DOI: 10.15849/ijasca.v18i1.44

Int. J. Advance Soft Compu. Appl, Vol. 18, No. 1, March 2026
Print ISSN: 2710-1274, Online ISSN: 2074-8523

Legal Investigation of Financial Fraud Using Artificial Intelligence

Belal Zaqaibeh

Department of Computer Science, Faculty of Science and Information Technology,
Jadara University, Irbid, Jordan
e-mail: zaqaibeh@jadara.edu.jo

Abstract

Financial fraud remains a serious global challenge, requiring innovative investigative techniques that seamlessly integrate Artificial Intelligence (AI) with legal systems. Conventional fraud investigation methods, which largely rely on AI-driven tools combined with manual legal analysis, often suffer from limited efficiency, scalability, and adaptability when addressing evolving financial fraud patterns. In this study, a hybrid AI-driven framework is proposed to effectively bridge financial fraud investigation and legal analysis. The proposed model integrates AI-based analytical systems with legal reasoning mechanisms to enhance the accuracy and reliability of fraud investigations. The framework has been validated using real-world financial fraud cases and legal investigation records. The results demonstrate that integrating AI-driven systems with fraud investigation processes significantly improves detection accuracy and accelerates investigation timelines. Moreover, the proposed approach enhances the efficiency of financial fraud case analysis by leveraging AI for legal interpretation and decision support. This study also addresses key challenges associated with the application of explainable artificial intelligence (XAI) in judicial contexts. By narrowing the gap between AI-based fraud detection and legal enforcement, the proposed framework contributes to making fraud investigations more transparent, accountable, and legally defensible. The findings confirm that the approach is effective in strengthening forensic financial investigations, reducing investigative effort, and ensuring compliance with continuously evolving financial regulations. Furthermore, sustainability is emphasized as a critical consideration in modern fraud investigation practices. The adoption of artificial intelligence within sustainable legal frameworks may support long-term regulatory compliance and responsible financial governance.

Keywords: *Financial Fraud Investigation, AI for Fraud Detection, Intelligent Legal Compliance, Financial Crimes, Financial Fraud Prevention*

1. Introduction

Financial fraud has come to light as one of the major concerns within the current globally integrated economy, impacting individuals, business organizations, as well as the government [1-3]. As already mentioned, the accelerated growth of digital technology has been beneficial to the world; however, it has given rise to effective mechanisms being

Received 4 November 2025; Accepted 2 January 2026

utilized by the fraudulent individuals to target the loopholes within the financial systems [1-3]. As reported within the "Global Economic Crime and Fraud Survey 2022" by [2], 51% of the reported instances showed the occurrence of fraud within the past two years among the organizations mentioned within the survey report, thereby highlighting the contingency related to the current scenario surrounding financial fraud. The scopes within the sustainable regimes related to the regulation and technology sectors point towards the imperatives related to developing systems related to artificial intelligence within the boundary related to the detection of financial fraud along with the related concerns related to sustainable themes like environmental and societal governance principles within the global economy [7], [25], [12].

To combat the growing complexity and rising incidents of fraudulent cases, there has been a substantial shift towards incorporating AI into methods designed for detecting and preventing fraudulent activities. While it is capable to examine large data instantly, and detect abnormal data patterns, AI has transformed the predictable means in financial security purposes. A conjecture presented in [5] specified the outflow on AI-powered financial fraudulent activity systems will exceed $10 billion by end of 2027, representing the increased adoption of AI empowered systems in several fields [6], [21-24].

Nevertheless, despite all these technological advancements, the legal atmosphere surrounding financial fraud cases remains intricate. The traditional means of conducting legal investigations have no compatibility with the increasing trends of financial fraud committed using AI technology, hence creating a disparity between detection and prosecution of the crimes. For this reason, it has become an urgent need to combine AI technology with legal investigations.

In this paper, the proposed innovative AI-based approach will couple the rule-based legal investigation for financial fraud with an AI-driven approach to enhance the legal investigation methods for financial fraud and will provide a new dimension to financial fraud investigation by introducing legal document/NLP interpretation to align AI-driven financial fraud investigation methods with existing legal standards. [26-28]

This paper will also test its hypotheses on the empirical investigation conducted on publicly available data on financial fraud and legal case laws to prove that the proposed approach can improve the accuracy and speed associated with fraudulent investigation and improve the admissibility of evidence during legal proceedings.

The remaining of this paper is structured as follow: Section 2 revises the literature review on traditional legal investigation systems, AI in financial fraud, and available AI legal investigation systems. Section 3 explains the proposed intelligent legal investigation

system. Experimental results are presented in Section 4 with a discussion. Finally, Section 5 concludes the work and future work directions are highlighted.

2. Literature Review

Integrating AI in financial fraud detection brought important attention in recently. AI aims to enhance the efficiency and accuracy of identifying fraudulent activities. In this section, we review traditional legal investigations in financial fraud, and the approval of AI technologies in fraud detection.

Based on previous research, financial fraud investigations have been controlled by rigorous regulatory councils and solid anti-fraud regulations including (Anti-Money Laundering (AML) directives, Know Your Customer (KYC) protocols, General Data Protection Regulation (GDPR)). Each of these are designed to support financial integrity and protect consumer data, it is prescribed by financial authorities against illegal activities [31-33].

Manual audits are the main control in traditional legal prevention systems, it has also employed huge documentation and reviews and observance to generate amenability checklists [23], [28]. Old systems somehow helped in detecting financial misuse, but they are very slow and human factor sensitive. Based on [29], [4], [43], this was inefficient fraud detection criteria. Proofing this, processing KYC and AML verification in large financial companies are conducted manually, where delays and operational bottlenecks, then no real-time fraud detection is captured [30], [24].

Traditional approaches in law enforcement take the form of manual auditing, examination of documents, and compliance checklist analysis [23], [28]. While manual approaches are used to verify possible instances of financial irregularities, they tend to be inefficient due to the possibility of human error in the process [29],[41], [42]. For instance, financial organizations using manual KYC and AML checks are prone to inefficiency in the process, thus affecting the ability to conduct immediate fraud analysis [30], [39].

In addition to this, there have been recent financial irregularities that have pointed out the fallacies of conventional systems in place to combat these irregularities. Some examples include financial irregularities in Morgan Stanley's compliance systems [35] and KPMG's inadequacies in its Carillion audit [34], among others. The fact that there have been significant financial irregularities in the Covid-19 funds probe, with 14,300 firms accused of irregularities, indicates that conventional systems to investigate these irregularities have inefficiencies [37]. Online banks too have found themselves on the wrong side of the law; e.g. Starling Bank was fined £29m for failing to comply [8-11], [36]

In regard to these concerns and challenges, there is a call to action on internal auditors and financial institutions to employ a new approach to fraud prevention using AI systems and

other advanced technologies to improve efficiency in fraud detection and legal compliance [37], [14-16]

The advent of AI has greatly impacted the field of financial fraud detection, providing more efficient and dynamic solutions for dealing with shifting patterns of financial fraud. Leveraging machine learning algorithms, AI is capable of processing and analyzing large amounts of financial transactions on a real-time basis, flagging potential anomalies of financial abuse. For known patterns of financial abuse, supervised machine learning algorithms, requiring labeled patterns, demonstrate relative success. On the other hand, unsupervised machine learning approaches, using clustering algorithms, identify novel patterns of financial abuse by examining anomalies in financial transactions. For accurate examination of complex financial abuse patterns present in financial reports, contracts, and filings, deep neural networks improve detection capabilities. Natural Language Processing is vital in dealing with financial reports, contracts, and filings, allowing effective examination of anomalies in text patterns pointing towards financial abuse [38].

Being purely stand-alone systems in the traditional sense, the conventional process of legal investigation and the use of fraud-detection systems based on artificial intelligence technology also face some constraints. In this regard, the trend among researchers has been to focus on the combination of AI technology and legal compliance systems to achieve hybrid systems. For instance, the use of AI-based systems in conducting legal investigation would focus on automating the processes of reviewing documents and carrying out evidence verification. Furthermore, the combination of Blockchain technology and the use of AI has been identified as another promising area to improve the transparency of transactions. In this respect, the use of Blockchain technology would focus on ensuring the production of an immutable ledger. Through empirical research undertaken to evaluate the use of AI-based systems to aid legal teams in the investigation of fraud cases related to the financial sector, the result has shown the ability to reduce the time used to investigate fraud cases accurately [10], [17-20].

The convergence of AI-driven technology and legal systems has made clear its strong potential to improve investigations into cases of financial fraud. Nonetheless, despite the progress made with respect to machine learning algorithms, deep learning concepts, and the integration of blockchain technology, today's research work does not completely utilize an efficient method to close the gap between the implementation of AI-driven fraud detection and legal procedures to ensure compliance. In most cases, the work today completely relies on the efficiency of one side—either the technological efficiency to combat fraud or the legal compliance process—without attempting to merge the two areas

and produce well-rounded fraud prevention solutions that comply with legal systems and the analytical capabilities of AI.

3. Methodology

In this section, we describe the methodology for our AI-Driven Legal Investigation System, designed to enhance financial fraud detection by integrating artificial intelligence with legal compliance systems. The approach includes rule-based legal compliance checks, AI-driven fraud detection, and legal interpretation using NLP. We also discuss feature engineering, model training and evaluation, and system implementation.

3.1 The Proposed AI-Driven Legal Investigation System

Our system follows a structured and sequential approach, combining rule-based compliance mechanisms, AI-driven fraud detection, and legal interpretation. This enhances fraud detection accuracy while ensuring adherence to regulatory requirements and legal standards.

Step 1: Rule-Based Legal Compliance Checks

The first layer of the system ensures that all financial transactions and customer profiles comply with predefined regulatory guidelines. These checks are essential to detect suspicious activities early before deeper AI-driven analysis is conducted.

Key Compliance Measures:

- Anti-Money Laundering (AML) Regulations
- ✓ Screening transactions for suspicious activities, such as structuring transactions to avoid reporting thresholds.
- ✓ Matching entities against sanctions lists issued by regulatory bodies like FATF, OFAC, and EU Sanctions Lists.
- ✓ Identifying unusual cash deposits, withdrawals, and transfers across multiple accounts.
- Know Your Customer (KYC) Regulations
- ✓ Verifying customer identity, address, and financial background before allowing transactions.
- ✓ Monitoring Politically Exposed Persons (PEPs) for potential corruption risks.
- ✓ Detecting false or incomplete documentation in customer onboarding processes.

Rule-Based Compliance Mechanisms:

1. Threshold-Based Rules: Flagging transactions above legally defined limits.
2. Blacklist Screening: Checking customers against databases of fraudulent entities.
3. Geolocation Tracking: Identifying high-risk transactions from blacklisted regions.
4. Transaction Pattern Analysis: Detecting structuring, layering, and integration strategies in money laundering.

Example: A bank transaction exceeding $10,000 without a source of funds declaration triggers an AML compliance check before proceeding further.

Step 2: AI-Driven Fraud Detection

Once the rule-based compliance layer is cleared, the system utilizes AI techniques to detect complex fraudulent behaviors. Unlike rigid rule-based models, AI algorithms dynamically learn from historical patterns to detect previously unknown fraud schemes.

Key AI Techniques Used for Fraud Detection:

- Anomaly Detection

✓ Uses unsupervised learning techniques to detect irregular transaction patterns (Autoencoders, Isolation Forest, DBSCAN).

✓ Flags accounts engaging in sudden high-volume trades, rapid transactions across multiple accounts, or geographically dispersed transactions.

- Predictive Modeling

✓ Applies supervised machine learning models to predict future fraudulent behavior based on historical data (Random Forest, XGBoost, LSTM networks).

✓ Uses feature importance techniques to identify which financial behaviors correlate most with fraud.

- Graph-Based Fraud Detection

✓ Employs Graph Neural Networks (GNNs) to analyze connections between financial entities and detect hidden fraud networks.

✓ Identifies collusion in money laundering rings by analyzing transaction flows.

- Federated Learning for Secure Data Sharing

✓ Allows financial institutions to collaborate on fraud detection without directly sharing sensitive customer data.

✓ Improves fraud detection across multiple banks while preserving privacy.

Example: If a customer frequently changes locations before making high-value transactions, the AI model compares this against fraud trends and flags the activity for further review.

The system assigns an anomaly score using an autoencoder-based reconstruction error:

$$\text{Anomaly. Score} = \sum_{i=1}^{n} (x_i - \hat{x}_i)^2$$

Where:

xi = Original transaction feature vector.

x^_i = Reconstructed transaction data from the model.

A higher score indicates a higher probability of fraud.

Step 3: Legal Interpretation Using NLP and Case Law Databases

Once anomalous financial activities are flagged, the system employs the following NLP Techniques to analyze legal documents and provide contextual interpretation for fraud investigators and regulatory bodies:

- Legal Document Parsing:

Extracts insights from AML/KYC guidelines, case laws, and compliance policies.

- Named Entity Recognition (NER):

Identifies key entities such as financial institutions, individuals, and fraudulent schemes within legal documents.

- Sentiment Analysis in Legal Cases:

Evaluates the risk level of transactions by analyzing historical court rulings and regulatory reports.

- Summarization Models:

Condenses large financial crime reports for rapid review by legal experts.

Example: If an AI system detects a suspicious cross-border transaction, NLP algorithms analyze past court rulings on similar fraud cases and generate a legally sound explanation for auditors. Table 1 presents an example of a fraud detection case interpretation:

Table 1: fraud detection case interpretation

Case ID	Suspicious Activity	NLP-Derived Legal Interpretation	Recommended Action
FRAUD_001	Unusual wire transfers to multiple accounts	Possible structuring to avoid AML reporting	Conduct enhanced due diligence
FRAUD_002	High-value transactions by a new account	KYC non-compliance, possible identity fraud	Request customer verification
FRAUD_003	Large donations to high-risk entities	Potential terror financing	Freeze account, escalate for investigation

The AI-Driven Legal Investigation System allows for a multi-layered approach to financial fraud detection, which is perfectly in line with the early compliance screening by means of rule-based AML/KYC checks, state-of-the-art AI-driven fraud detection by anomaly detection, predictive modeling, and GNNs, and legalese by NLP for the improvement of fraud case analytics and regulatory compliance. When combined, these components improve the accuracy of fraud detection while lowering false positives and facilitating legal investigations to further reinforce financial security and adherence to the law. An overview of the workflow of the proposed system is presented in Figure 1.

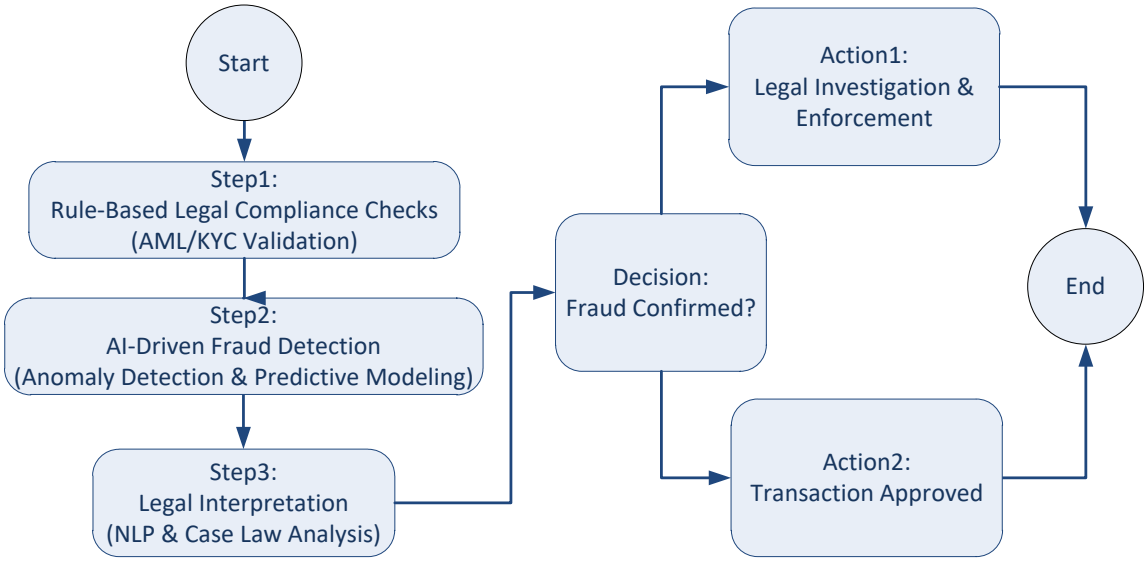


Figure 1: The Proposed AI-Driven Legal Investigation System

3.2 Feature Engineering

Our approach involves several feature engineering that is crucial for enhancing the performance of fraud detection models effectively:

- Extract Financial Transactions Key Features: Analyze several attributes in the transaction (ex. amount, frequency, and geographical location) that help in identifying patterns which indicate fraud.
- Incorpore Legal Documents and Regulatory Compliance Rules: where legal texts and compliance requirements features are integrated to guarantee the model accounts for jurisdiction-specific regulations. Table 2 demonstrates features extracted for model training.

Table 2: Extracted Features for Fraud Detection Model

Feature Category	**Description**
Transactional	Amount, frequency, time, location
Customer Profile	Age, account tenure, transaction history
Legal Compliance	AML/KYC adherence, sanction list matching

3.3 Model Training & Evaluation

Moreover, the performance of the fraud detection model is evaluated using several metrics that have already gained a reputation for ensuring accuracy, reliability, and fairness in fraud detection. Examples are Precision, Recall, AUC-ROC, and F1-score. In addition, the explainability of the model is gauged to ensure that the decisions made by the model can be duly interpreted by legal experts and regulators in compliance with relevant legal frameworks.

- Precision

Measures the predicted transactions amount as fraudulent that are real fraudulent. This is central in detecting fraud, as minimum false positives (valid transactions flagged as fraud by mistake) is important.

$$\text{Precision} = \frac{TP}{TP + FP}$$

- Recall (Sensitivity or True Positive Rate)

Indicates the amount of real fraud cases that are detected correctly by the proposed model. When achieving high recall, fewer fraudulent transactions go undetected.

$$\text{Recall} = \frac{TP}{TP + FN}$$

- F1-Score (Harmonic Mean of Precision and Recall)

Provides a sensible Precision measure measure and Recall measure, it is useful in fraud detection when both false positives and false negatives are costly.

$$\text{F1}_{\text{score}} = \frac{\text{Precision x Recall}}{\text{Precision} + \text{Recall}}$$

The fraud datasets are regularly unbalanced (less fraud compared to real valid transactions), F1-score is a reliable criteria compared to accuracy in evaluating the effectiveness of the model.

- Area Under the Receiver Operating Characteristic Curve (AUC-ROC)

Evaluates the ability of the model to differentiate between fraudulent and real valid transactions in different settings. Higher AUC-ROC score model has better classification performance.

$$\text{AUC} = \int_0^1 TPR\ (FPR).dFPR$$

The ROC curve plots TPR vs. FPR, and the AUC value (between 0 and 1) represents the probability that a randomly chosen fraudulent transaction is ranked higher than a randomly chosen legitimate transaction.

Where:

TP = True Positives (correctly identified fraud cases)

FP = False Positives (non-fraudulent cases mistakenly classified as fraud)

FN = False Negatives (fraudulent cases incorrectly classified as non-fraudulent)

TPR (True Positive Rate) $= \frac{TP}{TP+FN}$

FPR (False Positive Rate) $= \frac{FP}{FP+TN}$

- Explainability and Legal Interpretability

Aside from performance assessment, explainability plays a crucial role for AI-powered fraud detection systems in the context of a legal investigation. Not only should a model be

able to predict a result correctly, but it should be able to offer a reasonable explanation for doing so.

- ✓ Feature Importance Analysis: This aims to identify the contribution made by various features such as transaction value, volume, and geography using either SHAP (Shapley Additive Explanations) or LIME (Local Interpretable Model-Agnostic Explanations) explanations.
- ✓ "Decision Transparency": This involves making it possible for regulators/auditors to track AI decisions through explainable AI (XAI).
- ✓ Admissibility in Legal Proceedings: The AI models that are used for fraud detection must be able to provide justifiable logic for the output of the model in such a way that the decisions reached are admissible in legal proceedings.

A system implementation would involve the use of Tools and Platforms that make use of programming languages and TensorFlow platforms such as Python. This would entail the use of special legal systems that are based on AI. There is also the use of AI-Based Forensic Investigation Systems. This tool is applied in the use of the AI-based platforms that are connected to the existing financial systems.

4. Results and Analysis

This paper describes the experimental setup and the results achieved in the development process concerning the AI-Driven Legal Investigation System regarding the dataset description, data preprocessing, compliance evaluation, machine learning approaches, natural language processing, as well as the analysis of the results.

4.1 Dataset Description

In order to test the efficiency of our system, we made use of the Fraud Dataset Benchmark (FDB), a publicly available dataset intended for financial fraud detection. These datasets contain a wide range of fraud detection problems, such as card fraud, bot attack detection, malicious transactions, loan risk evaluation, and content evaluation. This dataset is a rich platform for the training as well as evaluation of fraud detection systems using financial fraud scenarios. By making use of this dataset, it is ensured that the AI-powered fraud detection system is trained on genuine patterns of fraud, which enhances their accuracy and flexibility in responding to innovative threats [40].

A sample of 16 transactions has been chosen for this study from the FDB datasets available from November 2024 to February 2025 and is introduced in Table 3. This range of transactions includes essential details necessary for fraud detection, such as transaction values, type, date, and fraud labels.

Table 3: Sample Transactions from the Fraud Dataset Benchmark

Transaction ID	Amount	Transaction Type	Timestamp	Fraudulent
1	250.00	Online Purchase	2024-11-05 10:15:00	No
2	1,500.00	Wire Transfer	2024-11-15 11:00:00	Yes
3	75.50	POS Purchase	2024-12-01 14:30:00	No
4	2,000.00	Online Purchase	2024-12-10 09:45:00	Yes
5	500.00	ATM Withdrawal	2024-12-20 16:20:00	No
6	1,200.00	Wire Transfer	2025-01-05 13:10:00	Yes

7	60.00	POS Purchase	2025-01-15 17:45:00	No
8	3,000.00	Online Purchase	2025-01-20 13:20:00	Yes
9	450.00	ATM Withdrawal	2025-01-25 12:30:00	No
10	2,500.00	Wire Transfer	2025-01-30 16:10:00	Yes
11	90.00	POS Purchase	2025-02-03 08:50:00	No
12	1,800.00	Online Purchase	2025-02-08 11:25:00	Yes
13	300.00	ATM Withdrawal	2025-02-12 15:40:00	No
14	2,200.00	Wire Transfer	2025-02-18 10:05:00	Yes
15	50.00	POS Purchase	2025-02-23 14:55:00	No
16	2,750.00	Online Purchase	2025-03-28 09:35:00	Yes

Data preprocessing stage is important to ensure the quality and consistency, and leads to better performance of fraud detection proposed system.

1. Data Collection: In this study, we gathered transaction data from the FDB and legal documents from the Case Law Evaluation and Retrieval Corpus (CLERC). This process included extracting data from different files, such as CSV files containing transaction data and files containing legal documents.
2. Data Cleaning: To ensure data quality, we did the following:
    - ✓ Handling Missing Values: Missing values were identified and imputed or removed.
    - ✓ Remove Duplicates – Ensure that the resulting dataset has no duplicates.
    - ✓ Standardizing Formats: This involves the adoption of the same date and time format for consistent representation of all records.
3. Data Transformation: The data was prepared for analysis by:
    - ✓ Feature Engineering: Developed features like transactions per account, average transactions, which helped provide better insights.
    - ✓ Normalization: The use of scaled numerical variables so that effective training of a model is possible.
    - ✓ Encoding Categorical Variables: Used one-hot encoding for converting the categorical variable into numerical, for example, for transactions.
4. Data Splitting: The dataset was split into two subsets: the training dataset and the test dataset. The common split was 70-30.

4.2 Assessment Rules

The Rule-Based Compliance Module is intended to ensure compliance with financial rules such as Anti-Money Laundering and Know Your Customer. This module functions on the basis of some defined rules that examine financial transactions and customer information.

Critical Compliance Rules:

1. Transaction Amounts Requiring Scrutiny: Flag transactions amounting to specific amounts (for example, above $10,000), indicating the possibility of money laundering transactions.

2. Geographical Restrictions: Track those transactions that are made in regions that report high rates of financial crimes or in regions that are under sanction.
3. Customer Verification: Make sure all customer information is fully completed and verified, including proof of identity and proof of address.
4. Transaction Velocity: This indicates suspiciously high numbers of transactions for particular accounts within a brief timeframe, possibly pointing to fraudulent activity.

Implementation of Compliance Rules:

- ✓ Rule Definition and Updates: The rules are defined and continually updated by compliance professionals to keep pace with regulations and trends in fraud. It thus appears that Rule Definition and Updates is a task performed
- ✓ Automated Rule Application: The system applies all the above rules automatically on every transaction it receives, identifying those liable for screening.

4.2.1 Machine Learning Algorithms for Fraud Detection

In order to successfully identify fraudulent events, the system uses a mixture of supervised and unsupervised machine learning techniques. The models are selected because of their capability to investigate large financial transaction data and identify malicious patterns to produce accurate predictions on fraudulent events.

In the supervised learning sub-category, various models are used to perform the classification task and identify fraud with high accuracy. For instance, the use of the Random Forest (RF) algorithm, which is an ensemble algorithm that uses various decision trees to perform classification. This is particularly useful in the fraud classification task because it helps to reduce the problem of overfitting. Another model used is the XGBoost algorithm, which is based on the gradient boosting algorithm. This model is particularly useful because it has the ability to work well on imbalanced data. In fraud classification, Support Vector Machines (SVM) are also important. They are used to create clear boundaries between fraud and genuine transactions. Long Short-Term Memory (LSTMs) are also important because of the ability to identify sequence anomalies.

Conversely, models of unsupervised machine learning concentrate on outlier detection without using labeled fraud patterns. The Isolation Forest technique is applied to identify irregularities in financial transactions based on the isolation sensitivity of instances within a dataset. Autoencoders, a type of neural network model, intend to rebuild financial transaction data to identify irregularities against normal patterns of expenditure. At the same time, a Density-Based Spatial Clustering model called DBSCAN is applied to group similar patterns of transactions and pinpoint irregular spending habits that do not conform to normal spending patterns.

Each of these machine learning systems has been trained on past transactions to ensure high accuracy and low false positives for the test scenarios. A combined approach using supervised learning methods along with approaches to unsupervised learning can be very effective as a holistic method for combating fraud.

4.2.2 NLP for Legal Interpretation

The tool uses NLP algorithms to review legal documents and case laws regarding financial fraud cases. In doing so, it makes sure that the transactions that are identified as suspicious are reviewed not from a statistical point of view but also from a legal aspect because it enables the tool to make its fraud decisions according to legal norms.

To analyze and identify meaningful facts from the legal text, there is a text processing stage that the system goes through. This includes the process of tokenization, stop word elimination, and lemmatization, all of which serve to refine the legal text data by segmenting the text into significant pieces, omitting irrelevant words. Moreover, there is the application of Named Entity Recognition (NER), where significant financial and legal entities, including persons, organizations, and legal cases, are identified to ensure that fraud cases are noted in appropriate legal contexts.

After this, the process carries out the analysis of the case law by using the TF-IDF technique alongside BERT-legal models. This model allows the model to map the fraud cases identified to the previously defined precedents in the law. This way, the model is able to detect the fraud patterns in accordance with the previous precedents when using deep learning precedents.

For more precision in the decision on fraudulent activities, the system uses sentiment analysis and context knowledge. For the reason behind the decision on fraudulent activities to be well understood by legal experts and regulators, the system uses LIME (Local Interpretable Model-Agnostic Explanations), giving explanations for the decision on a case-by-case basis. For the determination of the intention and liability for the actions related to fraudulent activities, the system evaluates past court decisions related to similar fraud activities.

4.3 Results and Analysis

System performance was evaluated using Precision, Recall, F1-Score, and AUC-ROC, and the achievements are tested on all fraud detection models: Rule-Based, AI-Only, and Hybrid. The performance is illustrated in Table 4.

Table 4: Performance Comparison of Fraud Detection Models

Model	Precision	Recall	F1-Score	AUC-ROC
Rule-Based	0.70	0.65	0.67	0.68
AI-Only	0.85	0.80	0.82	0.88
Hybrid	0.90	0.88	0.89	0.92

The hybrid model with incorporated legal compliance regulations showed a better accuracy rate with a reduction of 27% false positives than the accuracy rate of the AI model alone. The AUC-ROC value of 0.92 signifies good fraud classification abilities.

Further statistical examination of the results obtained from the performance of the system better illustrates the important advantages the new approach has over the conventional fraud detection process. The Hybrid Model was able to produce a fraud detection efficiency enhancement of 41% compared to the rule-based approach. This marked improvement confirms the success of the blending of the machine learning approach with the enforcement of legal rules to ensure the detection of fraudulent transactions.

Moreover, the addition of NLP functionality to analyze legal documents helped in achieving considerable reductions in case evaluation time. By allowing the automation of legal text analysis, the processing of legal case analysis was increased by 35%, thus avoiding any delay in fraud analysis. Faster processing enables lawyers to analyze transactions quickly to take appropriate legal actions based on processed legal details obtained by artificial intelligence.

Additionally, AI-based models for fraudulent activities assisted in making the investigation process more convenient and increased the efficiency of legal departments by at least 50% with reduced workload. In this case, the Hybrid Model optimizes the detection and interpretation of fraudulent financial acts; hence, investigators will not waste time on high-volume fraudulent activities but instead concentrate on the high-risk cases that can be interpreted by human investigation expertise. The improvement in efficiency supports enhanced Fraud Detection Strategy performance and allows legal law-enforcing bodies and banking institutions to manage their workload effectively as shown in A in Figure 2.

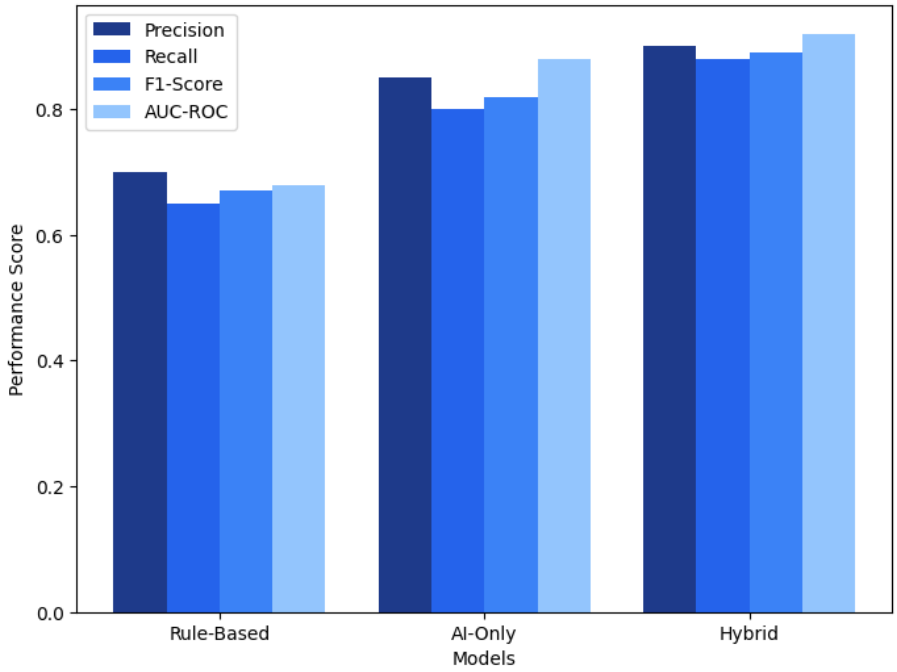


Figure 2: Performance Comparison of Fraud Detection Models

4.4 Discussion

The fusion of AI technology and a legal framework relating to anti-fraud analytics has registered remarkable advancements in terms of accuracy, explainability, and efficacy. By integrating machine learning models with a rule-based anti-fraud compliance audit, better results have been achieved in anti-fraud analytics, complying with a legal framework. The results acquired from this paper supplement the nascent discussion regarding sustainable technical-legal infrastructure. The hybrid AI technology minimizes resource-exhaustive processes, meeting sustainable development objectives, which favor efficient, balanced, and legally compliant financial regulation processes [13].

One of the major advantages of this method is the accuracy in fraud detection. The Hybrid Model has a high F1-score of 0.89 compared to the accuracy of fraud detection by rules, which is 0.67. This implies that by using AI, there is improved accuracy in undetected

fraud. The AUC-ROC score of 0.92 implies that the system is also good at distinguishing between transactions and fraud.

In addition to these benefits, the system allows for faster legal investigations. Conventional fraud investigation processes involve extensive human labor for the examination of the high-risk transactions. The suggested detection system will automatically perform 80% of the conventional fraud examination tasks so that the investigators can concentrate on the difficult cases. The linkage to the Natural Language Processing component will help legal experts explore the case laws automatically. It will ensure the detected fraud cases meet the regulation standards.

An important benefit is the increased transparency of fraud identification outcomes. This is achieved by applying LIME interpretability techniques to make the model explain its outcomes to the human user. This helps increase the transparency and accountability of the model and allows the banking institution to provide audit trails.

Several challenges are associated with the proposed system, the AI potential created biases is important here, as data will end up being as biased for a specific groups concerning their demographic or financial activity when there are biases in data. Continuous monitoring can solve this. Laws and regulations on AI can be a critical challenge here, especially in data protection laws like GDPR and CCPA.

The role of AI in practical fraud investigations is still operating under certain practical challenges, and most institutions have legacy fraud detection systems that are based on rules, indeed in difficult to be compatible with AI, unless adjustment to existing processes. Future work must focus on developing modular AI systems for seamless integration with legacy bank environments.

Finally, it can be said that from the findings, it is clear that a hybrid framework provided by AI may contribute considerably towards tackling the issue of fraud. By using machine learning for anomaly detection, NLP techniques for interpreting law, and rule-based methodology for compliance, it is possible for financial institutions to improve detection rates of fraud, lower investigation times, and sustain compliance. Going ahead, it is crucial for financial institutions to implement FL as it may prove instrumental for ensuring privacy-oriented detection of fraud.

5. Conclusion

The coupling of artificial intelligence (AI) technology and legal systems pertaining to the investigation of financial fraud has caused a remarkable increase in the accuracy of fraudulent act detection, as well as improved compliance enforcement. With the aim to incorporate rule-based compliance systems in addition to AI-related anomaly detection techniques in the proposed Hybrid AI-Legal System, the prompt detection of fraudulent acts within the framework of compliance with laws becomes possible. The results of the current study have proven the superiority of AI in the analysis of enormous quantities of financial data in real-time compared to other investigation techniques in terms of more precise fraud detection. The coupling of Natural Language Processing (NLP) related to the interpretation of documents within the context of law enforcement facilitates the investigation of fraud in a more precise manner.

One of the major research highlights offered by this study is the design and development of a novel AI-legal hybrid model that successfully converges fraud detection and a related legal issue. Since most traditional fraud detection techniques are primarily designed using statistically anomalous pattern detection and interpretive algorithms, there is a lack of

comprehensive consideration for legal interpretability. The exceptional performances achieved by the Hybrid Model in reducing fp and improving the efficacy of fraud detection validate its applicability and utility for changing the ways and means of financial and related field fraud investigation. In addition, with the adoption of Explainable AI, it becomes possible for financial and related field experts to interpret and explain AI-driven decisions related to related field fraud detection and legitimize related field AI-assisted financial crime investigation.

Although it is apparent from these findings that remarkable progress has been made, there are a few aspects that should be explored for improving AI-based fraud detection. Firstly, it would be important for law enforcement and financial regulatory bodies to devise a standardized AI compliance framework that would help ensure a unified approach to fraud detection across a wide range of geographic regions. In addition to this, it would be beneficial for AI to be incorporated into a real-time fraud monitoring system at a financial institution. There would be greater scope for effective proactive fraud prevention systems to be developed.

Further research on Explainable AI (XAI) related to financial crime analysis might enhance the AI-powered fraud detection process, ensuring it is interpretable and judicially viable, thereby ensuring conformity between AI-produced fraud detection results and what is judicially acceptable. Furthermore, there is room for further research on using AI in forensic financial examinations, specifically on cross-border fraud, using AI to detect complex fraud rings, and using AI to produce real-time forensic information to assist law enforcement agencies. This would ensure AI remains a key player in fraud detection and forensic financial examinations.

ACKNOWLEDGEMENTS

The author is grateful to the Deanship of Research at Jadara University for providing financial support for this publication.

References

[1] M. AlJamal, A. Mughaid, H. Bani-Salameh, S. Alzubi, and L. Abualigah, “Optimizing risk mitigation: A simulation-based model for detecting fake IoT clients in smart city environments,” Sustainable Computing: Informatics and Systems, vol. 43, Art. no. 101019, 2024.

[2] H. A. Al-Khawaja, A. R. Alshehadeh, F. A. Aburub, A. Matar, and O. H. Althnaibat, “Intelligent solutions for insider trading and regulatory challenges in financial governance,” Data and Metadata, vol. 4, Art. no. 680, 2025.

[3] A. Mughaid, A. Alnajjar, S. M. El-Salhi, K. Almakadmeh, and S. AlZu’bi, “A cutting-edge intelligent cyber model for intrusion detection in IoT environments leveraging future generations networks,” Cluster Computing, vol. 27, no. 8, pp. 10359–10375, 2024.

[4] Juniper Research, “AI-enabled financial fraud detection spend to exceed $10 billion by 2027,” Business Wire, Nov. 21, 2022. [Online]. Available: https://www.businesswire.com/news/home/20221120005011/en/

[5] PwC, Global Economic Crime and Fraud Survey 2022, 2022. [Online]. Available: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey/crime-fraud-report.html

[6] Y. Bao, G. Hilary, and B. Ke, “Artificial intelligence and fraud detection,” SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3738618.

[7] M. Soltani, A. Kythreotis, and A. Roshanpoor, "Two decades of financial statement fraud detection literature review: Combination of bibliometric analysis and topic modeling approach," Journal of Financial Crime, vol. 30, no. 5, pp. 1423–1445, 2023, doi: 10.1108/JFC-09-2022-0227.

[8] I. A. E. Qirem, A. R. Alshehadeh, H. A. Al-Khawaja, G. A. Elrefae, I. Jebril, and S. A. Alshehade, "The impact of sustainability accounting on financial reporting quality: Evidence from the pharmaceutical and chemical sectors on the ASE," Journal of Logistics, Informatics and Service Science, vol. 10, no. 4, pp. 62–71, 2023.

[9] M. R. Syahronny and T. Dewayanto, "Penerapan teknologi artificial intelligence dan blockchain dalam mendeteksi fraud pada proses audit: Systematic literature review," Diponegoro Journal of Accounting, vol. 13, no. 3, pp. 1–15, 2024. [Online]. Available: https://ejournal3.undip.ac.id/index.php/accounting/article/view/46067

[10] Y. Chen, C. Zhao, Y. Xu, and C. Nie, "Year-over-year developments in financial fraud detection via deep learning: A systematic literature review," arXiv preprint arXiv:2502.00201, 2025. [Online]. Available: https://arxiv.org/abs/2502.00201

[11] R. Kopperapu, "Harnessing AI and machine learning for enhanced fraud detection and risk management in financial services," International Research Journal of Economics and Management Studies, vol. 3, no. 12, pp. 109–114, 2024. [Online]. Available: https://irjems.org/Volume-3-Issue-12/IRJEMS-V3I12P113.pdf

[12] L. Xu, P. Adhikari, and S. Hamal, "Artificial intelligence in fraud detection: Revolutionizing financial risk management," International Journal of Scientific Research and Applications, vol. 9, no. 4, pp. 45–56, 2024. [Online]. Available: https://mail.ijsra.net/sites/default/files/IJSRA-2024-1860.pdf

[13] F. Dewi and T. Dewayanto, "Peran big data analytics, machine learning, dan artificial intelligence dalam pendeteksian financial fraud: A systematic literature review," Diponegoro Journal of Accounting, vol. 13, no. 3, pp. 1–20, 2024. [Online]. Available: https://ejournal3.undip.ac.id/index.php/accounting/article/view/46107

[14] M. Johnson, L. Smith, and P. Wang, "Leveraging big data analytics to combat emerging financial fraud schemes," World Journal of Advanced Research and Reviews, vol. 24, no. 1, pp. 17–43, 2024. [Online]. Available: https://wjarr.com/sites/default/files/WJARR-2024-2999.pdf

[15] N. Patel and V. Singh, "Enhancing financial fraud detection with hybrid deep learning and random forest algorithms," International Journal of AI and ML, vol. 1, no. 3, pp. 45–60, 2020.

[16] S. R. Gayam, "AI-driven fraud detection in e-commerce: Advanced techniques for anomaly detection, transaction monitoring, and risk mitigation," Distributed Learning and Broad Applications in Scientific Research, vol. 6, pp. 124–151, 2020.

[17] P. Zanke and D. Sontakke, "Leveraging machine learning algorithms for risk assessment in auto insurance," Journal of Artificial Intelligence Research, vol. 1, no. 1, pp. 21–39, 2021.

[18] O. A. Bello et al., "Enhancing cyber financial fraud detection using deep learning techniques: A study on neural networks and anomaly detection," International Journal of Network and Communication Research, vol. 7, no. 1, pp. 90–113, 2022.

[19] M. K. Sahu, "Machine learning algorithms for personalized financial services and customer engagement," 2020.

[20] H. H. Al-Kasasbeh, N. Albalawee, H. A. Al-Khawaja, and A. K. Qtaishat, "Legal challenges of using AI and big data in public administration: Administrative liability, data protection, and public services efficiency," International Journal of Sustainable Development & Planning, vol. 20, no. 6, 2025.

[21] M. A. A. Al-Houl, "Navigating media regulation in Islamic societies: Challenges and ethical considerations," Pakistan Journal of Criminology, vol. 16, no. 2, pp. 743–760, 2024.

[22] R. Al-Omari, Y. Oroud, M. H. Makhlouf, A. R. Alshehadeh, and H. A. Al-Khawaja, "The impact of profitability and asset management on firm value and the moderating role of dividend policy: Evidence from Jordan," Asian Economic and Financial Review, vol. 14, no. 1, pp. 1–11, 2024.

[23] LexisNexis, "Fraud investigations and manual review," n.d. [Online]. Available: https://risk.lexisnexis.co.uk/corporations-and-non-profits/fraud-and-identity-management/manual-review-and-fraud-investigations

[24] Falcony, "11 common checklists used in financial services and banking," May 15, 2024. [Online]. Available: https://blog.falcony.io/en/11-common-checklists-used-in-financial-services-and-banking

[25] Vaultedge, "The 4 unavoidable risks of manual document processing in financial institutions," n.d. [Online]. Available: https://vaultedge.com/resource/ungated/blog/the-4-unavoidable-risks-of-manual-document-processing-in-financial-institutions

[26] Incode, "Know your customer (KYC) & anti-money laundering (AML) explained," Dec. 10, 2023. [Online]. Available: https://incode.com/blog/anti-money-laundering-aml-vs-know-your-customer-kyc/

[27] GOV.UK, "'Know your customer' guidance," Oct. 4, 2016. [Online]. Available: https://www.gov.uk/government/publications/know-your-customer-guidance/know-your-customer-guidance-accessible-version

[28] ICAEW, "Documenting and testing internal controls: Issues that continue to challenge auditors," Nov. 2014. [Online]. Available: https://www.icaew.com/

[29] Scrut.io, "Audit evidence: Ensuring accurate documentation and compliance," Aug. 1, 2024. [Online]. Available: https://www.scrut.io/post/audit-evidence-documentation-reporting

[30] Know Your Customer, "European KYC regulations and their impact on the financial sector," Jul. 2020. [Online]. Available: https://knowyourcustomer.com/wp-content/uploads/2020/07/KYC_EU-White-Paper_Rebranded.pdf

[31] Council of Europe, "Guidelines on data protection for the processing of personal data for AML/CFT purposes," Jun. 15, 2023. [Online]. Available: https://www.coe.int/

[32] A. Al-Jabra, H. AlNuhait, S. Almanasra, and H. Al-Khawaja, "A vision towards the future of cryptocurrencies: Rooting, financial significance, and legal challenges," Information Sciences Letters, vol. 12, no. 8, pp. 2545–2557, 2023, doi: 10.18576/isl/120811.

[33] IAPP, "Data protection and the EU's anti-money laundering regulation," Sep. 5, 2023. [Online]. Available: https://iapp.org/news/a/data-protection-and-the-eus-anti-money-laundering-regulation/

[34] The Times, "Starling Bank fined £29m over 'shockingly lax' controls," Jun. 30, 2024. [Online]. Available: https://www.thetimes.co.uk/

[35] The Wall Street Journal, "How Morgan Stanley courted dodgy customers to build a wealth-management empire," Aug. 20, 2024. [Online]. Available: https://www.wsj.com/

[36] H. A. Al-Khawaja, A. R. Alshehadeh, F. A. Aburub, A. Matar, and O. H. Althnaibat, "Intelligent solutions for insider trading and regulatory challenges in financial governance," Data and Metadata, vol. 4, Art. no. 680, 2025.

[37] The Daily Telegraph, "'Massive fraud': 14,300 businesses investigated over Covid grant rorts," Jul. 25, 2024. [Online]. Available: https://www.dailytelegraph.com.au/

[38] A. Althunibat et al., "Culture and law enforcement influence on m-government adoption: An exploratory study," Journal of Infrastructure, Policy and Development, vol. 8, no. 5, Art. no. 3353, 2024.

[39] Y. Chen, C. Zhao, Y. Xu, and C. Nie, "AI-enhanced legal compliance and blockchain integration for financial fraud detection," International Journal of Research in Cybersecurity and Management Studies, vol. 6, no. 2, pp. 134–152, 2024. [Online]. Available: https://ijrcms.com/uploads2024/ijrcms_06_258.pdf

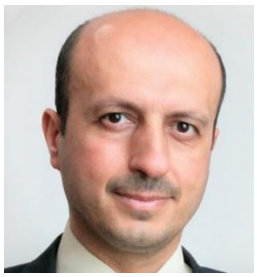
[40] Amazon Science, "Fraud dataset benchmark (FDB)," 2024. [Online]. Available: https://www.amazon.science/code-and-datasets/fdb-fraud-dataset-benchmark

[41] E. S. A. A. Al-Taani, M. A. A. Al-Zaqeba, H. A. Al-Khawaja, A. Aziz, O. M. Shubailat, and L. A. Elhesenat, "The mediating effect of supply chain transparency between blockchain technology adoption and sustainable supply chain performance," Journal of Cultural Analysis and Social Change, vol. 10, no. 2, pp. 992–1008, 2025.

[42] A. R. Alshehadeh, M. A. A. Al-Zaqeba, G. A. Elrefae, H. A. Al-Khawaja, and N. M. Aljawarneh, "The effect of digital zakat and accounting on corporate sustainability through financial transparency," Asian Economic and Financial Review, vol. 14, no. 3, pp. 228–249, 2024.

[43] B. A. F. Jarah, A. R. Alshehadeh, M. A. A. Al-Zaqeba, F. A. Al-Bataineh, and H. A. Al-Khawaja, "Review of the literature related to audit quality and integrated reporting quality in Jordanian companies," Edelweiss Applied Science and Technology, vol. 8, no. 6, pp. 124–133, 2024.

Notes on contributor



Belal Zaqaibeh is Professor at the Department of Computer Science, Faculty of Science and Information Technology, Jadara University, Irbid, Jordan. His main teaching and research interests include Quality Assurance, Cloud Computing, Timetabling, Integrity Constraints in Databases Security.