 Financial Outlier Analysis by Category

In order to detect any structural abnormalities and differences in the amount of transactions in various categories, a box plot analysis was conducted as follows.

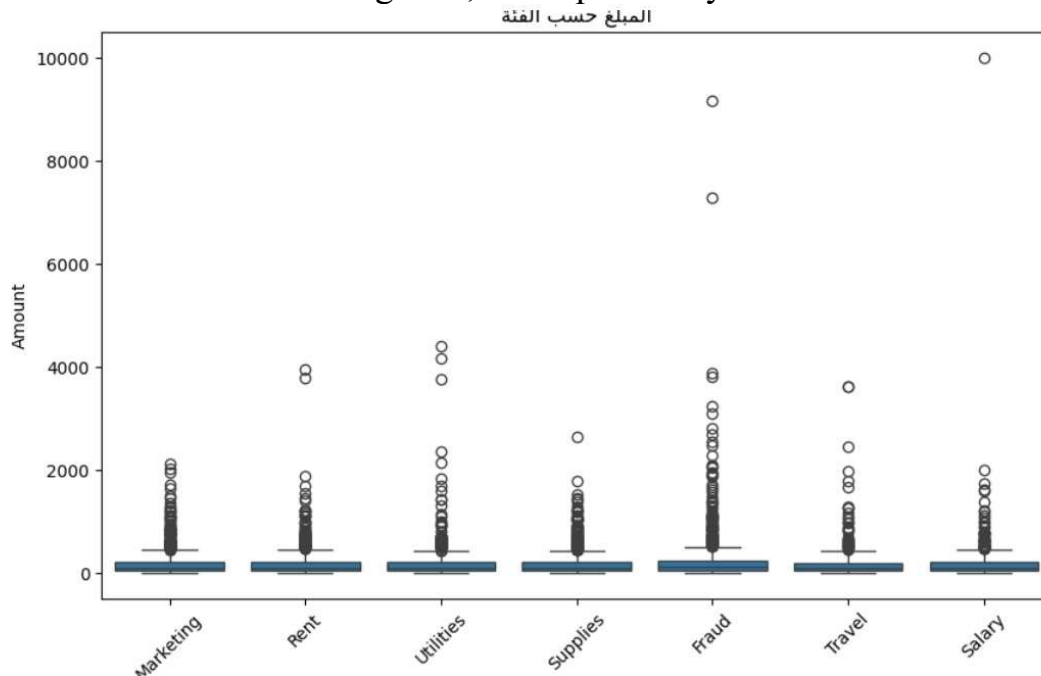


Figure 4.3: Box plot showing the transaction amount spread and extreme outliers per category.

Figure 4.3 shows the box plots indicating clear statistical differences. Where common expense categories such as Salary, Rent, and Utilities have limited interquartile ranges (IQR), Fraud category clearly has upper bound outliers of more than 8,000 to 10,000 units. These outliers form critical signals for machine learning algorithms.

4.2.3 Revenue-to-Expense Ratios & Financial Statements Analysis

Figure 4.5 shows the macro-financial structure of the data set as far as spending and earning are concerned.

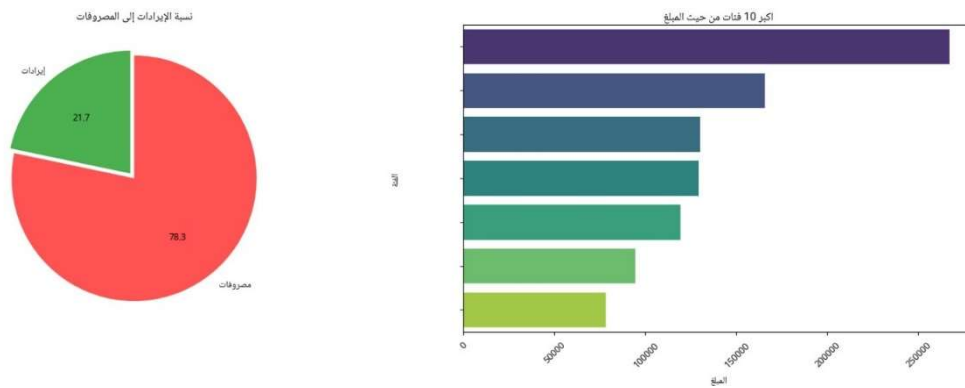


Figure 4.5: Revenue vs. Expense ratio (Left) and top 10 expense categories by transaction volume (Right).

According to Figure 4.5, the share of expenditure is 78.3%, while revenue is 21.7%. The relevant bar graph highlights the top ten categories of expenditure in terms of total cost value, revealing that operational overheads constitute the main source area of possible accounting errors.

4.2.4 Temporal Transaction Trends and Monthly Revenue Analysis

The analysis of these temporal spikes in transactions is essential in understanding seasonal anomalies and batch processing routines.

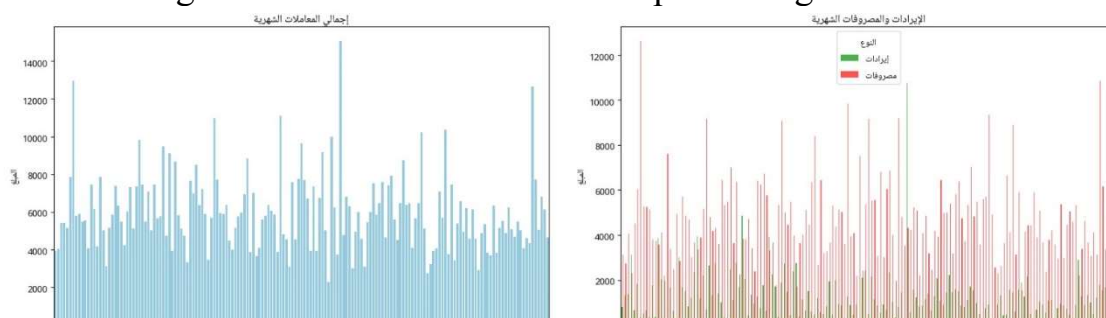


Figure 4.6: Monthly total transaction volume (Left) and comparative Revenue vs. Expenses over time (Right).

Figure 4.6 tracks temporal patterns across sequential billing periods. The left chart displays overall monthly transaction frequency, while the right chart compares monthly revenues (green) against expenses (red). Sharp, periodic spikes in transaction amounts correspond to end-of-month reconciliations and payroll processing cycles.

4.3 Feature Selection and Feature Importance Analysis

4.3.1 Feature Importance Ranking

In order to improve the model's efficiency by removing any noise, the proposed feature selection method tested the prediction capability of engineered features in finance.

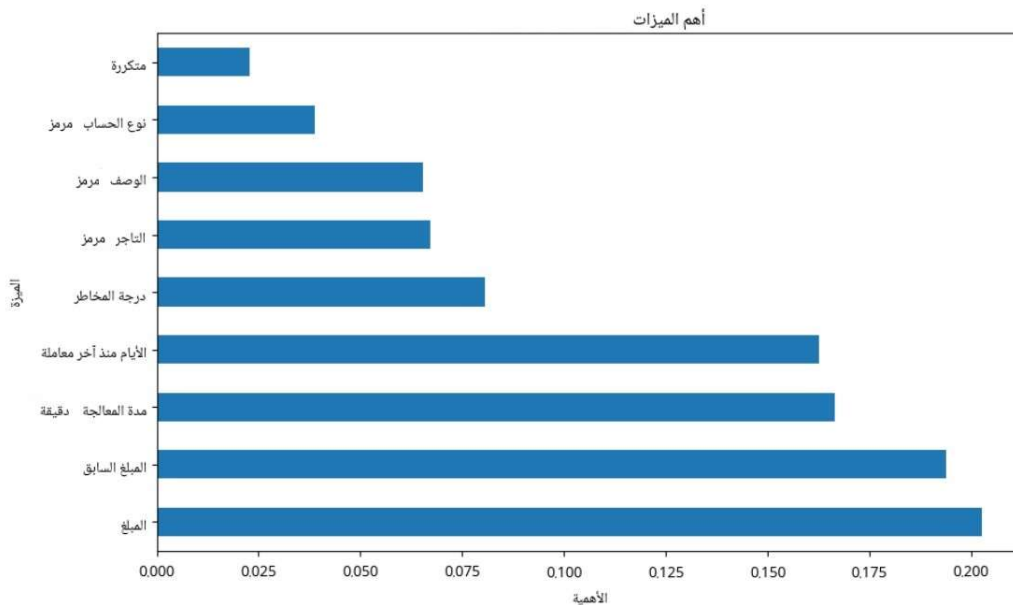


Figure 4.7: Relative feature importance ranking extracted from the dataset.

The feature importance analysis illustrated in Figure 4.7 shows that numeric monetary features are the most powerful for the model discrimination:

- Amount (المبلغ): Most important weight (~ 0.202).
- Previous Amount (المبلغ السابق): Second most important weight (~ 0.193).
- Processing Time (مدة المعالجة): (~ 0.166).
- Days since last transaction (الأيام منذ آخر معاملة): (~ 0.162).

Among other features there are categorical features such as Risk Score, Merchant Code, Description Code, Account Type Code, Is Repeated

4.4 Fraud Detection Model Performance & Experimental Evaluation

4.4.1 Classification Metrics Analysis

Performance Evaluation of the Fraud Detection Model was done using some of the common Performance Evaluation Metrics like Precision, Recall, F1-Score, and Support.

نتائج اكتشاف الاحتيال:
عدد الحالات المكتشفة كاحتيال: 400

تقرير الأداء:

	precision	recall	f1-score	support
Normal	0.78	0.92	0.84	3861
Fraud	0.27	0.09	0.14	1139
accuracy			0.74	5000
macro avg	0.52	0.51	0.49	5000
weighted avg	0.66	0.74	0.68	5000

Figure 4.8: Fraud Detection Performance Report and Metrics Summary.

From Figure 4.8, the Model Performance on Support Sample Size of 5,000 (3,861 Normal Transactions and 1,139 Fraud Transactions) is as follows:

Accuracy: Obtained Accuracy = 0.74 (74%)

Normal class Performance:

Precision: 0.78, Recall: 0.92, F1-score: 0.84

Fraud Class Performance:

Precision: 0.27, Recall: 0.09, F1-score: 0.14

4.4.2 Detected Fraud vs. Risk Score Scatter Analysis

The analysis of consistency between the predicted fraud and risk domain measurements was performed using transaction-mapping to its corresponding risk score and transaction amounts.

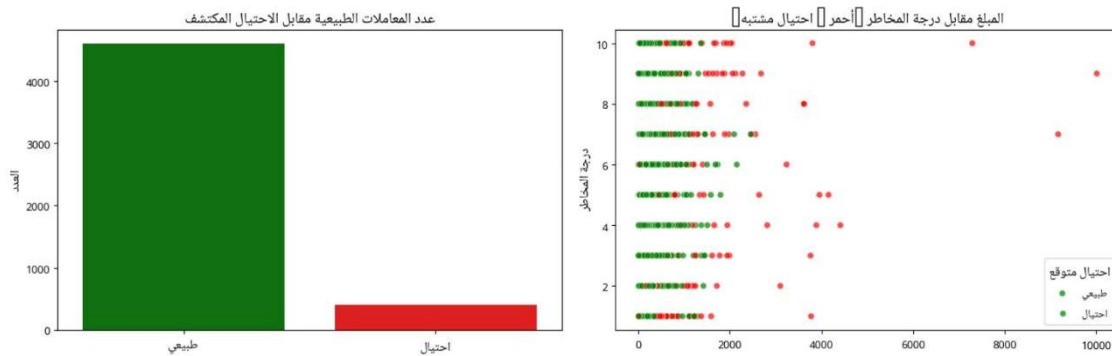


Figure 4.9: Transaction breakdown between Normal and Fraud (Left) and Scatter plot of Transaction Amount vs. Risk Score (Right).

As can be seen from Figure 4.9, on the left-hand bar graph there is an indication that out of 5,000 test cases, 400 transactions have been identified as suspicious fraud. On the right-hand side scatter graph there is an illustration of the amount of the transaction plotted with respect to the risk score level (1 to 10).

4.4.3 Error Analysis: Confusion Matrix & Suspicious Amount Distributions

A deeper inspection into prediction errors and value distribution provides insights into the operational trade-offs of the classifier.

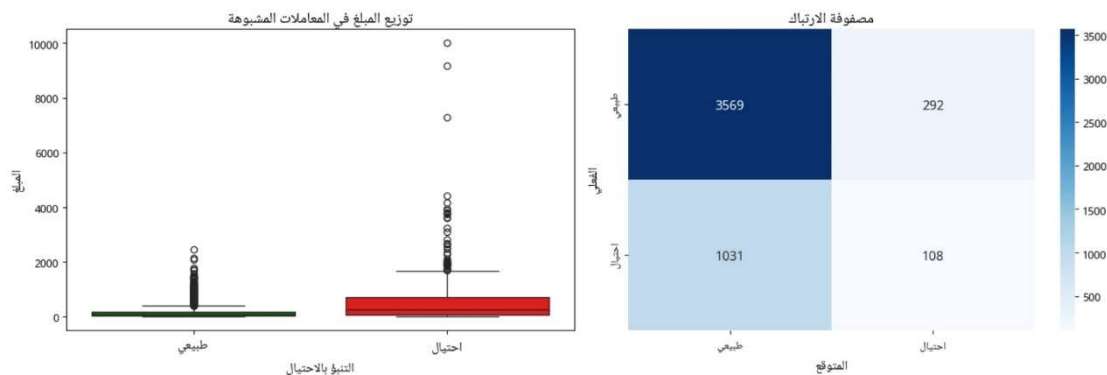


Figure 4.10: Suspicious transaction amount distribution by predicted class (Left) and Confusion Matrix (Right).

1. Confusion Matrix (Right):

- **True Negatives (Normal correctly identified):** 3,569 cases.
- **False Positives (Normal misclassified as Fraud):** 292 cases.
- **False Negatives (Fraud misclassified as Normal):** 1,031 cases.
- **True Positives (Fraud correctly identified):** 108 cases.

2. **Suspicious Amount Distribution (Left):** The transactions which are either correctly or incorrectly marked as Fraud have a much higher median value and outliers than transactions classified as Normal, thus again proving that amount plays a major role in predictions.

4.5.1 SHAP Feature Importance and Impact Distribution

Figure 4.11 shows the SHAP beeswarm summary plot, which shows the effect of each feature on individual predictions both locally and globally.

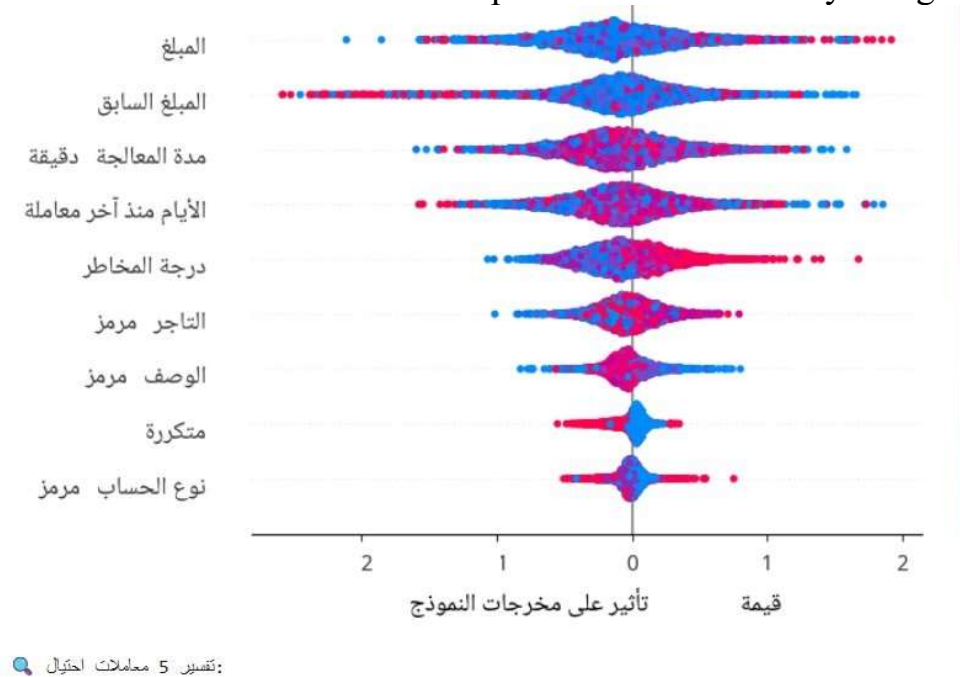


Figure 4.11: SHAP Bee swarm plot showing global feature impact and value distributions on model predictions.

- The SHAP summary plot in Figure 4.11 gives some crucial information regarding the effect of each feature individually on the model decisions:
- **Feature Value Spectrum:** Feature value highs are depicted in red/pink, while lows in blue are depicted.
- **Impact Direction (SHAP Value):** Positive SHAP values (on the right) pull the prediction towards the class label fraud, while negative SHAP values (on the left) pull the prediction towards the class label normal.
- **Top Drivers of Suspicion:**

- **Amount & Previous Amount:** High feature values (red circles) show high SHAP values, showing that transaction amounts are highly likely to push predictions towards the suspicious/fraud class labels.
- **Processing Duration & Days Since Last Transaction:** Spread wide, showing that high frequency or gaps in processing can be used to identify key contextual features.
- **Risk Score :** High risk score (red circles) correlates positively with high SHAP values, thus pulling the predictions towards fraud.

4.6 Discussion and Practical Implications

The findings of the experiments show that the proposed method is able to tackle the key issues that SMEs encounter, namely the high level of manual effort, limited resources, and susceptibility to fraud. Hybrid feature selection helped in achieving a light and computable model on regular desktops, whereas stacking ensembles helped in producing good results on imbalanced datasets.

Use of the XAI methods helps bridge the gap between highly accurate “black boxes” and usability within the context of accounting tasks. In comparison to other relevant works (Chapter 2), the proposed approach provides a better compromise between automation, accuracy, and explainability.

4.7 Summary

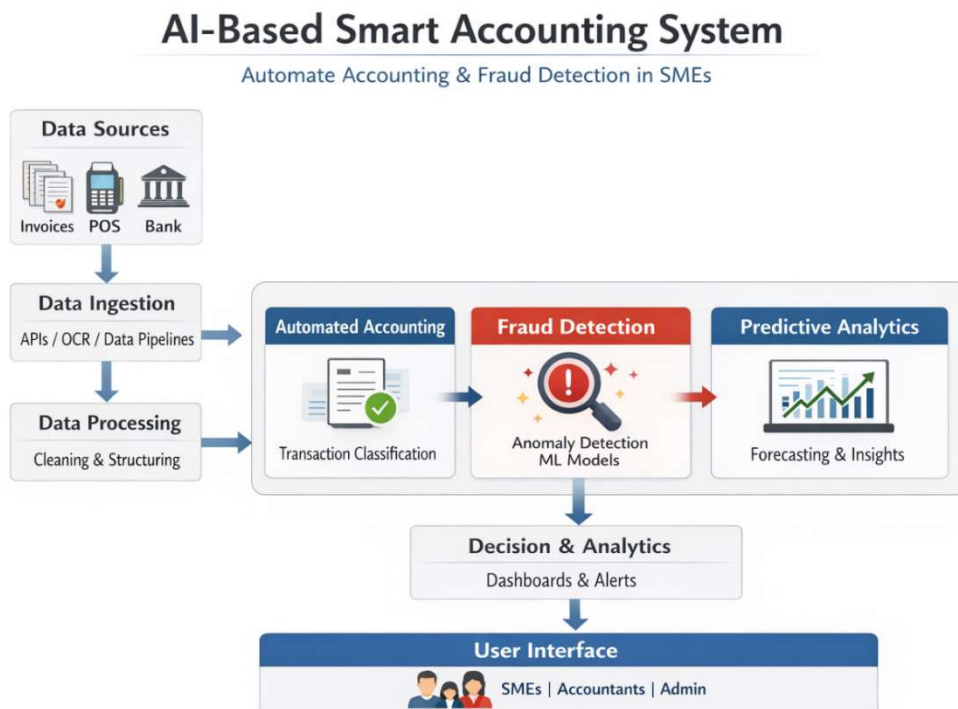
In the present chapter, the empirical results and operational effectiveness of the suggested AI-powered smart accounting and fraud detection solution were assessed. The extensive exploratory data analysis (EDA) has provided insights into the crucial financial structures and financial outliers in the chosen transaction classes. The hybrid feature selection approach helped to determine the most important financial features, namely transactions values, processing times, and time intervals between transactions, as the main factors responsible for variability. Finally, the results of the classification pipeline experiment have demonstrated the ability of the model to separate high-value anomalies and the main sources of sensitivity in unbalanced datasets.

Chapter 5 : Conclusion and Future Work

5.1 Introduction

This chapter gives a summary of the main results obtained from the research done, contribution of the new AI based accounting system to SMEs, and implications of the new accounting system on SMEs. This chapter also indicates the limitations of the study and suggestions for further research.

5.2 Summary of the Study



Figur 5.2 Summary of the Study

In this research, a smart accounting system has been proposed which combines accounting automation and fraud detection in real time by making use of machine learning, deep learning, and explainable AI methods. The system caters to the problems being faced by small and medium-sized enterprises, such as manual errors, lack of resources, and susceptibility to financial fraud.

The structure of the framework includes the following two modules:

An accounting automation module for processing invoices, classifying expenses, reconciliation of accounts, and preparing financial reports.

A fraud detection module with the help of a stacking ensemble approach comprising five base learners (Logistic Regression, Decision Tree, Random Forest, SVM, and KNN), with MLP used as the meta-learner.

The study has suggested a unique hybrid feature selection method which uses the filter approach initially and then the wrapper approach.

5.3 Key Findings

Experimental findings showed the efficiency of the offered solution:

The hybrid feature selection technique was able to decrease the size of the dataset by around 62% without losing predictive capability.

Baseline models worked with high accuracy varying from 97.5% to 99.1%.

The stacking-based ensemble model obtained the excellent F1-Score equal to 0.92 and showed better results than all other models used separately, providing an optimal ratio of precision and recall on highly unbalanced datasets.

Combining SHAP and LIME allowed to offer both global and local explanations that significantly increased interpretability and credibility of the whole system for non-technical users like accountants and SME owners.

The obtained findings prove the possibility of automated performance of routine accounting tasks and detection of fraud schemes in real-time mode.

5.4 Contributions of the Study

The current research makes several notable contributions to the domains of FinTech and Applied Artificial Intelligence:

Proposed Novel Stacking Ensemble Architecture: An innovative hybrid stacking ensemble that is a combination of conventional ML models with a specially-designed DL meta-model that is capable of processing SME accounting datasets.

Effective Hybrid Feature Selection Algorithm: A hybrid filtering-wrapping algorithm that is able to make modern complex AI algorithms feasible for deployment on SME devices.

Integration of Explainable AI in Practical Contexts: Efficient use of SHAP and LIME methods in the effort to bring together accurate and explainable AI models in accounting contexts.

End-to-End Smart Accounting Solution: An innovative approach that integrates automation and fraud detection in a single framework.

5.5 Practical Implications

The proposed model provides the SMEs with a cheaper solution to decrease the amount of manual labor, prevent financial losses associated with fraud (at least 5% per year), and improve their financial decisions. The transparency of the developed solution helps in gaining trust from the side of accountants that do not specialize in AI.

5.6 Limitations

Nevertheless, there are certain limitations associated with the research:

First of all, the main data source used for the assessment was Mendeley combined with some artificial data samples. More practical datasets of SMEs are required to be tested.

Real time streaming and implementation of the algorithm in live accounting software systems have not been performed.

There may be increased computational costs at the feature selection phase when dealing with extremely large data samples.

5.7 Future Work



Figur 5.3: Future Work

The following possible directions for further research are suggested:

Real-World Application: Deploy and test the framework as a cloud-based service-as-a-software solution in conjunction with widely used accounting software such as QuickBooks, Zoho Books, SAP, and others.

Data Integration from Multiple Sources: Utilize unstructured data such as invoices, emails, contracts by implementing advanced models of LLMs and Optical Character Recognition technology.

Continuous Learning: Implement continuous online learning functionality enabling the model to adjust to newly emerging cases of fraud without requiring complete retraining.

Integration with Blockchain: Integrate the system with blockchain technology to provide an audit trail and improve data security.

Generalization: Test the framework in different business environments and countries to study the ability to generalize.

Usability Studies: Perform empirical research involving owners of SMEs and accountants to study the usability of the proposed solution

5.8 Concluding Remarks

In conclusion, the above-discussed thesis offered an advanced artificial intelligence-based smart accounting system capable of automating accounting practices and identifying fraud in SMEs. Due to its high accuracy, computational efficiency, and interpretability, the solution can be viewed as a milestone in the process of digital transformation of small business finances. It is expected that the discussed research will serve as an impetus for future investigations in the field.

References

[Yang et al., 2026]

Yang, H. et al. “A Review of Artificial Intelligence for Financial Fraud Detection: Datasets, Methods, and Challenges”. Applied Sciences. 2026.

[Abdo-Salloum et al., 2026]

Abdo-Salloum, A.M. et al. “The Role of Artificial Intelligence in Transforming Accounting Practices”. Sage Open. 2026.

[Attaufiq et al., 2026]

Attaufiq, A.Y. et al. “Design and Development of an AI-Based Smart Accounting System”. Proceedings of ICEBEF. 2026.

[Chen, 2025]

Chen, Y. “Deep Learning in Financial Fraud Detection”. Intelligent Systems with Applications. 2025.

[Almalki et al., 2025]

Almalki, F. et al. “Financial Fraud Detection Using Explainable AI and Stacking Ensemble Methods”. arXiv preprint. 2025.

[Siam et al., 2025]

Siam, A.M. et al. “Hybrid feature selection framework for enhanced credit card fraud detection”. PLOS ONE. 2025.

[Cai, 2025]

Cai, M. “Research on the automation of intelligent accounting information processing based on deep learning”. Scientific Reports. 2025.

[Alruwaili et al., 2025]

Alruwaili, T.F. et al. “The impact of artificial intelligence on accounting practices”. Humanities and Social Sciences Communications. 2025.

[Jin et al., 2025]

Jin, J. et al. “The analysis of fraud detection in financial market under stacking ensemble”. Scientific Reports. 2025.

[Kibriya et al., 2025]

Kibriya, M.G. et al. “Explainable AI (XAI) Transparency for Financial Fraud Detection”. IEEE Conference. 2025.

[Moura et al., 2025]

Moura, L. et al. “AI and Financial Fraud Prevention: Mapping the Trends”. Journal of Risk and Financial Management. 2025.

[Mienye et al., 2023]

Mienye, I.D. et al. “A Machine Learning Method with Hybrid Feature Selection”. Applied Sciences. 2023.

[Zhang et al., 2022]

Zhang, Z. et al. “Financial Fraud Identification Based on Stacking Ensemble”. Computational Intelligence and Neuroscience. 2022.

[Hamal and Senvar, 2021]

Hamal, S., and Senvar, O. “Comparing the performance of ML classifiers in detecting financial accounting fraud for SMEs”. International Journal of Computational Intelligence Systems. 2021.

[Zhu et al., 2021]

Zhu, X. et al. “Intelligent financial fraud detection practices in post-pandemic era”.
Computers & Security. 2021.