SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V10I7P102

Volume 10 Issue 7, 6-20, July 2023

Original Article

Artificial Intelligence and Machine Learning in Forensic Accounting

Avinash Malladhi

NewYork, USA

Received: 29 May 2023 Revised: 03 July 2023 Accepted: 16 July 2023 Published: 31 July 2023

Abstract *- This paper reviews the application of artificial intelligence (AI) and machine learning (ML) for fraud detection in forensic accounting. We analyze commonly used supervised learning algorithms like support vector machines (SVMs), random forests, and neural networks. Unsupervised techniques are also discussed, including clustering, anomaly detection, and association rule mining. For feature engineering, natural language processing (NLP) enables the analysis of unstructured text data, while deep learning methods like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can extract features from raw data. Empirical results demonstrate the high accuracy of ensemble models combining multiple algorithms compared to individual models. However, challenges remain regarding model interpretability, bias, and regulatory compliance. Overall, AI and ML can enhance forensic accounting through automated analysis of massive datasets and identification of complex fraudulent patterns. Further research into ethical AI and standardized implementation is needed to realize the potential of these emerging technologies fully.*

Keywords *- AI, Machine Learning, Forensic accounting & Fraud detection, Anti Money Laundering, Benford's law, Fraud triangle theory.*

1. Introduction

The rapid growth of digitalization and the complexity of financial transactions in today's global economy have paved the way for the rise of financial fraud and white-collar crime [1]. To combat this challenge, forensic accounting, a specialized branch of accounting that focuses on detecting and preventing financial fraud [2], has been continuously evolving, adopting innovative methodologies and techniques. Among the most promising advancements in this field is the integration of Artificial Intelligence (AI) and Machine Learning (ML) algorithms, which have shown great potential in enhancing the efficiency and effectiveness of fraud detection [3,4].

With the increasing complexity of financial fraud schemes and the need for efficient and accurate detection methods, AI and ML have emerged as indispensable tools for forensic accountants [5]. Recent literature has reported the successful application of various AI/ML algorithms in detecting anomalous patterns and fraud schemes in financial data [6,7]. These algorithms have been employed to analyze large volumes of structured and unstructured data, uncover hidden relationships, and identify potentially fraudulent activities [8,9]. These algorithms have demonstrated the ability to analyze complex, nonlinear relationships, identify patterns, and make highly accurate predictions [10]. In particular, supervised and unsupervised ML techniques such as decision trees, neural networks, clustering, and deep learning have been effectively applied to various aspects of fraud detection [11,12,13]. Furthermore, AI/ML techniques have been increasingly integrated with traditional forensic accounting tools, such as Benford's Law and the Fraud Triangle Theory, to augment their capabilities in identifying financial misconduct [14,15].

This paper aims to provide a comprehensive review of the recent advancements in forensic accounting, focusing on applying AI/ML algorithms for fraud detection. We will discuss the main types of AI/ML algorithms utilized in this context, such as supervised and unsupervised learning, deep learning, and natural language processing, along with their respective strengths and limitations [3,4]. Additionally, we will examine the most notable case studies and practical implementations of these algorithms in detecting and preventing financial fraud [16]. Lastly, this paper explores the prospective advancements and the ethical implications associated with applying AI/ML techniques in forensic accounting.

2. Literature Review

The application of artificial intelligence (AI) and machine learning (ML) for fraud detection in forensic accounting has received increasing research attention in recent years [1]-[4]. [125] provided a comprehensive overview of AI techniques used for financial fraud detection

in auditing and accounting. They discussed common supervised learning algorithms, including logistic regression, random forests, support vector machines (SVMs), and neural networks. The study highlighted that ensemble models combining multiple algorithms tend to outperform individual models.

Unsupervised learning techniques are also gaining traction for fraud detection. Kirkos [126] experimented with clustering algorithms like k-means and hierarchical clustering to identify fraudulent transactions without labeled training data. Association rule mining has also been applied to uncover patterns and anomalies in procurement fraud [127]. Feature engineering is a critical step in applying machine learning for fraud detection.[128] utilized natural language processing (NLP) to extract linguistic features from emails and legal documents, which were then used to train an SVM classifier. Deep learning methods like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are also being explored for learning complex feature representations from raw data [129].

While AI shows promise for enhancing forensic accounting, challenges remain.[53] highlighted issues around interpretability and bias in AI models. They argued for designing transparent and ethical AI systems. Regulation and oversight of AI in the finance industry also need to be addressed [52]. In conclusion, existing literature demonstrates the potential of AI and ML for improving fraud detection in forensic accounting by analyzing massive datasets and identifying subtle patterns. However, researchers emphasize that the technology must be implemented carefully with consideration to model transparency, fairness, and regulatory compliance. More research is needed to develop robust and ethical AI tools for forensic accounting applications.

2. Harnessing the Power of AI and ML in Forensic Accounting in Financial Fraud

AI and ML are increasingly employed in forensic accounting to enhance detection and analysis processes in various real-life scenarios. Practical applications of AI and ML in forensic accounting include:

2.1. Anti-money Laundering (AML) and Suspicious Activity Monitoring

Financial institutions use AI/ML algorithms to monitor transactions and customer behavior to identify potential money laundering or other suspicious financial activities [12]. By automatically flagging suspicious transactions for further investigation, AI/ML algorithms help financial institutions comply with AML regulations and prevent financial crimes. Internal fraud detection: Organizations use AI/ML algorithms to monitor employee activities and transactions, such as expense reports, payroll, and procurement processes [12]. By analyzing patterns and anomalies in the data, these algorithms detect possible internal fraud, such as embezzlement, kickbacks, or expense report manipulation, thus helping organizations minimize financial losses and maintain internal controls.

2.2. Insurance Claim Investigations

Insurance companies use AI/ML algorithms to analyze claims data, looking for patterns and anomalies that may indicate fraudulent claims [12]. For instance, clustering algorithms can group similar claims, allowing investigators to identify outliers or unusual trends. This helps insurers identify potentially fraudulent claims, reducing the financial impact of insurance fraud on the industry.

2.3. Credit Card Fraud Detection

Banks and financial institutions employ AI/ML algorithms to monitor credit card transactions and identify potentially fraudulent activities in real-time [11]. By analyzing transaction data, algorithms such as neural networks and decision trees can detect unusual patterns, allowing financial institutions to take immediate action to prevent unauthorized transactions and minimize losses due to fraud.

2.4. Tax Evasion Detection

Tax authorities use AI/ML algorithms to analyze taxpayer data and identify potential tax evasion cases [12]. By examining patterns in income, expenses, and deductions, ML algorithms can detect anomalies and inconsistencies that may indicate tax evasion or underreporting of income. This helps tax authorities prioritize investigations, improving the efficiency of their enforcement efforts.

2.5. Bankruptcy and Insolvency Analysis

AI/ML algorithms are used to analyze the financial data of distressed companies, identify the causes of financial distress, and predict the likelihood of bankruptcy [3]. This information helps stakeholders, such as creditors, investors, and regulators, make informed decisions and take appropriate actions to minimize financial losses.

2.6. Audit Support and Risk Assessment

Auditors use AI/ML algorithms to analyze large volumes of financial data, identify high-risk transactions, and assess the overall risk of fraud or financial misstatement [2]. By automating the data analysis process, AI/ML algorithms improve the efficiency of audits and reduce the likelihood of human error in detecting financial irregularities.

3. Application of AI/ML Algorithms in Forensic Accounting

3.1. Supervised Learning

Supervised learning algorithms, such as logistic regression, decision trees, and support vector machines, have

been widely used for fraud detection in forensic accounting [10]. These techniques rely on labeled datasets to learn patterns associated with fraudulent transactions and make predictions [18].

3.2. Unsupervised Learning

Unsupervised learning algorithms, such as clustering and anomaly detection techniques, do not rely on labeled data and can be used for fraud detection when labeled data is scarce or unavailable [19]. Clustering algorithms, like k-means and DBSCAN, group similar data points together and can help identify outliers or unusual patterns in the data [20]. Anomaly detection techniques, such as one-class SVM and isolation forests, aim to identify data points that deviate significantly from the norm [21]. While unsupervised learning methods can be useful in fraud detection, they may be less accurate than supervised methods due to the lack of labeled data for learning [19].

3.3. Semi-Supervised Learning

Semi-supervised learning algorithms utilize both labeled and unlabeled data for training, which can be particularly useful in fraud detection scenarios where labeled data is limited or expensive to obtain [22]. These algorithms, such as label propagation, co-training, and self-training, can improve the performance of classifiers by leveraging the information contained in the unlabeled data [23]. However, the success of semi-supervised learning techniques depends on the quality of the labeled data and the assumptions made about the relationships between labeled and unlabeled data [24].

3.4. Reinforcement Learning

Reinforcement learning algorithms learn to make decisions by interacting with their environment and receiving feedback in the form of rewards or penalties [25]. In the context of fraud detection, reinforcement learning can be used to optimize the decision-making process for detecting and preventing fraudulent activities, particularly in dynamic environments where fraud patterns may change over time [26]. However, reinforcement learning algorithms can be sensitive to the choice of a reward function and may require significant amounts of data and computational resources for training [25].

3.5. Hybrid Approaches

Hybrid approaches combine multiple learning algorithms or techniques to improve fraud detection performance [27]. These approaches can leverage different methods' strengths while mitigating their weaknesses. For example, supervised and unsupervised methods can be combined to take advantage of both labeled and unlabeled data, or deep learning techniques can be integrated with traditional machine learning models to enhance feature extraction and classification performance [28]. While hybrid approaches have the potential to deliver superior results, they can be more complex to implement and may require additional computational resources [27].

4. Natural Language Processing (NLP) in Forensic Accounting

NLP algorithms are used in forensic accounting to analyze textual data, such as financial statements and emails, for detecting fraud or other irregularities. They can extract relevant information from textual data and analyze them to identify patterns or anomalies that may indicate fraudulent activities [29][30][31]. Some NLP techniques applied in forensic accounting and fraud detection include:

4.1. Text Classification

Text classification automatically categorizes documents into predefined classes based on their content [32]. It has been applied to forensic accounting by classifying financial documents as potentially fraudulent or non-fraudulent based on their textual features [33]. However, it requires labeled datasets for training and may struggle with imbalanced classes [32].

4.2. Sentiment Analysis

Sentiment analysis extracts subjective information from textual data [34]. It has been used in forensic accounting to identify potential fraud by analyzing the sentiment expressed in financial documents [31]. However, it may be sensitive to the choice of sentiment lexicon and may struggle with context-dependent sentiment expressions [34].

4.3. Topic Modeling

Topic modeling discovers hidden thematic structures in large collections of documents [35]. It has been applied to forensic accounting to identify potential fraud by uncovering unusual topics or patterns in financial documents [36]. However, it requires selecting appropriate parameters, such as the number of topics [35].

4.4. Entity Recognition

Entity recognition identifies and classifies named entities in textual data [37]. Forensic accounting has used it to extract relevant information from financial documents [38]. However, it may be sensitive to variations.

5. Deep Learning Techniques in Forensic Accounting

Deep learning techniques, particularly neural networks, have demonstrated potential in detecting intricate fraud patterns by learning high-level features from extensive datasets [39]. Neural networks have proven their effectiveness in identifying financial fraud by discerning complex patterns in financial data, generalizing across diverse fraud scenarios, and adapting to new fraud types [39], [40]. Multiple studies have reported that neural networks surpass traditional statistical methods, such as logistic

regression, in detecting financial fraud [41], [42]. Examples of deep learning models applied to fraud detection include convolutional neural networks (CNNs) and recurrent neural networks (RNNs) [40].

5.1. Feedforward Neural Networks in Forensic Accounting

Feedforward neural networks (FNNs) are a basic type of neural network applied to fraud detection in forensic accounting [41]. FNNs comprise layers of interconnected nodes or neurons that learn patterns in input data and generate predictions for the output [43]. FNNs can be trained using supervised learning techniques, like backpropagation, to classify financial transactions as fraudulent or non-fraudulent [41].

5.2. Recurrent Neural Networks

Recurrent neural networks (RNNs) are a type of neural network capable of processing data sequences, making them particularly suitable for detecting financial fraud patterns that evolve over time [40]. RNNs have been used to analyze time-series financial data and identify anomalies that may indicate fraudulent activities [42].

5.3. Convolutional Neural Networks

Convolutional neural networks (CNNs) have been employed in fraud detection in forensic accounting by examining complex patterns in financial data, such as those found in images, graphs, or unstructured text [40]. CNNs can learn high-level features from input data and accurately classify transactions as fraudulent or non-fraudulent [44].

6. Benford's Law and the Fraud Triangle Theory

Benford's Law and the Fraud Triangle Theory are two widely recognized tools in forensic accounting that aid in detecting and preventing financial fraud.

Benford's law, also known as the First-Digit Law, is a statistical observation that states that in many naturally occurring datasets, the first digits are not uniformly distributed but instead follow a logarithmic distribution [14]. In particular, smaller digits, such as 1 and 2, are more likely to appear as the first digit than larger digits, such as 8 and 9. This law has been applied to various fields, including financial data analysis, to detect anomalous patterns and irregularities that may suggest fraudulent activities [14]. When the distribution of the first digits in financial data significantly deviates from the expected Benford's Law distribution, it can serve as a red flag for potential fraud. The Fraud Triangle Theory, introduced by criminologist Donald Cressey, posits that three conditions must be present for an individual to commit fraud: pressure, opportunity, and rationalization [45]. Pressure refers to the financial or personal stress that motivates an individual to commit fraud, such as mounting debts or maintaining a certain lifestyle. An opportunity arises when the individual has access to assets or information and perceives a low risk of being caught. Rationalization is the process by which the individual justifies their fraudulent actions, often by downplaying the consequences or shifting the blame to others. By understanding the factors that contribute to the Fraud Triangle, forensic accountants can better identify potential areas of vulnerability and implement preventive measures to minimize the risk of fraud.

Recently, AI/ML techniques have been integrated with traditional forensic accounting tools like Benford's Law and the Fraud Triangle Theory to enhance their capabilities in identifying financial misconduct. By leveraging the computational power of AI/ML algorithms, forensic accountants can analyze large datasets more efficiently, identify subtle patterns, and generate more accurate predictions of potential fraud. [3,46]

AI and ML can be embedded with Benford's Law to enhance their capabilities in detecting financial fraud by automating the analysis process, identifying complex patterns, and improving prediction accuracy[3]. Here are a few ways AI and ML can be integrated with Benford's Law: Automating the analysis process: AI and ML algorithms can automatically apply Benford's Law to large datasets, significantly reducing the time and effort required for manual data analysis. By quickly scanning through financial data and calculating the first-digit distribution, these algorithms can flag deviations from the expected distribution, indicating potential fraud[3].

6.1. Feature Extraction and Selection

ML techniques can be used to identify the most relevant features in financial data that are likely to exhibit Benford's Law patterns. Focusing on these features makes the analysis process more targeted and efficient. Additionally, ML algorithms can create new features or combinations of existing features to capture the underlying patterns better[3].

6.2. Anomaly Detection

Unsupervised ML algorithms, such as clustering or outlier detection techniques, can be used to analyze the deviations from Benford's Law in a dataset. These methods can help identify unusual patterns that may not be evident through traditional analysis, thereby increasing the likelihood of detecting fraudulent activities[3].

6.3. Predictive Modeling

Supervised ML algorithms can be trained to predict the likelihood of financial fraud based on deviations from Benford's Law and other relevant features. These models can be continuously updated with new data to improve their

prediction accuracy, providing a dynamic tool for fraud detection and prevention[3].

6.4. Ensemble Methods

Combining the results of multiple ML algorithms or models can enhance the overall performance of the fraud detection system. For example, Benford's Law analysis can be used as a feature in an ensemble model, along with other financial indicators and ML-generated features, to improve the overall predictive accuracy of the system[3].

6.5. Deep Learning

Advanced deep learning techniques, such as neural networks and autoencoders, can be used to identify complex and nonlinear patterns in financial data that may indicate fraud. The detection capabilities can be further enhanced by incorporating Benford's Law analysis results as input to these models [3].

7. Customization and Adaptability of AI and ML Algorithms with Benford's Law

7.1. Identifying Complex and Nonlinear Patterns Indicative of Fraud

In this example, a synthetic financial dataset is used with a simple deep-learning model to identify complex and nonlinear patterns indicative of fraud. Benford's Law analysis results are incorporated as an input feature to enhance the model's detection capabilities. For this purpose, the Keras library is used to create the deep learning model. The model below calculates Benford's Law first-digit distribution for the 'amount' column in the synthetic financial dataset. We create a new feature, 'benford_deviation,' which measures the deviation of each transaction's first digit from the most common first digit according to Benford's Law.

Deep learning model with this new feature and the original features as input to the program

```
import numpy as np import
pandas as pd
from sklearn.model_selection import train_test_split from
sklearn.preprocessing import StandardScaler from
sklearn.metrics import classification_report,
confusion_matrix
from keras.models import Sequential from
keras.layers import Dense
from keras.optimizers import Adam

def benfords_law_first_digit(data):
    first_digits = data.astype(str).str[0].astype(int)
      first_digit_distribution =
first_digits.value_counts(normalize=True).sort_index()
    return first_digit_distribution

# Load synthetic financial dataset
data = pd.read_csv('synthetic_financial_data.csv')

# Calculate Benford's Law first-digit distribution
first_digit_distribution=
benfords_law_first_digit(data['amount'])

        # Add deviation from Benford's Law as a new feature
        data['benford_deviation']= data['amount'].apply(lambda
                                        x:abs(int(str(x)[0]) -
first_digit_distribution.idxmax()))

# Split data into features (X) and target (y) X =
data.drop(columns=['is_fraud'])
y = data['is_fraud']

# Split the data into train and test sets
    X_train, X_test, y_train, y_test = train_test_split(X, y,
test_size=0.2, random_state=42)


# Print classification report and confusion matrix
print(classification_report(y_test, y_pred))
print(confusion_matrix(y_test, y_pred))
```

7.2. Creation of a Real-Time Fraud Detection System using Benford's Law and an AI Algorithm

Step 1 - Install necessary libraries:

```
pip install pandas numpy scikit-learn
```

Step2- Create a Python script. real_time_fraud_detection.py.

```
import numpy as np import pandas as pd import time
from sklearn.ensemble import
RandomForestClassifier
from sklearn.model_selection import train_test_split from
sklearn.preprocessing import StandardScaler from
sklearn.metrics import classification_report,
confusion_matrix

def benfords_law_first_digit(data):
    first_digits = data.astype(str).str[0].astype(int)
      first_digit_distribution
    = first_digits.value_counts(normalize=True).sort_index()
    return first_digit_distribution       # Scale the feature data
scaler = StandardScaler()
              X_train = scaler.fit_transform(X_train) X_test
              = scaler.transform(X_test)

              # Define the deep learning model model =
              Sequential()
              model.add(Dense(32,
                                    input_dim=X_train.sha
          pe[1], activation='relu'))
              model.add(Dense(16, activation='relu'))
              model.add(Dense(1, activation='sigmoid'))
```

```
    # Compile the model optimizer =
    Adam(lr=0.001)
    model.compile(loss='binary_crossentropy',
optimizer=optimizer, metrics=['accuracy'])

    # Train the model
    model.fit(X_train, y_train, epochs=100,
    batch_size=32, verbose=0)

    # Evaluate the model on the test set y_pred =
    model.predict_classes(X_test)
    def preprocess_data(data,
    first_digit_distribution, scaler=None):
  data['benford_deviation']=
data['amount'].apply(lambda x: abs(int(str(x)[0]) -
first_digit_distribution.idxmax()))

      if scaler is None:
        scaler = StandardScaler()
        scaler.fit(data)

      data_scaled = scaler.transform(data)
      return data_scaled, scaler

  # Load historical financial dataset
  data = pd.read_csv('historical_financial_data.csv')

  # Calculate Benford's Law first-digit distribution
  first_digit_distribution=
benfords_law_first_digit(data['amount'])

  # Split data into features (X) and target (y) X =
  data.drop(columns=['is_fraud'])
  y = data['is_fraud']# Split the data into train and
  test sets
    X_train, X_test, y_train, y_test =
train_test_split(X, y, test_size=0.2,
random_state=42)

    # Preprocess the training data
    X_train,      scaler      =
                  preprocess_data(X_train,
first_digit_distribution)

    # Train a Random Forest classifier
    clf =
    RandomForestClassifier(n_estimators=100)
    clf.fit(X_train, y_train)

    # Continuously process new transactions in
    real-time while True:
      # Fetch new transaction data from the
database (replace with actual database query)
new_transactions=
pd.read_csv('new_transactions.csv')

      # Preprocess the new transaction data
new_transactions_scaled,      _=
preprocess_data(new_transactions,
first_digit_distribution, scaler)

      # Predict the likelihood of fraud for the
new transactions
fraud_predictions=
clf.predict(new_transactions_scaled)

      # Save or output the fraud predictions
(e.g., to a database or alerting system)
      print("Fraud predictions:", fraud_predictions)

      # Wait for some time before fetching the next
batch of transactions
      time.sleep(60)
```

8. Optimizing Fraud Detection: Feature Engineering and Evaluation Metrics, and Addressing Imbalanced Data

8.1. Feature Selection and Dimensionality Reduction

Feature selection and dimensionality reduction play a critical role in preprocessing fraud detection steps to remove irrelevant or redundant features and improve model performance [47]. It involves the creation of new features or transforming existing features to improve their usefulness for machine learning models, which may include techniques such as scaling, normalization, encoding, and aggregation [48]. Feature selection techniques can be divided into filter methods, wrapper methods, and embedded methods [49]. Filter methods, such as correlation-based feature selection, evaluate features individually based on their relevance to the target variable, while wrapper methods, like recursive feature elimination, evaluate feature subsets based on the performance of a specific classifier [50]. Embedded methods, such as LASSO, perform feature selection during the learning process by incorporating feature selection into the optimization process [51].

Dimensionality reduction techniques, such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), can be employed to transform the original feature space into a lower-dimensional space while preserving the essential information for classification [47]. Dimensionality reduction can help improve model performance by reducing noise, computational complexity, and the risk of overfitting [48].

8.2. Evaluation Metrics for Fraud Detection

Evaluating the performance of fraud detection models is crucial to ensure their effectiveness and reliability. Common evaluation metrics used in fraud detection include accuracy, precision, recall, F1-score, and the area under the Receiver Operating Characteristic (ROC) curve (AUC-

ROC) [54]. Since fraud is often an imbalanced classification problem, with fraudulent cases being the minority class, metrics like precision, recall, and F1-score are preferred over accuracy, as they are less sensitive to class imbalance [55]. AUC-ROC provides a comprehensive measure of a model's performance, considering both true positive and false positive rates [54].

Precision measures the proportion of true positive cases among the predicted positive cases, while recall (sensitivity) measures the proportion of true positive cases among the actual positive cases [57]. F1-score is the harmonic mean of precision and recall, providing a single metric that balances both [58]. AUC-ROC represents the trade-off between true and false positive rates, with higher AUC-ROC values indicating better model performance [54]. These evaluation metrics provide a more comprehensive understanding of a model's performance detecting fraud in imbalanced datasets.

8.3. Addressing Imbalanced Data - Imbalanced Data and Sampling Techniques

Imbalanced datasets are common in fraud detection, where the number of fraudulent cases is typically much smaller than the number of non-fraudulent ones [60]. This imbalance can cause classifiers to become biased toward the majority class, leading to poor performance in detecting the minority class (fraudulent cases) [61]. Various sampling techniques can be applied to address the class imbalance, including oversampling the minority class, undersampling the majority class, or employing a combination of both [62]. Alternatively, cost-sensitive learning approaches can be employed, which assign different misclassification costs to each class to encourage the classifier to focus on the minority class [63].

Oversampling techniques, such as the Synthetic Minority Over-sampling Technique (SMOTE), create synthetic instances of the minority class to balance the class distribution [64]. Undersampling techniques, like the Random Under-Sampling (RUS) method, remove majority class instances to balance the class distribution [65]. Combining oversampling and undersampling, such as the Adaptive Synthetic (ADASYN) approach, adaptively generates synthetic instances for the minority class based on the density distribution of the original data [66]. While these techniques can improve model performance on imbalanced data, they may introduce new challenges, such as increased computational complexity or overfitting [67].

8.4. Imbalanced Data Handling Techniques

Apart from sampling techniques, other methods can be employed to handle imbalanced data in fraud detection, including the use of advanced machine learning algorithms, ensemble methods, and evaluation metric optimization [68].

8.5. Advanced Machine Learning Algorithms

Some machine learning algorithms, such as Support Vector Machines (SVM) and decision trees, have built-in mechanisms to handle class imbalance [61]. For instance, SVM can utilize class weights to balance the classes during training, while decision trees can employ class-specific splitting criteria [70]. These algorithms may provide better performance on imbalanced datasets without the need for additional preprocessing steps.

8.6. Ensemble Methods

Ensemble techniques, such as bagging, boosting, and stacking, can improve the performance of individual classifiers on imbalanced data [71]. Bagging, which creates multiple classifiers based on random subsets of the dataset, can reduce overfitting and improve the classifier's stability [72]. Boosting, a method that sequentially trains classifiers with an emphasis on the misclassified instances from previous iterations, can enhance the performance of weak classifiers [73].

Stacking combines the predictions of multiple classifiers to form a final prediction, often yielding better results than individual classifiers [74]. These ensemble methods can be further customized to address the class imbalance by employing different sampling techniques or class weighting schemes during the training process [54].

8.7. Evaluation Metric Optimization

Optimizing the evaluation metrics less sensitive to class imbalance, such as F1-score, balanced accuracy, or AUC-ROC, can help improve the performance of fraud detection models on imbalanced data [76]. By focusing on these metrics during the model development process, classifiers can be better tailored to handle the specific challenges of imbalanced datasets, ensuring their effectiveness in detecting fraudulent cases [77].

9. Ethical Considerations of Utilizing AI/ ML in Forensic Accounting

Utilizing AI and ML in forensic accounting brings significant benefits, including improved efficiency and accuracy in fraud detection. However, integrating these technologies also raises ethical considerations that need to be addressed. Some of the key ethical concerns include the following:

9.1. Bias and Fairness

AI and ML models are only as good as the data they are trained on [83]. The resulting model may make biased or unfair decisions if the training data contains biases or inaccuracies. Ensuring that the data used for training and validation is representative and unbiased is essential to prevent discrimination and maintain fairness in fraud detection [84].

9.2. Transparency and Explainability

AI and ML models, particularly deep learning models, can be complex and difficult to interpret [85]. This lack of transparency and explainability may hinder the ability of forensic accountants, auditors, and regulators to understand the rationale behind a model's decisions. Developing accurate and explainable models is crucial for maintaining trust and ensuring stakeholders can assess the validity of the model's output [86].

9.3. Accountability and Responsibility

As AI and ML systems become more autonomous, it can be challenging to determine who should be held accountable for the system's actions or decisions [87]. Clear guidelines should be established regarding the responsibility of developers, users, and organizations in the event of incorrect or unethical decisions made by the AI/ML system.

9.4. Overreliance on Technology

The increased use of AI and ML in forensic accounting may lead to an overreliance on technology and a potential loss of human expertise [88]. It is essential to balance human expertise and AI/ML systems, ensuring that forensic accountants continue developing and maintaining their skills and critical thinking abilities.

9.5. Legal and Regulatory Compliance

AI and ML in forensic accounting must comply with relevant laws and regulations, such as data protection laws and financial reporting standards [89]. Ensuring the technologies are legally compliant is crucial for maintaining trust in the system and preventing potential legal issues.

9.6. Ethical use of AI/ML Predictions

The predictions made by AI/ML models should be used ethically and responsibly [90]. For example, organizations must only use predictions to unfairly target individuals or entities with a proper investigation. Decisions based on AI/ML predictions should be supported by evidence and follow established procedures to ensure fairness and due process.

10. AI and Machine Learning in Action: Improving Fraud Detection for Major Financial Institutions

10.1. JPMorgan Chase's COIN (Contract Intelligence)

JPMorgan Chase implemented a machine learning system called COIN to analyze legal documents, such as loan agreements, and identify potential fraud, errors, or inconsistencies [78]. This system has helped reduce the time spent on document review by 360,000 hours per year, increasing efficiency and reducing the likelihood of human errors [78].

10.2. PayPal's Fraud Detection System

PayPal, a leading global online payment platform, uses machine learning algorithms to detect and prevent fraudulent transactions [79]. The company's system analyzes over 25 million transactions daily, identifying patterns and anomalies that may indicate fraud [79]. By utilizing AI and ML, PayPal has managed to reduce its false positive rate by 50% and improve the accuracy of its fraud detection efforts [79].

10.3. Mastercard's Decision Intelligence

Mastercard implemented an AI-driven platform called Decision Intelligence to analyze transaction data and detect fraudulent activities [80]. This platform uses machine learning algorithms to assess various factors, such as spending habits and transaction history, to determine the likelihood of a transaction being fraudulent. As a result, Mastercard has reported a 50% reduction in false declines and a 10% increase in overall customer satisfaction [80].

10.4.HSBC's Anti-Money Laundering (AML) System

HSBC, a multinational banking and financial services company, uses AI and ML algorithms to detect and prevent money laundering activities [81]. Their system analyzes large volumes of transaction data, equivalent to 1.2 trillion searches per year, to identify patterns and trends that may indicate money laundering [81]. By leveraging AI and ML, HSBC has improved the efficiency and accuracy of its AML efforts, leading to the identification of 20% more suspicious activities [81].

10.5. American Express's Fraud Detection System

American Express, a leading global financial services provider, uses AI and ML algorithms to analyze transaction data and identify potentially fraudulent activities [82]. Their system assesses various factors, such as spending patterns and customer behavior, to determine the likelihood of fraud. This AI-driven approach has enabled American Express to reduce false positives by 30% and improve the overall effectiveness of its fraud detection efforts, with a 70% increase in fraud detection accuracy [82].

11. Potential Future Developments

As AI/ML technologies continue to advance, their integration into forensic accounting is expected to lead to further improvements in fraud detection and prevention [91]. The future prospects of AI and ML in forensic accounting appear promising as technology continues to evolve and improve. With further advancements in AI and ML, forensic accounting will likely benefit from enhanced capabilities, leading to more efficient and accurate fraud detection and financial analysis.

Some of the future prospects for AI and ML in forensic accounting include the following:

11.1. Reinforcement Learning

Reinforcement learning (RL) is a type of ML where an agent learns to make decisions by interacting with its environment and receiving feedback in the form of rewards or penalties [104]. RL has shown potential in various domains, such as robotics, game-playing, and recommendation systems [105]. Applying RL to forensic accounting could enable adaptive and interactive fraud detection systems that continuously learn and update their strategies in response to changes in the financial environment [106].

11.2. Transfer Learning

Transfer learning is a technique in which a pre-trained model is fine-tuned for a new, related task [107]. Transfer learning can save time and computational resources by leveraging knowledge gained from previous tasks, particularly useful when training data is limited or expensive to obtain [108]. In the context of forensic accounting, transfer learning could help improve the performance of ML models by leveraging knowledge from related financial domains or industries [109].

11.3. Federated Learning

Federated learning is a distributed approach to ML that allows multiple organizations to collaboratively train a shared model while keeping their data locally [110]. This approach can help address privacy concerns and data-sharing restrictions in forensic accounting by allowing different financial institutions to collaborate on fraud detection without compromising sensitive data [111]. Federated learning can also help improve the generalizability of ML models by incorporating diverse and representative data from multiple sources [112].

11.4. Explainable AI

Explainable AI (XAI) aims to make ML models more transparent and understandable by providing explanations for their predictions [113]. In forensic accounting, explainability is crucial for gaining the trust of stakeholders, regulators, and auditors and for supporting decision-making processes [114]. Future research could focus on developing XAI techniques tailored to forensic accounting applications' specific challenges and requirements, such as providing evidence for legal proceedings or helping auditors identify the root causes of financial fraud [115].

11.5. More Proactive Fraud Detection

AI and ML can help shift forensic accounting from reactive to proactive by predicting and preventing potential fraud before it occurs [98]. By analyzing historical data and detecting patterns, AI and ML algorithms can predict the likelihood of fraud in specific scenarios, enabling organizations to implement preventive measures [99].

11.6. Enhanced Data Analysis and Visualization

The use of AI and ML can lead to more advanced data analysis and visualization techniques in forensic accounting, helping forensic accountants better understand complex financial data and identify patterns, trends, and anomalies [97].

11.7. Improved AI and ML Algorithms

As AI and ML research continues, new and improved algorithms will be developed to detect better and analyze financial irregularities. These advanced algorithms may offer higher accuracy, better generalization, and improved interpretability, further enhancing their usefulness in forensic accounting [92].

11.8. Automated and Continuous Auditing

Integrating AI and ML into the auditing process can enable continuous and automatic auditing, allowing for real-time financial irregularities and fraud detection [95]. This can significantly improve the efficiency of audits and reduce the risk of undetected fraud [96].

11.9. Personalized Learning and Training

AI and ML can be used to create personalized learning and training programs for forensic accountants, helping them develop the necessary skills and knowledge more efficiently [100]. These personalized programs can adapt to individual learning styles and preferences, improving the effectiveness of training and education in the field [101].

11.10. AI-Driven Decision Support Systems

Integrating AI and ML in decision support systems can provide forensic accountants with real-time, data-driven insights to support their decision-making processes [102]. These systems can help forensic accountants make more informed decisions, improving the overall effectiveness of their investigations and analysis [103].

11.11. Integration with Other Emerging Technologies

Combining AI and ML with other emerging technologies, such as blockchain, big data, and the Internet of Things (IoT), can lead to innovative solutions for fraud detection and financial analysis [93]. For example, integrating AI with blockchain can provide enhanced traceability and transparency in financial transactions, making detecting anomalies and potential fraud easier [94].

12. Conclusion

AI and ML techniques have shown great potential in forensic accounting for detecting various types of financial fraud, including anti-money laundering, internal fraud, insurance claims fraud, credit card fraud, tax evasion, bankruptcy and insolvency analysis, and audit support [116].

Supervised learning algorithms, such as logistic regression, decision trees, support vector machines, and ensemble methods, have been widely used for fraud detection [117]. Unsupervised learning techniques, including clustering algorithms and anomaly detection methods, are also applied to identify suspicious activities [118].

Deep learning approaches, such as neural networks, autoencoders, and recurrent neural networks, have emerged as promising techniques for handling large and complex datasets in forensic accounting [119]. The choice of features, data preprocessing, and handling class imbalance are essential aspects of developing effective fraud detection models [120]. Finally, appropriate evaluation metrics, including precision, recall, F1-score, and AUC-ROC, are critical for assessing the performance of fraud detection models, particularly when dealing with imbalanced datasets [121].

As AI and ML continue to advance, these techniques are expected to play an increasingly important role in forensic accounting, improving the efficiency and effectiveness of fraud detection and prevention efforts [122]. Future research could focus on developing more sophisticated models, incorporating advanced AI techniques and domain-specific knowledge to enhance the performance of fraud detection systems [123]. Additionally, addressing challenges such as data privacy and security and the interpretability of complex models will be essential for successfully deploying AI and ML solutions in forensic accounting [124].

References

[1] Carlene Beth Wynter, and Lynne Oats, "Don't Worry, We are not After You! Anancy Culture and Tax Enforcement in Jamaica," *Critical Perspectives on Accounting*, vol. 57, pp. 56-69, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] James A. DiGabriele, and Marianne Ojo, "Objectivity and Independence: The Dual Roles of External Auditors," *Journal of Forensic & Investigative Accounting*, vol. 6, no. 2, pp. 200-224, 2014. [Google Scholar] [Publisher Link]

[3] Deniz Appelbaum et al., "Impact of Business Analytics and Enterprise Systems on Managerial Accounting," *International Journal of Accounting Information Systems*, vol. 25, pp. 29-44, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Federico Berruti, Emily Ross, and Allen Weinberg, "The Transformative Power of Automation in Banking," *McKinsey & Company*, 2017. [Google Scholar] [Publisher Link]

[5] Y. Hou, S. Li, and M. Xia, "Forensic Accounting and Fraud Detection Using Artificial Intelligence Techniques," *Journal of Forensic Accounting Research*, vol. 3, no. 1, pp. A45-A64, 2018.

[6] Josh Baker, "*Using Machine Learning to Detect Financial Statement Fraud*," *Business: Student Scholarship & Creative Works*, 2019. [Google Scholar] [Publisher Link]

[7] Xiao Ding et al., "Deep Learning for Event-Driven Stock Prediction," *Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence*, pp. 2327-2333, 2015. [Google Scholar] [Publisher Link]

[8] Sepp Hochreiter, and Jürgen Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735-1780, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[9] Brett Lantz, *Machine Learning with R*, Packt Publishing Ltd., 2013. [Google Scholar] [Publisher Link]

[10] Richard J. Bolton, and David J. Hand, "Statistical Fraud Detection: A Review," *Statistical Science*, vol. 17, no. 3, pp. 235-249, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[11] J.R. Dorronsoro et al., "Neural Fraud Detection In Credit Card Operations," *IEEE Transactions on Neural Networks*, vol. 8, no. 4, pp. 827-834, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[12] Jarrod West, and Maumita Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," *Computers & Security*, vol. 57, pp. 47-66, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. B. Kotsiantis, "Supervised Machine Learning: A Review of Classification Techniques," *Emerging Artificial Intelligence Applications in Computer Engineering*, vol. 160, pp. 3-24, 2007. [Google Scholar] [Publisher Link]

[14] Mark J. Nigrini, *Benford's Law: Applications For Forensic Accounting, Auditing, And Fraud Detection*, John Wiley & Sons, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[15] Jack Dorminey et al., "The Evolution of Fraud Theory," *Issues in Accounting Education*, vol. 27, no. 2, pp. 555-579, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[16] T. H. Davenport, and R. Kalakota, "The Potential for Artificial Intelligence in Banking," *MIT Sloan Management Review*, vol. 60, no. 4, pp. 59-62, 2019. [Online]. Available: https://sloanreview.mit.edu/article/the-potential-for-artificial-intelligence-in-banking/

[17] J. Adler, F. Schirmacher, and N. Peluso, "Artificial Intelligence in Forensic Accounting: Opportunities and Risks," *Business Law Review*, vol. 43, no. 2, pp. 255–269, 2019.

[18] Efstathios Kirkos, Charalambos Spathis, and Yannis Manolopoulos, "Data Mining Techniques for the Detection of Fraudulent Financial Statements," *Expert Systems with Applications*, vol. 32, no. 4, pp. 995-1003, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[19] Varun Chandola, Arindam Banerjee, and Vipin Kumar, "Anomaly Detection: a Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1-58, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[20] J. MacQueen, "Some Methods for Classification and Analysis of Multivariate Observations," *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*, pp. 281-297, 1967. [Google Scholar] [Publisher Link]

[21] Larry M. Manevitz, and Malik Yousef, "One-Class SVMs for Document Classification," *Journal of Machine Learning Research*, vol. 2, pp. 139-154, 2001. [Google Scholar] [Publisher Link]

[22] Xiaojin Jerry Zhu, "*Semi-Supervised Learning Literature Survey*," University of Wisconsin-Madison Department of Computer Sciences, vol. 1530, no. 3, 2005. [Google Scholar] [Publisher Link]

[23] Olivier Chapelle, Bernhard Schölkopf, and Alexander Zien, "Semi-Supervised Learning," MITPress, 2006. [Publisher Link]

[24] Yoshua Bengio, and Yann LeCun, "Scaling Learning Algorithms Towards Ai," *Large-Scale Kernel Machines*, vol. 34, no. 5, pp. 1-41, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[25] Richard S. Sutton, and Andrew G. Barto, *Reinforcement Learning: An Introduction*, *MIT Press*, vol. 1, no.1, 1998. [Google Scholar] [Publisher Link]

[26] F. H. Tseng et al., "Dynamic Credit Card Fraud Detection Using Reinforcement Learning," *International Conference on Information Security and Cryptology*, Springer, pp 174-188, 2009.

[27] S. M. Thennakoon, R. K. Y. Li, and K. C. C. Chan, "A Hybrid Approach to Financial Fraud Detection: Integrating Statistical Methods with Machine Learning Techniques," *Journal of Risk Management in Financial Institutions*, vol. 13, no. 1, pp. 68-87, 2020.

[28] Abhinav Srivastava et al., "Credit Card Fraud Detection Using Hidden Markov Model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37-48, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[29] Fawaz Mahiuob Mohammed Mokbal et al., "XGBXSS: An Extreme Gradient Boosting Detection Framework for Cross-Site Scripting Attacks Based on Hybrid Feature Selection Approach and Parameters Optimization," *Journal of Information Security and Applications*, vol. 58, p. 102813, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] K. Singh, P. Best, and C. Cheong, "Developing a Forensic Accounting Curriculum: A Case Study Using the Backward Design Process," *Journal of Education for Business*, vol. 93, no. 8, pp. 374-385, 2018.

[31] P. Ravisankar et al., "Detection of Financial Statement Fraud and Feature Selection using Data Mining Techniques," *Decision Support Systems*, vol. 50, no. 2, pp. 491-500, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[32] Fabrizio Sebastiani, "Machine Learning in Automated Text Categorization," *ACM Computing Surveys*, vol. 34, no. 1, pp. 1-47, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[33] Luis Perez, and Jason Wang, "The Effectiveness of Data Augmentation in Image Classification Using Deep Learning," *arXiv preprint arXiv:1712.04621*, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[34] Bing Liu, "Sentiment Analysis and Opinion Mining," *Synthesis Lectures on Human Language Technologies*, vol. 5, no. 1, pp. 1-167. 2012. [Publisher Link]

[35] David M. Blei, Andrew Y. Ng, and Michael I. Jordan, "Latent Dirichlet Allocation," *Journal of Machine Learning Research*, vol. 3, pp. 993-1022, 2003. [Google Scholar] [Publisher Link]

[36] Tim Loughran, and Bill Mcdonald, "When is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-ks," *The Journal of Finance*, vol. 66, no. 1, pp. 35-65, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[37] David Nadeau, and Satoshi Sekine, "A Survey of Named Entity Recognition and Classification," *Lingvisticae Investigationes*, vol. 30, no. 1, no. 3-26. 2007. [CrossRef] [Google Scholar] [Publisher Link]

[38] Jiwei Li, Alan Ritter, and Eduard Hovy, "Weakly Supervised User Profile Extraction From Twitter," *Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics*, vol. 1, pp. 165-174, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[39] J.R. Dorronsoro et al., "Neural Fraud Detection In Credit Card Operations," *IEEE Transactions on Neural Networks*, vol. 8, no. 4, pp. 827-834, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[40] Y. Cao et al., "Deep Learning for Fraud Detection in the Financial Industry: A Systematic Literature Review," *Information Processing & Management*, vol. 57, no. 5, 2020.

[41] Indranil Bose, and Radha K. Mahapatra, "Business Data Mining - A Machine Learning Perspective," *Information & Management*, vol. 39, no. 3, pp. 211-225, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[42] W. Chen, and P. Y. Chau, "Using Neural Networks in the Analysis of Financial Health of Companies," *37th Annual Hawaii International Conference on System Sciences*, 2004.

[43] David E. Rumelhart, Geoffrey E. Hinton, and Ronald J. Williams, "Learning Representations By Back-Propagating Errors," *Nature*, vol. 323, no. 6088, pp. 533-536, 1986. [CrossRef] [Google Scholar] [Publisher Link]

[44] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436-444, 2015. [Google Scholar] [Publisher Link]

[45] Donald R. Cressey, "Other People's Money: A Study in the Social Psychology of Embezzlement," Patterson Smith, 1953. [Google Scholar] [Publisher Link]

[46] M. Chui et al., "The Future of Forensic Accounting: A Framework for Integrating Artificial Intelligence and Machine Learning," vol. 6, no. 1, pp. 1-35, 2021.
[47] Karl Pearson, "On Lines and Planes of Closest Fit to Systems of Points in Space," *Philosophical Magazine*, vol. 2, no. 11, pp. 559–572, 1901. [CrossRef] [Google Scholar] [Publisher Link]
[48] R. A. Fisher, "The Use of Multiple Measurements in Taxonomic Problems," *Annals of Eugenics*, vol. 7, no. 2, pp. 179–188, 1936. [CrossRef] [Google Scholar] [Publisher Link]
[49] Isabelle Guyon and Andre Elisseeff, "An Introduction to Variable and Feature Selection," *Journal of Machine Learning Research*, vol. 3, no. 3, pp. 1157–1182, 2003. [Google Scholar] [Publisher Link]
[50] Ron Kohavi, and George H. John, "Wrappers for Feature Subset Selection," *Artificial Intelligence*, vol. 97, no. 1-2, pp. 273–324, 1997. [CrossRef] [Google Scholar] [Publisher Link]
[51] Robert Tibshirani, "Regression Shrinkage and Selection via the Lasso," *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 58, no. 1, pp. 267–288, 1996. [CrossRef] [Google Scholar] [Publisher Link]
[52] M. Richey, J. Morgan, and S. Li, "Ethical Artificial Intelligence for Fraud Prevention in Finance and Accounting," *Ethics in Information Technology*, vol. 22, no. 2, pp. 175–193, 2022.
[53] J. Zhang, A. Khan, and Q. Wu, "Deep Learning Models for Fraud Detection in Financial Statements," *Proceedings under International Conference on Acoustics, Speech, and Signal Processing*, pp. 2760-2764, 2021.
[54] Tom Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006. [CrossRef] [Google Scholar] [Publisher Link]
[55] Christopher M. Bishop, *Pattern Recognition and Machine Learning*, *Springer*, 2006. [Google Scholar] [Publisher Link]
[56] Tom Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006. [CrossRef] [Google Scholar] [Publisher Link]
[57] S. B. Kotsiantis, I. D. Zaharakis, and P. E. Pintelas, "Machine Learning: A Review of Classification and Combining Techniques," *Artificial Intelligence Review*, vol. 26, no. 3, pp. 159–190, 2006. [CrossRef] [Google Scholar] [Publisher Link]
[58] C. J. Van Rijsbergen, *Information Retrieval*, 2nd Edition, Butterworth- Heinemann, 1979. [Publisher Link]
[59] Tom Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006. [CrossRef] [Google Scholar] [Publisher Link]
[60] N. V. Chawla et al., "SMOTE: Synthetic Minority Over-sampling Technique," *Journal of Artificial Intelligence Research*, vol. 16, no. 1, pp. 321–357, 2002. [CrossRef] [Google Scholar] [Publisher Link]
[61] Gustavo E. A. P. A. Batista, Ronaldo C. Prati, and Maria Carolina Monard, "A Study of the Behavior of Several Methods for Balancing Machine Learning Training Data," *ACM SIGKDD Explorations Newsletter*, vol. 6, no. 1, pp. 20–29, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[62] Haibo He, and Edwardo A. Garcia, "Learning from Imbalanced Data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 9, pp. 1263–1284, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[63] Z. Zhang, and M. Savvides, "Addressing Class Imbalance in Face Recognition: A Review," *Artificial Intelligence Review*, vol. 53, no. 2, pp. 993–1021, 2020.
[64] Charles Elkan, "The Foundations of Cost-Sensitive Learning," *Proceedings of the 17th International Joint Conference on Artificial Intelligence*, Seattle, WA, USA, pp. 973–978, 2001. [Google Scholar] [Publisher Link]
[65] Hui Han, Wen-Yuan Wang, and Bing-Huan Mao, "Borderline-SMOTE: A New Over-Sampling Method in Imbalanced Data Sets Learning," *Proceedings of the 2005 International Conference on Advances in Intelligent Computing*, Hefei, China, pp. 878–887, 2005. [CrossRef] [Google Scholar] [Publisher Link]
[66] S. Y. Seo, G. S. Jo, and S. H. Ha, "Random Under-Sampling Integrated with SMOTE for Imbalanced Data Classification," *Proceedings of the 2016 International Conference on Information and Communication Technology Convergence*, Jeju, South Korea, pp. 511– 513, 2016.
[67] Haibo He et al., "ADASYN: Adaptive Synthetic Sampling Approach for Imbalanced Learning," *Proceedings of the 2008 IEEE International Joint Conference on Neural Networks*, Hong Kong, China, 2008, pp. 1322–1328, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[68] Andrew Estabrooks, Taeho Jo, and Nathalie Japkowicz "A Multiple Resampling Method for Learning from Imbalanced Data Sets," *Computational Intelligence*, vol. 20, no. 1, pp. 18–36, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[69] Gustavo Enrique A P A Batista, Ronaldo Cristiano Prati, and Maria Carolina Monard, "A Study of the Behavior of Several Methods for Balancing Machine Learning Training Data," *ACM SIGKDD Explorations Newsletter*, vol. 6, no. 1, pp. 20–29, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[70] Provost, and Foster, "Machine Learning from Imbalanced Data Sets 101," *Proceedings of the AAAI 2000 Workshop on Imbalanced Data Sets*, Austin, Texas, pp. 1–3, 2000. [Google Scholar] [Publisher Link]

[71] Nitesh Vijay Chawla, Nathalie Japkowicz, and Aleksander R Kołcz, "Editorial: Special Issue on Learning from Imbalanced Data Sets," *ACM SIGKDD Explorations Newsletter*, vol. 6, no. 1, pp. 1–6, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[72] Xu-Ying Liu, Jianxin Wu, and Zhi-Hua Zhou, "Exploratory Undersampling for Class-Imbalance Learning," *IEEE Transactions on Systems, Man, and Cybernetics*, Part B (Cybernetics), vol. 39, no. 2, pp. 539–550, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[73] G. Wu, and E. Y. Chang, "KBA: Kernel Boundary Alignment Considering Imbalanced Data Distribution," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, pp. 786–795, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[74] K. M. Ting, *Encyclopedia of Machine Learning*, Claude Sammut, and Geoffrey I. Webb, Eds. Boston, MA: Springer, pp. 781–781, 2010. [Publisher Link]

[75] Tom Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[76] John A. Swets, "Measuring the Accuracy of Diagnostic Systems," *Science*, vol. 240, no. 4857, pp. 1285–1293, 1988. [CrossRef] [Google Scholar] [Publisher Link]

[77] C. D. Manning, P. Raghavan, and H. Schütze, *Introduction to Information Retrieval*, New York, NY: Cambridge University Press, 2008. [Google Scholar] [Publisher Link]

[78] Hugh Son, JPMorgan Marshals an Army of Developers to Automate High Finance, *Bloomberg*, 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance

[79] P. Lemieux, How PayPal Boosts Security with Artificial Intelligence, MIT Technology Review, 2018. [Online]. Available: https://www.technologyreview.com/2018/11/15/139164/how-paypal-boosts-security-with-artificial-intelligence/

[80] Mastercard, Mastercard Rolls Out Artificial Intelligence Across Its Global Network, 2016. [Online]. Available: https://newsroom.mastercard.com/press-releases/mastercard-rolls-out-artificial-intelligence-across-its-global-network

[81] HSBC, HSBC to Use AI to Detect Money Laundering, 2017. [Online]. Available: https://www.hsbc.com/news-and-insight/2017/hsbc-to-use-ai-to-detect-money-laundering

[82] T. H. Davenport, and R. Kalakota, The Potential for Artificial Intelligence in Banking, MIT Sloan Management Review, 2019. [Online]. Available: https://sloanreview.mit.edu/article/the-potential-for-artificial-intelligence-in-banking/

[83] S. Barocas, and A. D. Selbst, Big Data's Disparate Impact, *California Law Review*, vol. 104, no. 3, pp. 671-732, 2016. [Online]. Available: https://www.californialawreview.org/printarticle/big-datas-disparate-impact/

[84] Indre Zliobaite, "On the Relation Between Accuracy and Fairness in Binary Classification," *Future of Computing & Informatics Journal*, vol. 1, no. 1, pp. 45-54, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[85] Davide Castelvecchi, “Can We Open the Black Box of AI?,” *Nature*, vol. 538, no. 7623, pp. 20-23, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[86] Alejandro Barredo Arrieta et al., "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI," *Information Fusion*, vol. 58, pp. 82-115, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[87] Brent Daniel Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society*, vol. 3, no. 2, pp. 1-21. 2016. [CrossRef] [Google Scholar] [Publisher Link]

[88] Thomas H. Davenport, and Julia Kirby, Just How Smart are Smart Machines?, *MIT Sloan Management Review*, vol. 57, no.3, pp. 21-25, 2016. [Online]. Available: https://sloanreview.mit.edu/article/just-how-smart-are-smart-machines/

[89] Lee A. Bygrave, "Data Protection by Design and by Default: Deciphering the Eu's Legislative Requirements," *Oslo Law Review*, vol. 6, no. 1, pp. 105-120. 2019. [CrossRef] [Google Scholar] [Publisher Link]

[90] S. Moral et al., "An Ethical Framework for the Digital Afterlife Industry," *Science and Engineering Ethics*, vol. 24, no. 4, pp. 1219-1242, 2018.

[91] Cohen, and M. Zimbelman, "Forensic Accounting and Fraud Detection: The Role of Artificial Intelligence and Machine Learning," *Journal of Forensic Accounting Research*, vol. 7, no. 2, pp. 123-136, 2014.

[92] Stuart J. Russell, and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th Edition, Pearson, 2020. [Google Scholar] [Publisher Link]

[93] K. N. K. R. Babu, "Emerging Technologies for Forensic Accounting: A Review," *International Journal of Accounting and Financial Reporting*, vol. 9, no. 1, pp. 134-145, 2019.

[94] Philip Treleaven, Richard Gendal Brown, and Danny Yang, "Blockchain Technology in Finance," *Computer*, vol. 50, no. 9, pp. 14-17, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[95] M. Alles, "Continuous Auditing and Reporting Systems: Implications for Assurance and Decision Making," *International Journal of Accounting Information Systems*, vol. 30, pp. 1-18, 2019.

[96] M. Vasarhelyi, and F. B. Roman, "Continuous Auditing in the Twenty- First Century: Lessons from Three Decades of Research and Practice," *Advances in Accounting*, vol. 47, p. 100420, 2019.

[97] R. E. Severson, "Data Analysis and Visualization for Forensic Accounting," *Handbook of Forensic Accounting*, M. K. Badawy, Ed. Wiley, pp. 317-332, 2021.

[98] S. Bhattacharya, S. Sengupta, and S. Saha, *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques*, 1st ed. Wiley, 2015, pp. 167-186.
[99] M. K. Badawy, *Fraud Detection and Prevention*, Handbook of Forensic Accounting, M. K. Badawy, Ed. Wiley, pp. 57-76, 2021.
[100] D. L. Silver, "Personalized Learning and Training with Machine Learning," *Proceedings of the 24th Annual ACM Symposium on Applied Computing*, pp. 45-49, 2009.
[101] M. Reigeluth, *Instructional-Design Theories and Models*, Volume IV: The Learner-Centered Paradigm of Education, 2017.
[102] Carr-Chellman, Eds. Routledge, pp. 49-64, 2017.
[103] G. Wang et al., "Decision Support Systems Driven by Machine Learning," *Decision Support Systems*, vol. 124, pp. 113078, 2019.
[104] Richard J. Boltonm, and David J. Hand, "Statistical Fraud Detection: A Review," *Statistical Science*, vol. 17, no. 3, pp. 235-255, 2002. [CrossRef] [Google Scholar] [Publisher Link]
[105] Richard S. Sutton, and Andrew G. Barto, *Reinforcement Learning: An Introduction*, 2nd Edition, MIT Press, 2018. [Google Scholar] [Publisher Link]
[106] Volodymyr Mnih et al., "Human-Level Control through Deep Reinforcement Learning," *Nature*, vol. 518, no. 7540, pp. 529-533, 2015. [Google Scholar] [Publisher Link]
[107] J. X. Chen et al., "Adaptive Fraud Detection Using Reinforcement Learning in Forensic Accounting," *Proceedings of the 29th International Conference on Computational Intelligence and Software Engineering*, pp. 315-320, 2020.
[108] Sinno Jialin Pan and Qiang Yang, "A Survey on Transfer Learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 10, pp. 1345-1359, 2010. [CrossRef] [Google Scholar] [Publisher Link]
[109] Rie Kubota Ando, and Tong Zhang, "A Framework for Learning Predictive Structures from Multiple Tasks and Unlabeled Data," *Journal of Machine Learning Research*, vol. 6, pp. 1817-1853, 2005. [Google Scholar] [Publisher Link]
[110] Jeff Donahue et al., "DeCAF: A Deep Convolutional Activation Feature for Generic Visual Recognition," *Proceedings of the 31st International Conference on Machine Learning*, 2014, pp. 647- 655. [Google Scholar] [Publisher Link]
[111] H. Brendan McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 2017, pp. 1273- 1282. [Google Scholar] [Publisher Link]
[112] R. K. Chinthala, and M. V. N. A. Prasad, "Secure Federated Learning for Fraud Detection in Banking and Finance," *International Journal of Intelligent Systems and Applications*, vol. 12, no. 10, pp. 68-77, 2020.
[113] Qiang Yang et al., "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 12:1-12:19, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[114] David Gunning, and David W. Aha, "DARPA's Explainable Artificial Intelligence (XAI) Program," *AI Magazine*, vol. 40, no. 2, pp. 44-58, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[115] F. Pasquini, M. L. P. Sá, and A. de Barros, "Explainable Artificial Intelligence (XAI) in Forensic Accounting: A Review of the Literature and Future Directions," *Proceedings of the 8th International Conference on Information Systems and Technology Management*, pp. 117-128, 2021.
[116] Amina Adadi and Mohammed Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138-52160, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[117] W. Steve Albrecht, Chad Albrecht, and Conan C. Albrecht, "Current Trends in Fraud and Its Detection," *Information Security Journal: A Global Perspective*, vol. 16, no. 1, pp. 2-12, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[118] E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection," *Proceedings of the IEEE/IAFE Conference on Computational Intelligence for Financial Engineering*, pp. 220- 226.1997. [CrossRef] [Google Scholar] [Publisher Link]
[119] Varun Chandola, Arindam Banerjee, and Vipin Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1-58, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[120] Yoshua Bengio, Aaron Courville, and Pascsl Vincent, "Representation Learning: A Review and New Perspectives," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 8, pp. 1798-1828, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[121] N. V. Chawla et al., "SMOTE: Synthetic Minority Over-sampling Technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321-357, 2002. [CrossRef] [Google Scholar] [Publisher Link]
[122] M. Powers, "Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation," *Journal of Machine Learning Technologies*, vol. 2, no. 1, pp. 37-63, 2011. [CrossRef] [Google Scholar] [Publisher Link]
[123] Pratyusa K. Manadhata and Jeannette M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371-386, 2011. [CrossRef] [Google Scholar] [Publisher Link]
[124] Mark J. Nigrini, "Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations," *Wiley*, 2011. [Google Scholar] [Publisher Link]
[125] Fred H. Cate, "The Failure of Fair Information Practice Principles," *Consumer Protection in the Age of the Information Economy*, J. K. Winn, Ed. Ashgate, pp. 341-377, 2006. [Google Scholar] [Publisher Link]

[126] J. Lee, R. Singh, and T. Tan, "A Review of AI and Machine Learning Models for Financial Fraud Detection," *Proceedings of International Conference on Machine Learning Applications*, pp. 210-216, 2021.

[127] Kirkos, "Unsupervised Learning with Clustering Algorithms for Credit Card Fraud Detection," *Proceedings of IEEE Symposium Computational Intelligence in Cyber Security*, pp. 45-51, 2020.

[128] M. Hagenau, B. Hedrich, and J. Neumann, "Automated Detection of Procurement Fraud using Association Rule Mining," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1455-1465, 2019.

[129] R. Fuller, D. Pai, and R. Kumar, "Document Fraud Detection Using Linguistics and SVM," *Proceedings of IEEE Security and Privacy Workshops (SPW)*, pp. 182-188, 2020.