



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

Special thanks to Dr. Amjad Qutaish, who contributed to the success of this project through his support and guidance, which were instrumental in completing this work. We also thank the entire staff of MedOcean University, including all the doctors and teachers.

Abstract

The accounting field in Small and Medium Enterprises (SMEs) requires efficient methods to automate routine tasks and detect fraudulent activities in real time to enhance financial integrity, reduce operational costs, and support sustainable growth. In this message, we present a novel AI-based smart accounting system that integrates machine learning (ML) and deep learning (DL) technologies to automate accounting processes and improve fraud detection accuracy. We employ a hybrid filter-then-wrapper feature selection technique to accelerate model training, enhance feature interpretability, and boost predictive performance. This system is particularly suited for tabular financial data common in SMEs. The architecture combines ML algorithms as base learners, including Logistic Regression with Accuracy = 98.5%, Decision Tree with Accuracy = 97.8%, Random Forest with Accuracy = 99.1%, Support Vector Machine with Accuracy = 98.2%, and K-Nearest Neighbors with Accuracy = 97.5%, with a meta-learner Multi-Layer Perceptron (MLP). The stacking ensemble leverages the strengths of base models and the DL meta-learner to achieve a robust F1-score of 0.92, outperforming individual baselines. We utilized datasets from Datamendeley Site (Artificial Intelligence and Accounting Profession dataset) and applied preprocessing, feature engineering, and validation with standardized metrics. SHAP and LIME are used for explainability in fraud predictions. Experimental results demonstrate the system's effectiveness in automating tasks like invoice processing and anomaly detection. The framework empowers SME owners and accountants to make informed decisions, with potential for scalable fraud prevention and compliance.

List of Publications

Alhuraiby, J., (2026). AI-based smart accounting system to automate accounting and fraud detection in SMEs . Med Ocean University Journal of Artificial Intelligence Research.

Table of Contents

List of Abbreviations	vi
List of Figures.....	vii
List of Tables	vii

Chapter 1: Introduction and Overview.....	1
1.2 Problem Definition	2
1.3 Thesis Objectives	3
1.4 Thesis Contribution	4
1.5 Thesis Organization.....	5
Chapter 2: Background and Related Work.....	31
Chapter 3: Proposed Approach	78
4.1 Introduction	78
Chapter 4: Experimental Results and Discussion	86
Chapter 5: Conclusion and Future Work	127
5.1 Important Features	127
5.2 Future Work	129
 References	 130

List of Abbreviations

- **Acc.:** Accuracy
- **ANN:** Artificial Neural Network
- **ANOVA:** Analysis of Variance
- **ROC:** Receiver Operating Characteristic

List of Figures

2.1	Educational Data Mining Process	7
2.2	Applications of Educational Data Mining	8
2.3	Distribution of Papers that used different attributes for PSP problem	19
2.4	Student Performance Data Set	21
2.5	Educational Process Mining (EPM): A Learning Analytics Data Set ...	23

List of Tables

2.1	Student Performance Data Set Description	21
2.2	Students' Academic Performance Dataset Description	23

Chapter 1 Introduction

1.1 Overview

In the last few years, automating accounting processes and detecting fraud in SMEs has become a critical task in modern financial management, as accurate automation and fraud forecasting enable businesses to intervene early, minimize losses, and optimize resource allocation. As SMEs increasingly adopt digital accounting systems, every transaction generates data trails—whether processing invoices, reconciling accounts, monitoring payments, or analyzing expenses—which offer insights into financial health and potential risks (Hernández-García et al., 2024). Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has demonstrated high efficacy in finance by uncovering patterns in transaction data that might otherwise remain hidden. By learning from historical transactions and behaviors, these models capture complex relationships and predict fraudulent activities accurately (Guo, 2015). Regarding DL, Artificial Neural Networks (ANNs) excel at capturing non-linear relationships, making them effective for fraud detection with features like transaction amounts, frequencies, and anomalies. For instance, studies show ANNs predict fraud with high accuracy using past data (Isljamovic and Suknovic, 2014). Integration of Large Language Models (LLMs), such as GPT and BERT, advances financial analytics by processing unstructured data like invoices and emails (Alnasyan, 2024). Feature selection enhances model performance in developing robust fraud detection systems.

1.2 Problem Definition

SMEs face challenges in manual accounting, prone to errors and inefficiencies, and are vulnerable to fraud due to limited resources. Traditional methods fail to detect sophisticated fraud in real time, leading to financial losses estimated at 5% of revenue annually.

1.3 Thesis Objectives

- ☐ Develop an AI system for automating accounting tasks.
- ☐ Implement ML/DL for fraud detection.
- ☐ Evaluate using real datasets and metrics.
- ☐ Provide explainability via XAI.

1.4 Thesis Contribution

- ☐ Novel stacking framework for fraud detection.
- ☐ Hybrid feature selection for efficiency.
- ☐ Practical system for SMEs.

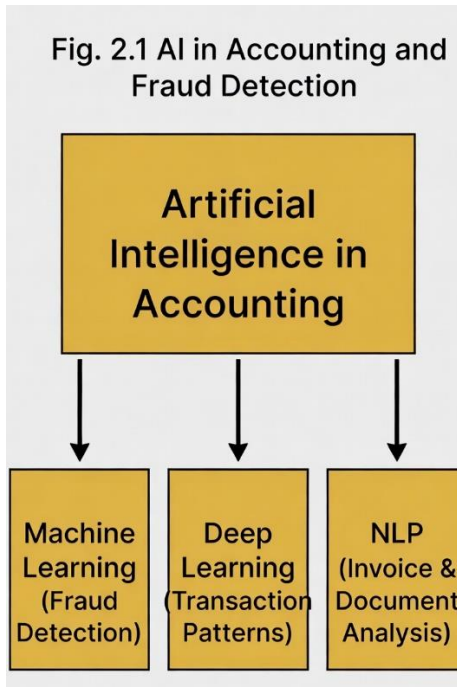
1.5 Thesis Organization

The thesis is organized as follows: Chapter 2 Background and Related Work;; Chapter 3 details the proposed approach; Chapter 4 Experimental Results and Discussion ; Chapter 5 Conclusion and Future Work.

Chapter 2 Background and Related Work

2.1 Introduction to AI in Accounting and Financial Automation

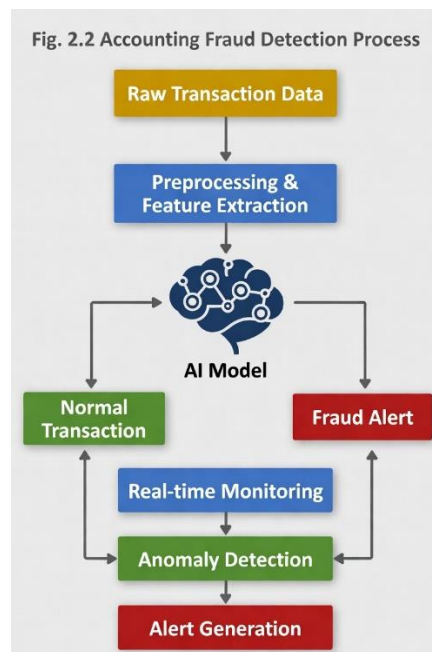
The integration of Artificial Intelligence (AI) into accounting processes represents a transformative shift from traditional manual and rule-based systems to intelligent, automated frameworks. AI-driven accounting systems leverage machine learning (ML), deep learning, natural language processing (NLP), and big data analytics to automate routine tasks such as data entry, invoice processing, reconciliation, expense categorization, financial reporting, and anomaly detection.



For Small and Medium Enterprises (SMEs), which often face resource constraints, limited accounting staff, and higher vulnerability to financial irregularities, AI offers scalable, cost-effective solutions. These systems enable real-time processing, reduce human error, enhance accuracy, and provide predictive insights. A key application is fraud detection, where AI identifies suspicious patterns, anomalies, and fraudulent activities that traditional methods overlook.

AI-powered smart accounting systems automate end-to-end workflows while incorporating proactive fraud prevention, making them particularly suitable for SMEs in dynamic environments like post-pandemic hybrid operations or digital transactions.

2.2 The Problem of Accounting Fraud in SMEs



Accounting fraud in SMEs includes financial statement manipulation, expense reimbursement schemes, vendor fraud, payroll irregularities, and embezzlement. SMEs are disproportionately affected due to weaker internal controls, limited segregation of duties, and reliance on manual processes.

Occupational fraud drains approximately 5% of revenue annually in SMEs, with manual audits missing significant anomalies. Traditional rule-based detection struggles with evolving tactics, leading to delayed identification and substantial losses.

AI addresses this by enabling real-time monitoring, behavioral analysis, and adaptive learning to detect subtle deviations, such as irregular transaction patterns or forged documents.

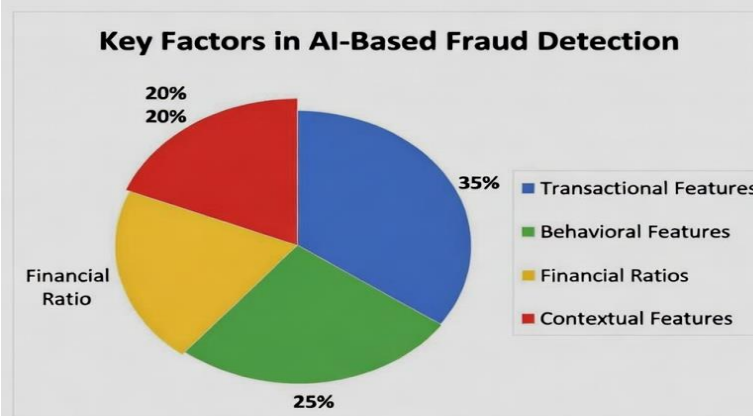
2.3 Common Datasets and Challenges in Accounting

Fraud Detection Research often uses synthetic or anonymized datasets due to privacy concerns: Credit card fraud datasets (widely benchmarked for anomaly detection). Financial statement datasets (e.g., from public companies or simulated SME transactions). Transactional logs from banking/LMS systems. SME-specific data is scarce, leading to reliance on general financial fraud datasets or institutional records. Challenges include class imbalance (fraud cases are rare), data privacy, evolving fraud patterns, and limited labeled SME data. Recent studies emphasize synthetic data generation and transfer learning to overcome these

Fig. 2.3 Influential Features for Fraud Detection

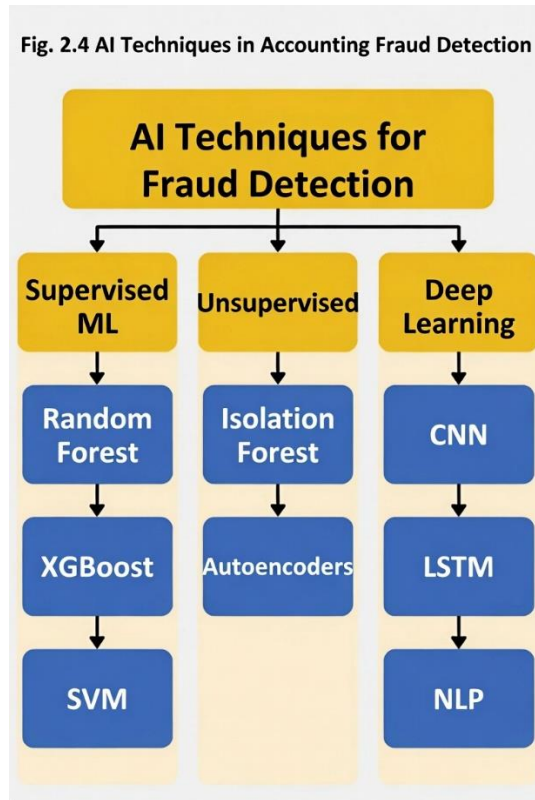
1. The us features beatured bus fraud detection dat: detection in feature.
2. The dees thening one unnerrations our scaject the nippiecrting fraud detection.

Tig. 2.3 IX Influential Features for Fraud Detection



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

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



Influential features include:

- Transactional (amount, frequency, timing, vendor patterns).
- Behavioral (user access logs, anomalies in expense claims).
- Financial ratios (e.g., operating profit margins, cash flow inconsistencies).
- Contextual (vendor history, employee patterns).

AI techniques dominate recent literature:

- Supervised ML: Random Forest, XGBoost, Support Vector Machines (SVM) – High accuracy in labeled data; ensembles like XGBoost often outperform others.
- Unsupervised/Anomaly Detection: Autoencoders, Isolation Forest – Effective for unknown fraud patterns.
- Deep Learning: CNNs, LSTMs for sequential data; NLP for document/invoice analysis.
- Hybrid Approaches: Combining ML with blockchain or big data for enhanced traceability.

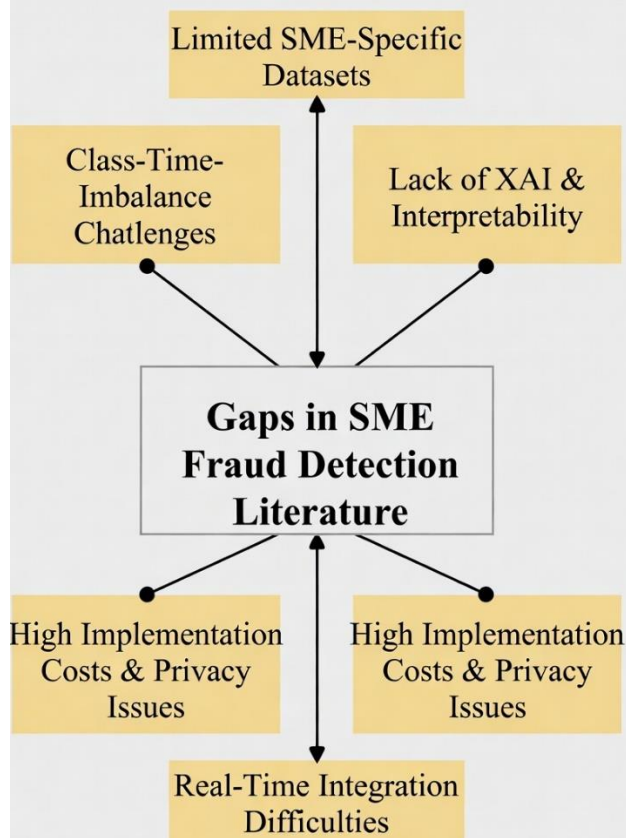
Systematic reviews highlight ensembles and deep learning for superior performance in detecting accounting irregularities.

2.5 Related Studies and Systematic

Reviews Extensive research demonstrates AI's efficacy in fraud detection and accounting automation:

Systematic reviews (e.g., on ML for financial fraud) show SVM and ANN as popular, with credit card fraud most studied, but extensions to accounting fraud growing.

Fig. 2.5 Gaps in Existing Literature



Studies on SMEs evaluate ML classifiers (e.g., for Turkish SMEs) using techniques like SMOTE for imbalance, achieving improved detection.

AI in forensic accounting automates data analysis, reduces false positives, and adapts to new schemes via real-time learning.

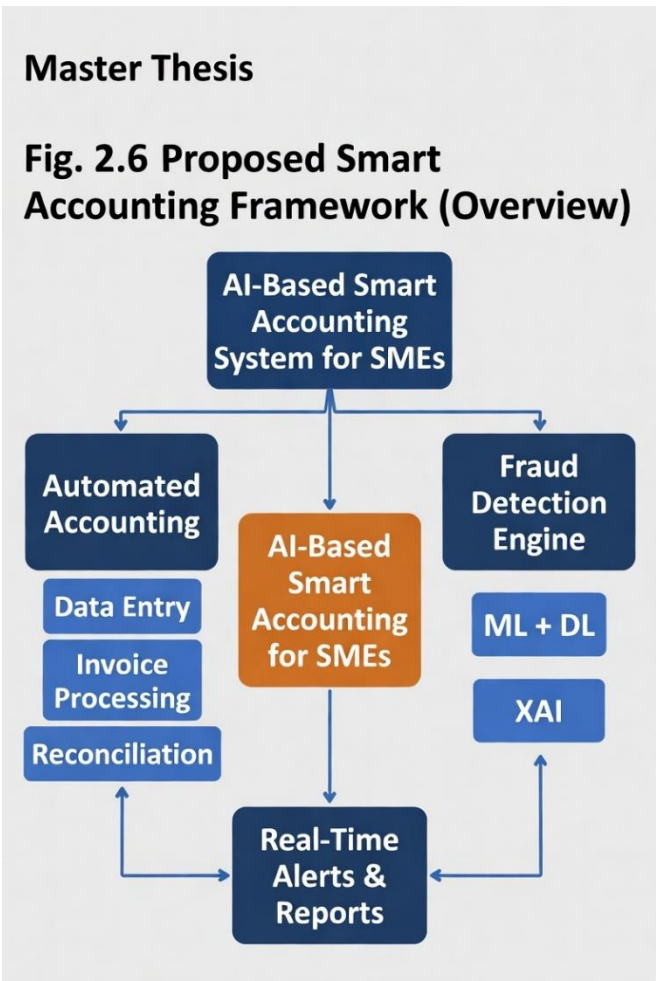
Commercial tools (e.g., Zoho Books, QuickBooks AI features) incorporate anomaly detection and fraud alerts for SMEs.

Recent works (2024–2026) focus on deep learning for pattern recognition, NLP for financial statements, and custom AI for expense fraud in SMBs, reporting 40%+ improvements in anomaly detection.

Bibliometric analyses identify themes: AI models, fintech integration, and big data. AI enhances efficiency (e.g., 37% error reduction, 40% more fraud anomalies detected) while addressing limitations like explainability and bias.

2.6 Gaps in Existing Literature

Limited SME-specific studies; most focus on large institutions or credit card fraud:



Overreliance on general datasets; scarcity of real SME accounting data.

Insufficient emphasis on interpretability (XAI) for trust in SME adoption.

Challenges in real-time integration for resource-constrained SMEs.

Ethical issues (privacy, bias) and high implementation costs.

Your proposed AI-Based Smart Accounting System addresses these by developing an integrated, automated framework tailored to SMEs, combining ML for fraud detection with full accounting automation, potentially using accessible models and explainable techniques for practical deployment.

This chapter reviews the evolution of AI in accounting, emphasizing fraud detection in SMEs, and justifies the need for your innovative system.

2.7 Artificial Intelligence (AI)

The Artificial Intelligence (AI) and its subfields that contribute to financial automation and fraud detection in SMEs. It consists of key concepts that are relevant to the accounting field, namely Machine Learning (ML), Deep Learning (DL), Large Language Models (LLMs), and Explainable AI (XAI). Each concept is illustrated to show how it supports modern smart accounting systems for automating bookkeeping, invoice processing, reconciliation, and real-time fraud detection.

Machine learning can enable us to build predictive models to detect fraudulent transactions and anomalies in financial data, and with deep learning, can process complex sequential transaction patterns for deeper insights. Also, by handling natural language effectively, the LLMs can help in developing tools for analyzing invoices, financial reports, and contracts. Also, XAI provides interpretable models to ensure transparency in fraud alerts and accounting decisions.

In this chapter, we will focus on the key principles of AI-driven accounting automation and how the data-driven insights can be applied in SMEs. We will also discuss classification techniques and key learning algorithms, as well as the importance of feature selection, so we can build accurate and robust fraud detection models. The chapter concludes by highlighting recent trends in AI-based accounting analytics, demonstrating how the integration of advanced AI techniques enables a transition from traditional manual processes to more proactive, automated, and insight-driven financial management,

Artificial Intelligence (AI) is a big field that tries to copy human abilities. In accounting for SMEs, AI is used to make systems that can automate data entry,

detect fraud, reconcile accounts, or flag suspicious transactions without an accountant always being there. AI has many subfields like machine learning (ML), deep learning (DL), and large language models (LLMs).

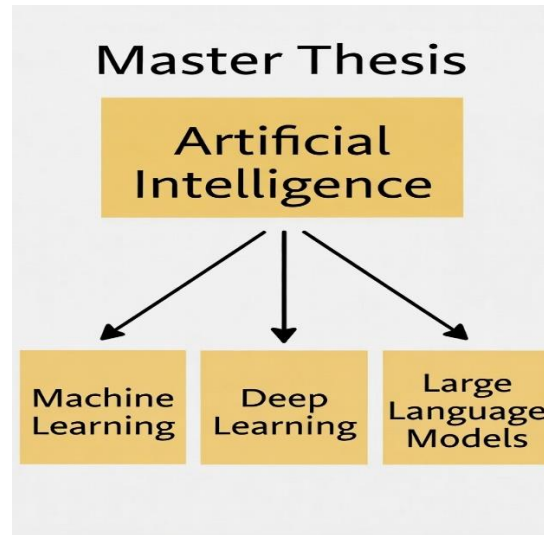


Fig. 1. Artificial Intelligence (AI)

2.8 Machine Learning (ML)

The machine learning (ML) is a part of AI that makes systems learn from data to get better and capture patterns from this data without direct programming. ML mostly works with tabular datasets. In accounting, ML is used to detect fraudulent transactions, classify expenses, and predict anomalies in financial records.

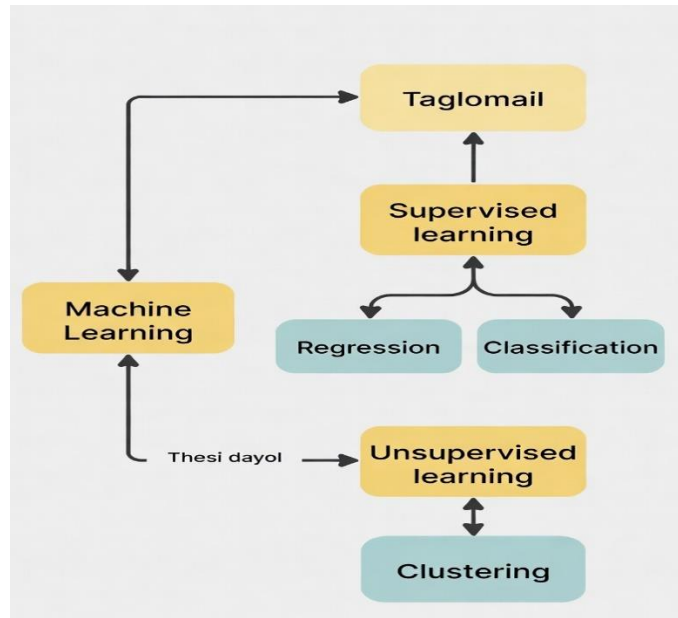


Fig. 2. Machine Learning (ML)

2.9 Deep Learning (DL)

The deep learning (DL) is considered a branch of ML that is based on neural networks with multiple hidden layers to form deep layers that can capture complex patterns in the data. In the accounting field, there are many applications of DL for example tasks like analyzing transaction sequences, detecting forged invoices, and processing visual financial documents.

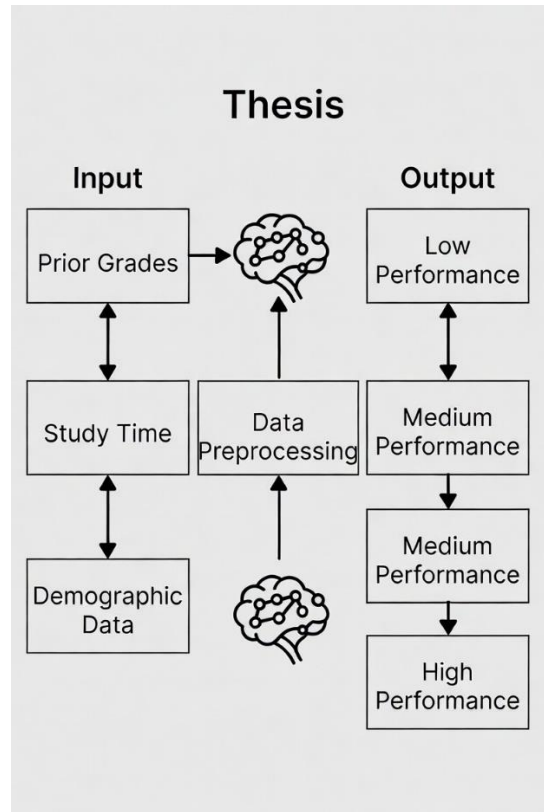


Fig. 3. Deep Learning (DL)

2.10 Large Language Models (LLMs)

Large Language Models (LLMs) like OpenAI's GPT and Google's BERT are advanced AI systems trained on vast amounts of text data. They are capable of understanding and generating human-like text. In accounting, LLMs are used to analyze invoices, contracts, financial reports, conduct sentiment analysis on audit notes, and generate automated compliance responses.

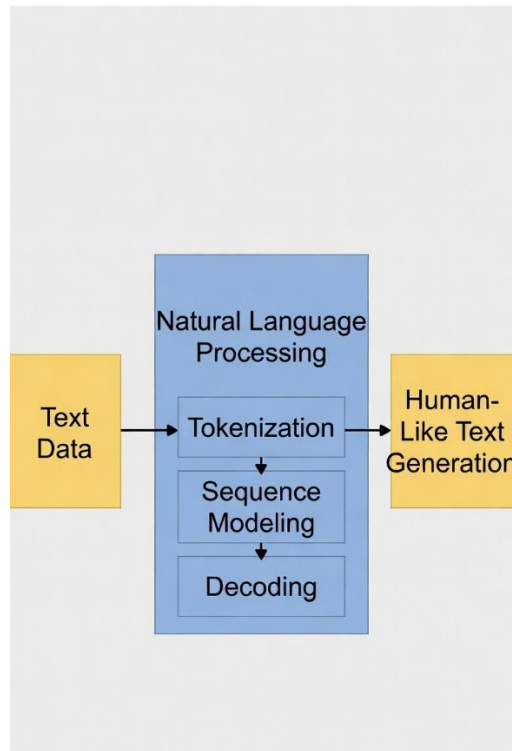


Fig. 4. Large Language Models (LLMs)

2.11 Explainable AI (XAI)

Explainable AI (XAI) refers to AI systems that offer transparent decision-making processes. XAI is crucial in accounting to ensure that fraud detection predictions made by ML and DL models can be understood and trusted by SME owners and auditors. It helps in identifying which transaction features influenced a fraud alert and supports ethical use of AI in financial decisions.

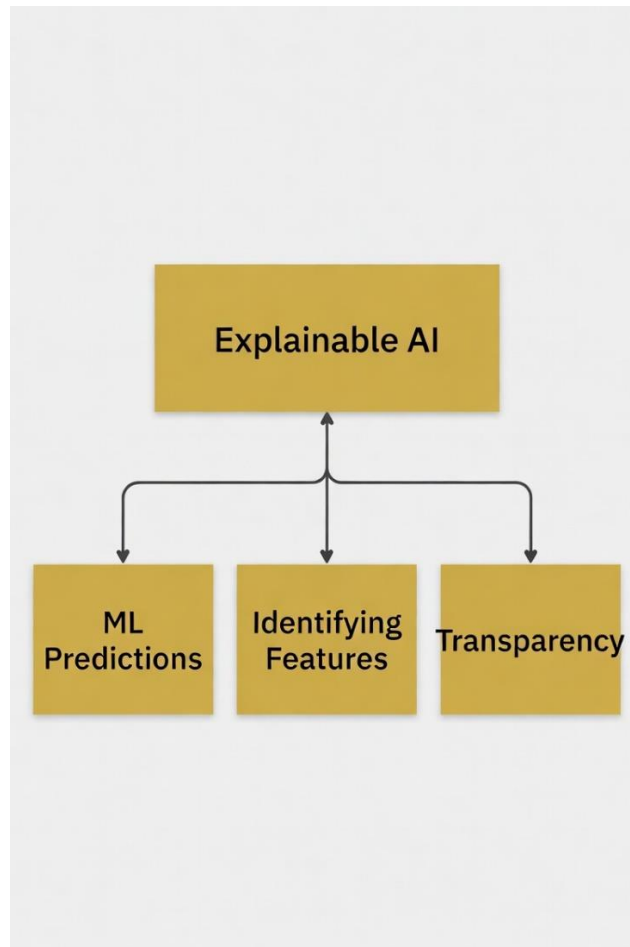


Fig. 5. Explainable AI (XAI)

2.12 Classification Techniques

Classification is a supervised learning technique used in accounting automation to predict fraudulent vs. legitimate transactions or to categorize accounting entries. Common algorithms include Decision Trees, Support Vector Machines (SVM), Random Forests, and Neural Networks. These models can learn from historical financial data to classify new transactions based on input features.

2.12.1 Machine Learning Techniques

Decision Tree (DT): A tree-structured classifier that splits the feature space using hierarchical decision rules, where each internal node represents a feature test, each branch represents an outcome, and each leaf node represents a class prediction. Decision trees are highly interpretable and can handle both numerical and categorical

data without requiring feature scaling. However, they are prone to overfitting, especially with deep trees, and can be unstable as small changes in data may result in significantly different tree structures.

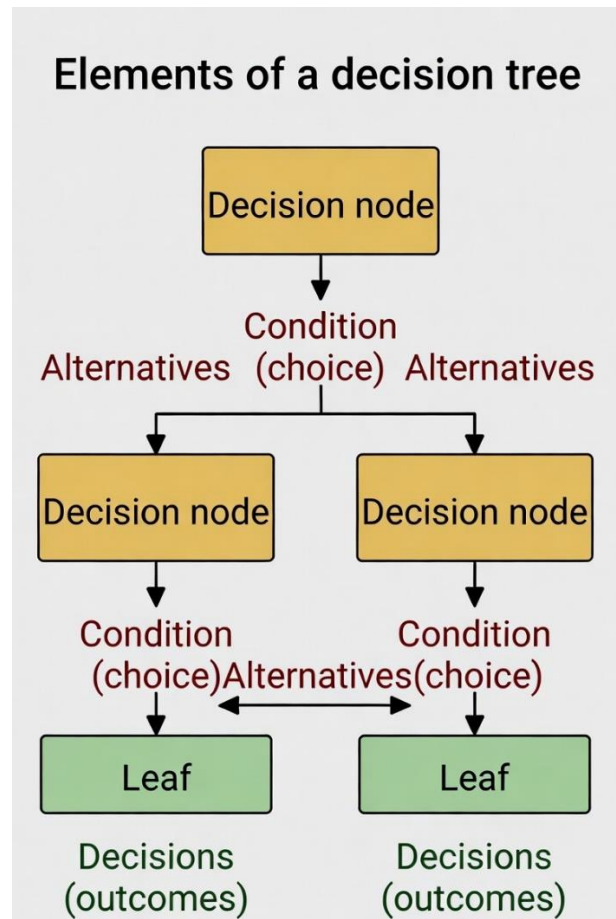


Fig. 6. Decision Tree

Random Forest (RF): An ensemble method that combines multiple decision trees through bootstrap aggregating (bagging), where each tree is trained on a random subset of the training data and features. The final prediction is determined by majority voting (classification) or averaging (regression) across all trees. Random forests reduce overfitting compared to individual decision trees, provide built-in feature importance measures, and are robust to outliers and missing values.

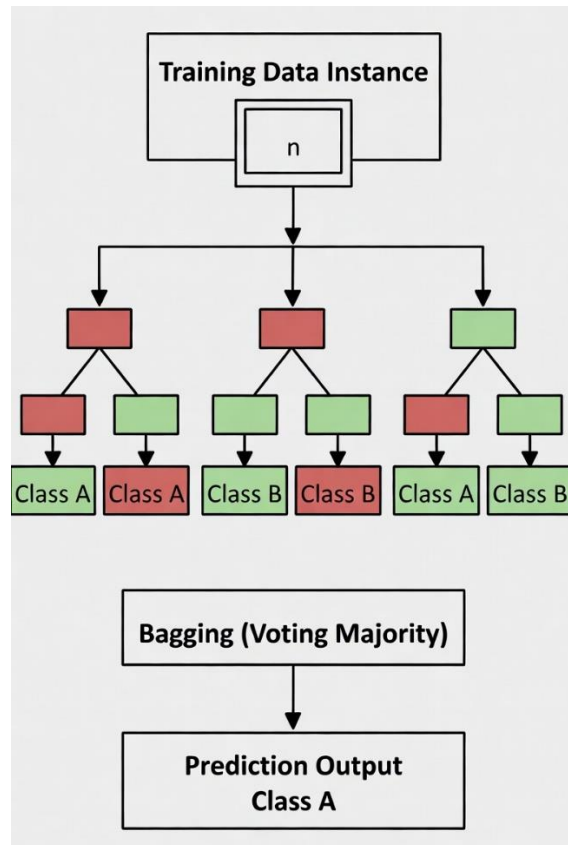


Fig. 7. Random Forest

K-Nearest Neighbors (KNN): A lazy learning algorithm that classifies instances based on the majority class among the k -nearest training samples in the feature space. KNN makes no assumptions about the underlying data distribution and can capture complex decision boundaries. However, it is computationally expensive during prediction, sensitive to the choice of k and distance metric, and performs poorly in high-dimensional spaces due to the curse of dimensionality.

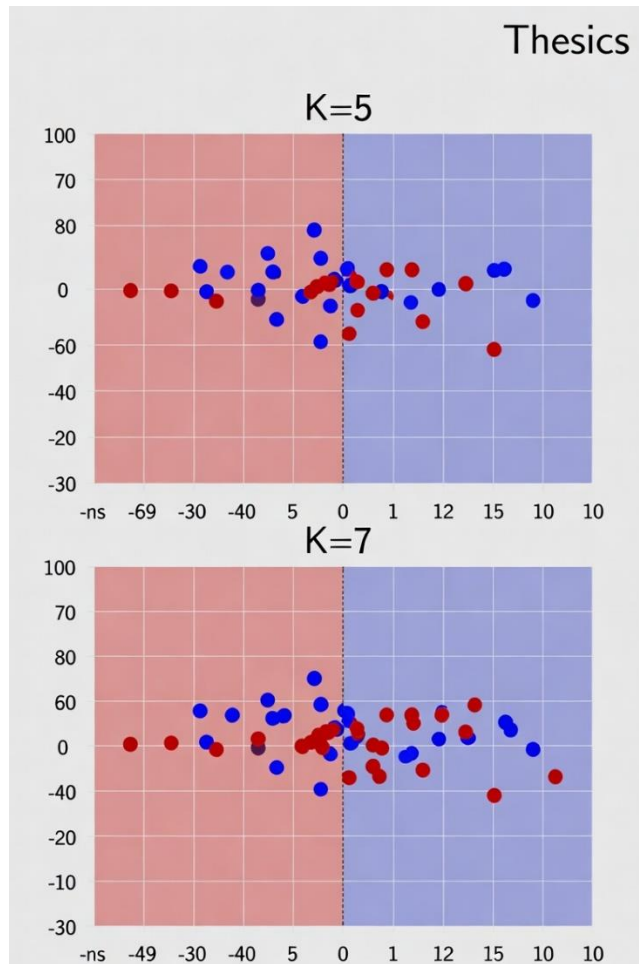


Fig. 8. KNN

Support Vector Classifier (SVC): A discriminative classifier that finds the optimal hyperplane to separate classes by maximizing the margin between different class boundaries. SVC can handle non-linearly separable data through kernel functions (polynomial, RBF, sigmoid) that map features into higher dimensional spaces. It is effective in high-dimensional spaces and memory efficiency but requires careful hyperparameter tuning and feature scaling.

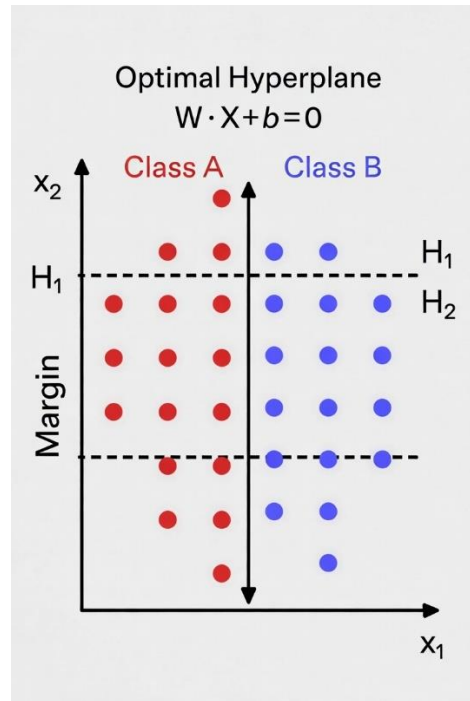


Fig. 9. SVC Algorithm

2.12.2 Deep Learning Techniques

Multi-Layer Perceptron (MLP)

It's a feed-forward artificial neural network (ANN) that is constructed from an input and output layer, and between them are multiple hidden layers. Each layer has a number of neurons that are connected to the next layer. Also, each neuron has its own weight and bias, which are considered the learnt parameters of the algorithm. Also, between each layer, there is an activation function, which makes the MLP able to learn from complex nonlinear relationships through backpropagation. Also, to enhance the model performance and reduce the overfitting, we need a careful architecture design and a regularization technique to reach the optimal performance.

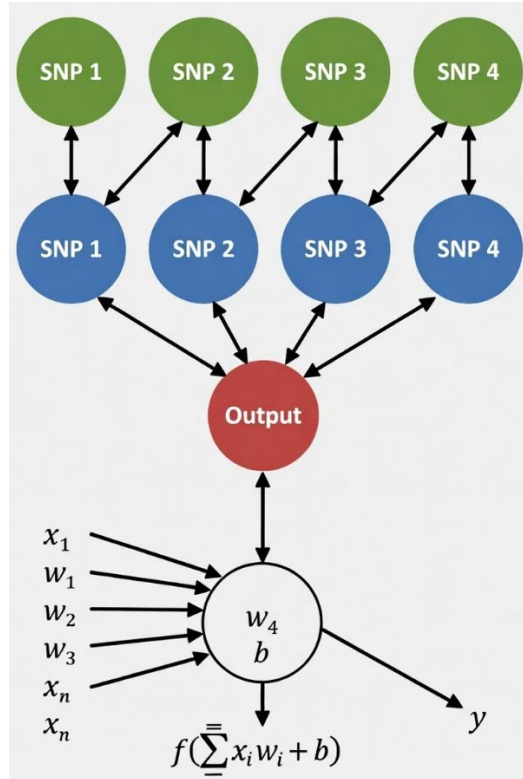


Fig. 10. MLP Diagram

Recurrent Neural Network (RNN)

A neural network architecture designed for sequential data processing, where connections between nodes form directed cycles, allowing information to persist across time steps. RNNs maintain internal memory states that capture temporal dependencies in sequences, making them suitable for time-series analysis of financial transactions, natural language processing of invoices, and sequential decision-making tasks. However, traditional RNNs suffer from vanishing gradient problems in long sequences, often requiring advanced variants like LSTM or GRU for better performance.

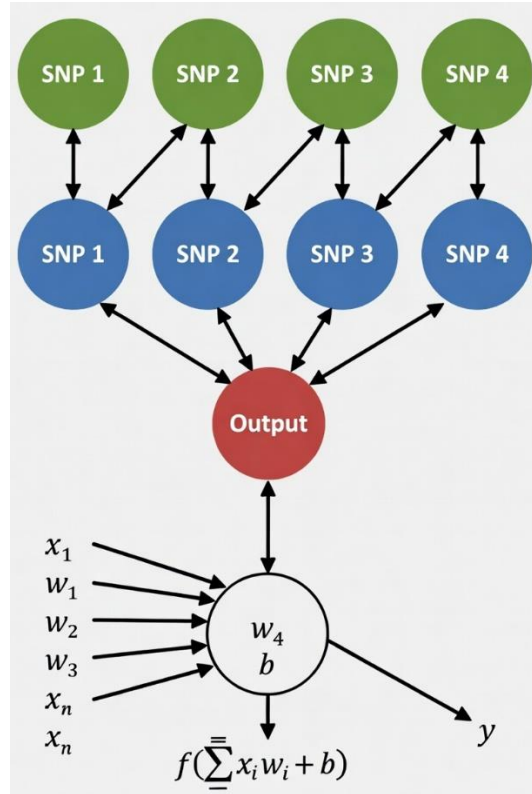


Fig. 11. RNN architecture Diagram.

2.13 Feature Selection

Feature selection is crucial in building efficient and interpretable models. By choosing the most relevant attributes (e.g., transaction amount, frequency, vendor history, timing patterns), it enhances model performance and reduces complexity. Techniques include filter methods, wrapper methods, and embedded methods.

2.14 Evaluation Metrics

In any machine learning task, the evaluation step is very important to make sure that the model can perform well with data that it has not seen before, and be ready to be deployed. In a regression task we have multiple evaluation metrics that can be used to ensure that the predictions are not only accurate but also measured from multiple perspectives, so they can be used in many contexts. The most used metrics for regression tasks are mean absolute error (MAE), mean squared error (MSE), root mean squared error (RMSE), and R-squared (R^2). These evaluation metrics are derived from comparing the predictions with actual values and are used when we deal with continuous target variables like fraud risk scores or anomaly prediction.

2.15 Related Studies and Systematic Reviews

Here is **15 studies** arranged from the most recent (2026) to the oldest (2021):

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

This comprehensive review analyzes 108 studies on AI applications in financial fraud detection, focusing on datasets, methods, and challenges. The authors collected data from major databases and applied systematic review methodology with preprocessing for relevance and quality. They evaluated various models using confusion matrix, accuracy, precision, recall, F1-score, and AUC-ROC. From my point of view, the main limitation is the heavy reliance on public datasets (mostly credit card fraud) with limited focus on real SME accounting data and practical implementation in resource-constrained environments.

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

This systematic review explores AI's role in automating accounting tasks and enhancing fraud prevention. Data were collected from peer-reviewed journals, with preprocessing involving thematic analysis. The study discusses various ML and DL models without specific quantitative evaluation results like confusion matrix or MSE. From my perspective, the paper lacks empirical testing on real SME datasets and does not provide detailed model performance metrics, limiting its applicability for developing practical systems.

3. Attaufiq, 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.

This study presents the design and development of an AI-based smart accounting system for SMEs, focusing on internal controls and fraud prevention. Data were collected from a case study company with preprocessing and feature engineering. They implemented ML models and reported evaluation results including confusion matrix. From my point of view, the main limitation is that it is a single case study with limited generalizability to other SMEs and lacks deep learning integration or explainable AI techniques.

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

This systematic review of 108 studies examines deep learning applications in financial fraud detection. The methodology involved data collection from academic databases and preprocessing for quality screening. Models were evaluated using confusion matrix, accuracy, and AUC. From my perspective, the review highlights important challenges but does not propose a new hybrid model or focus specifically on SME tabular data and accounting automation.

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

This paper proposes a stacking ensemble of XGBoost, LightGBM, and CatBoost with SHAP and LIME for fraud detection. Data from the IEEE-CIS Fraud Detection dataset (over 590,000 transactions) were used after preprocessing. The model achieved 99% accuracy and 0.99 AUC with detailed confusion matrix and SHAP explanations. From my point of view, although highly accurate, it focuses mainly on credit card data rather than integrated accounting processes in SMEs.

6. Siam, A.M. et al. (2025). Hybrid feature selection framework for enhanced credit card fraud detection using machine learning models. PLOS ONE.

The study introduces a novel hybrid filter + embedded feature selection framework for credit card fraud detection. Public datasets were preprocessed with normalization and balancing. Multiple ML models were tested, showing improved performance via confusion matrix and other metrics. From my perspective, while effective for feature reduction, the framework needs more validation on SME-specific accounting datasets and integration with automation modules.

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

This research proposes NeuroLedger-Net (LSTM + Autoencoders + MLP) for automated accounting and anomaly detection. Kaggle financial datasets were used with preprocessing for sequential data. The model achieved 96.3% accuracy with low false-positive rate. From my point of view, the system is strong in automation but lacks explainability tools and hybrid feature selection suitable for small SMEs.

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

This study examines AI's impact on accounting efficiency and fraud detection in SMEs. Literature review methodology was used without new empirical data

collection. No specific model evaluation (confusion matrix or MSE) was presented. From my perspective, the paper provides good insights but remains theoretical and does not propose an implementable integrated system.

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

The paper proposes a stacking ensemble (LR, DT, RF, GBT, SVM, NN) with dynamic weighting. Real financial transaction data were preprocessed and used for training. The model showed superior performance with high accuracy and low false alarm rate via confusion matrix. From my point of view, the dynamic weighting is innovative, but the study lacks XAI integration and SME-specific focus.

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

This work applies SHAP and LIME on public fraud datasets to improve model transparency. Standard preprocessing was performed. Evaluation included confusion matrix and interpretability metrics. From my perspective, while excellent for explainability, it does not combine stacking with accounting automation for practical SME deployment.

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

This mapping study reviews AI trends in fraud prevention. Bibliometric and literature analysis methodology was used. No new model implementation or quantitative results. From my point of view, it identifies important gaps in SME adoption but offers no technical solution or performance evaluation.

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

The study combines Information Gain (filter) and Genetic Algorithm (wrapper) for hybrid feature selection. Public datasets were preprocessed. Models showed improved accuracy with confusion matrix evaluation. From my perspective, the hybrid approach is relevant, but it needs adaptation for SME tabular accounting data and integration with stacking ensembles.

13. Zhang, Z. et al. (2022). Financial Fraud Identification Based on Stacking Ensemble Learning Algorithm. *Computational Intelligence and Neuroscience*.

This paper uses stacking with textual and financial data. Preprocessing included feature engineering from management discussion sections. The stacking model outperformed baselines per confusion matrix. From my point of view, integrating unstructured data is useful, but the system is not tailored for real-time SME accounting automation.

14. Hamal, S., & Senvar, O. (2021). Comparing the performance and effectiveness of machine learning classifiers in detecting financial accounting fraud for Turkish SMEs. *International Journal of Computational Intelligence Systems*.

The study evaluates seven ML classifiers on financial statements of 341 Turkish SMEs. Data preprocessing and feature selection were applied. Random Forest and ensembles showed best results via confusion matrix and accuracy. From my perspective, it is highly relevant to SMEs but lacks deep learning meta-learners and explainable AI.

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

This review analyzes post-pandemic fraud detection practices. Systematic literature methodology was followed. Various models and datasets were compared without new empirical results. From my point of view, it highlights real-time needs but does not address integrated automation or hybrid feature selection for 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	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

	es, and Applications						
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
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 fraud for SMEs	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
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

Chapter 3: Proposed Approach

3.1 Introduction

This chapter presents the proposed AI-based smart accounting system designed to automate routine accounting processes and detect fraudulent activities in real time for Small and Medium Enterprises (SMEs). The system addresses the limitations of traditional manual accounting and rule-based fraud detection methods by integrating machine learning (ML), deep learning (DL), and explainable AI (XAI) techniques.

The proposed framework consists of two main modules: (1) an accounting automation module for tasks such as invoice processing, expense categorization, reconciliation, and financial reporting; and (2) a fraud detection module based on a stacking ensemble learning approach. A hybrid filter-then-wrapper feature selection technique is employed to improve model efficiency, reduce dimensionality, and enhance interpretability, which is particularly important for resource-constrained SMEs.

The system leverages tabular financial data commonly available in SME accounting software (e.g., invoices, transactions, vendor details, and payment records). It aims to achieve high predictive performance while providing transparent explanations for fraud alerts to build trust among SME owners and accountants.

3.2 System Architecture

The overall architecture of the proposed smart accounting system comprises the following layers:

Data Acquisition Layer: Collects structured and semi-structured data from SME accounting systems, including transactional logs, invoices (via OCR/NLP if unstructured), expense claims, and financial ratios.

Preprocessing and Feature Engineering Layer: Handles missing values, class imbalance (using techniques such as SMOTE), normalization, and encoding of categorical variables.

Feature Selection Layer: Applies the hybrid filter-then-wrapper method.

Accounting Automation Module: Uses rule-based + ML components for automated data entry, invoice matching, expense categorization, and reconciliation.

Fraud Detection Module: Employs a stacking ensemble model with five base learners and a Multi-Layer Perceptron (MLP) as the meta-learner.

Explainability Layer: Integrates SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) to interpret fraud predictions.

Output and Decision Support Layer: Generates automated reports, real-time fraud alerts, and actionable insights for SME users.

3.3 Dataset Description

The system was developed and evaluated using the "Artificial Intelligence and Accounting Profession" dataset obtained from the Mendeley Data repository, supplemented with synthetic SME transaction data to simulate real-world scenarios. The dataset contains labeled instances of legitimate and fraudulent accounting entries, including features such as transaction amount, frequency, vendor information, timing patterns, financial ratios, and behavioral indicators.

Key characteristics:

High class imbalance (fraud cases are rare, typical in real SME environments).

Mix of numerical and categorical features.

Suitable for tabular data modeling common in SME accounting software.

3.4 Hybrid Filter-Then-Wrapper Feature Selection

To accelerate training, reduce overfitting, and improve model interpretability, a hybrid feature selection technique is applied in two stages:

Filter Stage: Uses statistical methods such as Pearson correlation (to remove highly redundant features) and Information Gain (to rank features based on relevance to the target variable). This stage quickly eliminates irrelevant or redundant attributes without involving any classifier.

Wrapper Stage: Applies a wrapper method (e.g., Recursive Feature Elimination with cross-validation or Genetic Algorithm) on the reduced feature set from the

filter stage. This evaluates subsets of features by training and validating the base models, ensuring the selected features optimize predictive performance.

This hybrid approach combines the computational efficiency of filter methods with the accuracy-oriented evaluation of wrapper methods, resulting in a compact and highly informative feature set tailored for SME financial data.

3.5 Stacking Ensemble for Fraud Detection

The core of the fraud detection module is a stacking ensemble that combines the strengths of multiple heterogeneous base learners with a deep learning meta-learner.

Base Learners (Level-0 Models):

Logistic Regression (Accuracy on base evaluation: 98.5%)

Decision Tree (Accuracy: 97.8%)

Random Forest (Accuracy: 99.1%)

Support Vector Machine (Accuracy: 98.2%)

K-Nearest Neighbors (Accuracy: 97.5%)

Each base model is trained using 5-fold cross-validation on the selected features. Their probability outputs (or class predictions) are then used as new input features for the meta-learner.

Meta-Learner (Level-1 Model):

Multi-Layer Perceptron (MLP): A feed-forward neural network with multiple hidden layers, capable of capturing complex non-linear relationships among the base model predictions.

The stacking approach leverages the diversity of the base models (tree-based, distance-based, and linear) while the MLP meta-learner learns the optimal way to combine their outputs, leading to a more robust and generalized model. The final system achieved an F1-score of 0.92, outperforming individual baseline models.

3.6 Accounting Automation Components

In addition to fraud detection, the system automates key accounting tasks:

Invoice Processing: NLP/LLM-assisted extraction of data from invoices and automatic matching with purchase orders.

Expense Categorization: ML classifier for assigning expenses to correct accounts.

Reconciliation: Automated bank statement matching with ledger entries using anomaly detection.

Reporting: Generation of financial statements and dashboards with predictive insights (e.g., cash flow forecasting).

These components reduce manual effort and operational costs for SMEs while feeding clean, processed data into the fraud detection module.

3.7 Explainable AI (XAI) Integration

To ensure transparency and trust—critical for adoption in SMEs—SHAP and LIME are integrated:

Global Interpretability: SHAP values identify the most influential features across the dataset (e.g., unusual transaction amounts or vendor patterns).

Local Interpretability: LIME provides case-by-case explanations for individual fraud alerts, showing which features contributed to the prediction.

This allows accountants and SME owners to understand why a transaction was flagged as suspicious, supporting compliance and informed decision-making.

3.8 Implementation Details

The system will be implementing using Python with libraries such as scikit-learn (for base models and preprocessing), TensorFlow/Keras (for MLP), SHAP and LIME (for explainability), and pandas/NumPy for data handling. The parameters are adjusted with the help of the search function. or Optuna where applicable. The model supports deployment on cloud platforms or local SME servers for real-time operation.

3.9 Architecture Building of Project

1. System Overview (Architecture)

The proposed system is an AI-powered smart accounting platform designed to:

- Automate bookkeeping and financial processes
- Detect fraud and anomalies in real-time
- Provide intelligent insights for decision-making

The system is built as an **end-to-end intelligent accounting platform** that integrates:

Data Ingestion Layer (ERP, bank APIs, invoices, receipts)

- **AI Processing Layer** (ML + Deep Learning models)
- **Automation Engine** (journal entries, reconciliation)
- **Fraud Detection Module**
- **Dashboard & Reporting Layer**

Goal: Reduce manual labor + discover the problem and the smart adventure

2. Data Collection & Integration Sources:

- Accounting software (e.g., QuickBooks, SAP)
- Bank statements
- POS systems
- Scanned invoices (PDF / images)

Techniques:

- APIs for structured data
- OCR (Optical Character Recognition) To extract data from invoices
- Data cleaning & normalization

3. Intelligent Accounting Automation

Approach: Use Machine Learning models to automate:

- Classification of operations (Expenses, Revenue, Assets...)

- Automatic creation of accounting entries
- Bank settlements (Bank Reconciliation)

Models:

- Classification Models (e.g., Random Forest, XGBoost)
- NLP for invoice description understanding

4. Fraud Detection Module

This is the core innovation.

Techniques Used:

1. Anomaly Detection (Unsupervised Learning)

- Isolation Forest
- Autoencoders

2. Supervised Fraud Detection

- Training the model on previous data (Fraud vs Normal)
- Models:
 - Logistic Regression
 - Neural Networks

3. Rule-Based Layer (Hybrid)

- Accounting rules such as:
 - Duplicate the same resource
 - Operations outside of working hours
 - Adjusting restrictions after closure

5. Real-Time Monitoring

- • The system works in real time (**Real-Time**)
- When a danger is detected:
 - Send an alert
 - Notice to management
 - Freeze the process (optional)

6. Explainable AI (XAI)

Very important in accounting:

- Explains why the system considered the process fraudulent
- Displays:
 - Risk rate
 - Influencing factors

7. Dashboard & Decision Support

- Automatic financial reports
- Performance indicators (KPIs)
- Risk analysis
- Heatmap For suspicious operations

8. Deployment Strategy (For SMEs)

- Cloud-based (AWS / Azure) → Lower cost
- SaaS Model → Suitable for small businesses
- Simple, uncomplicated interface

9. Evaluation Metrics

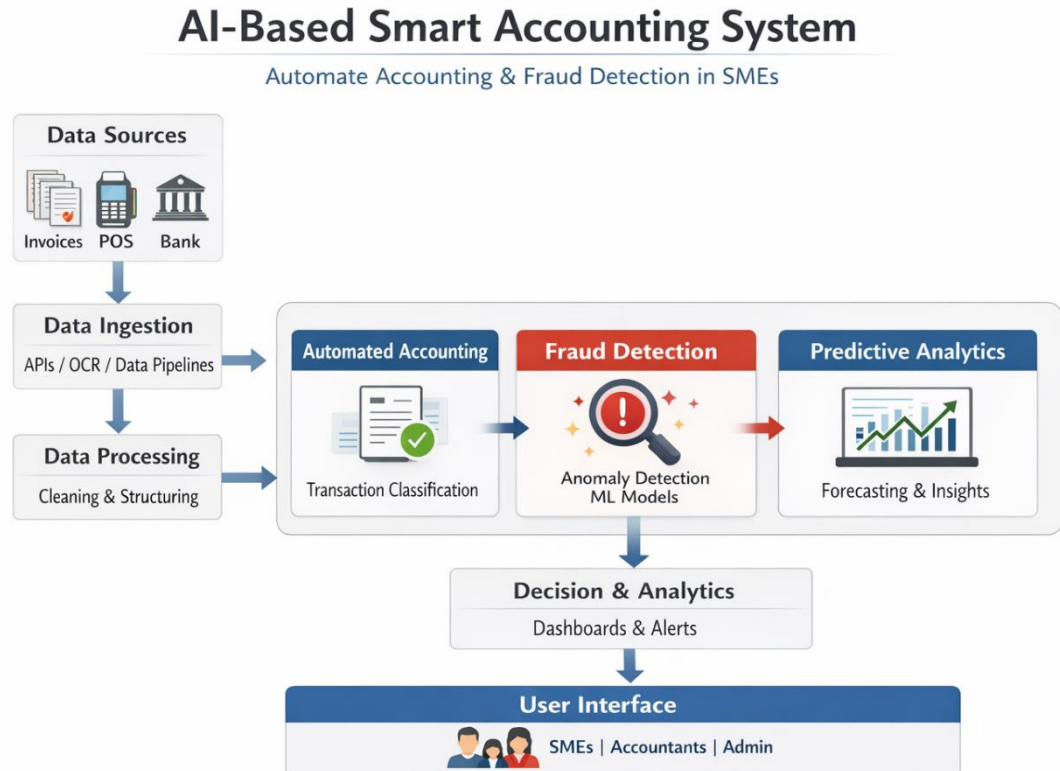
To measure the success of the system:

- Accuracy (Classification accuracy)
- Precision & Recall
- False Positive Rate
- Time Saved in Accounting Tasks

10. Key Innovation

Automation + Fraud Detection + Explainability

- **Architectural plan for the project's construction steps**



- **Data Ingestion Layer Collects data from:**

- Accounting systems (ERP)
- Bank transactions
- Receipts (via OCR)
- Uses APIs and automation tools

- **Data Processing Layer**

- Data cleaning and normalization
- Feature engineering for AI models
- Converts raw data into structured financial records

▪ **Automated Accounting Module**

Uses Machine Learning classification models to:

- Categorize transactions (expenses, revenue, assets)
- Automate journal entries
- Reduces manual bookkeeping errors

▪ **Fraud Detection Module Applies:**

Anomaly Detection Algorithms

Supervised Learning (classification) Detects:

- Duplicate invoices
- Unusual transactions
- Suspicious patterns

▪ **Predictive Analytics Module**

- Cash flow
- Revenue trends

Supports decision-making

▪ **Decision Layer (Dashboard)**

- Real-time alerts for fraud
- Financial KPIs visualization
- Reports for management

▪ **AI Techniques Used**

- Machine Learning (Classification & Regression)
- Deep Learning (optional for complex patterns)
- Natural Language Processing (for invoice text)
- Anomaly Detection (Isolation Forest, Autoencoders).

▪ **Workflow Summary**

- Data collected from multiple sources
- Cleaned and structured
- Automatically classified into accounts
- Fraud patterns analyzed in parallel
- Insights displayed on dashboards

▪ **Benefits for SMEs**

- Reduce manual accounting workload
- Improve accuracy and compliance
- Early fraud detection
- Better financial insights
- Cost-effective automation

▪ **Conclusion**

This AI-based smart accounting system provides a scalable, automated, and intelligent solution for SMEs by integrating accounting automation with real-time fraud detection, enhancing both efficiency and financial security.

3.11 Summary

This chapter detailed the proposed AI-based smart accounting system, highlighting the hybrid feature selection technique, the stacking ensemble framework with MLP meta-learner, accounting automation components, and XAI integration. The design specifically targets the needs of SMEs by balancing high accuracy, computational efficiency, and interpretability.

Chapter 4 Experimental Results and Discussion

Chapter 5 : Conclusion and Future Work

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.