**Journal of Management and Informatics (JMI)**
**Vol. 4 No. 1 April 2025**
E-ISSN: 2961-7731; P-ISSN: 2961-7472, Pages 706-722
*Publication Link: https://jmi.stekom.ac.id/index.php/jmi/issue/view/10*

# Effectiveness and Reliability of Artificial Intelligence in Fraud Detection: A Mixed-Method Study on Financial Audit

Khasif Naseer*[1], Hakeem Nazeer Ahmed[1]
Email: naseerkh@usa.edu.pk; hakeemdook@usa.edu.pk
[1]*Computer Science Department, University of South Asia, Lahore, 54000, Pakistan*
*Corresponding Author

**Abstract**
*Financial statement fraud threatens investor trust at a substantial level in the present market conditions. AI technology, through data pattern analysis, helps financial auditing reach better results when detecting rumors along with anomalies and suspicious trends. This research evaluates artificial intelligence's effectiveness in yeast-free detection systems through several investigative methods. An evaluation of AI systems by professionals indicates their ability to detect financial statement fraud accurately. A quantitative analysis of historical data through AI enables fraud pattern detection according to this study method. The researchers who utilize the qualitative method meet with forensic accountants for their research work. The research delivers both forensic accountants and financial auditors definitive information about the challenges they face and their perspectives toward AI system implementation in audit procedures. The results show that AI is very successful when recognising fraud trends, particularly when using machine learning and deep learning approaches. However, the quality of the data and the settings of the algorithms still have an impact on how reliable AI is. Furthermore, despite ongoing worries about result interpretation and accountability of AI models, qualitative data suggests that auditors generally embrace AI as a tool that speeds up the audit process. According to the study's findings, artificial intelligence (AI) can effectively assist financial audits; however, to improve the validity of fraud detection, it should be used in addition to the analysis of qualified examiners. To increase the accuracy of fraud detection in the future, this study suggests creating more transparent AI models and integrating AI with blockchain technology.*

**Keywords**: *Artificial Intelligence, Fraud, Financial Audit, Mixed-Method, Anomaly Detection*
*Received on February2025; Revised on March 2025; Accepted on March 2025; Published on April 2025*

## I. INTRODUCTION

Corporate stability and market integrity are at risk from financial fraud. WorldCom's 2002 accounting disagreement serves as evidence that businesses that engage in dishonest reporting may suffer severe consequences. (Ramazan Cakali et al., 2023) According to the Association of Certified Fraud Examiners (ACFE, 2022), fraud costs companies about 5% of their annual revenue. The identification of more complex fraud patterns remains a difficulty for conventional inspection procedures (Rasha Kassem, 2023). The detection of fraud requires critical novel approaches, including artificial intelligence (AI) according to Hafez et al., 2025. Artificial intelligence, specifically machine learning algorithms, represents a viable fraud detection method in banks because these algorithms demonstrate the automatic ability to detect irregular transaction patterns (Brown et al., 2021).

The analysis of big financial data through AI technologies enables the detection of anomalies leading to insights for predicted financial statement audit fraud (Rashid et al., 2023). Several problems persist in using artificial intelligence for fraud detection despite its successful results in various applications. AI model dependability rests primarily on the quality of the training data supplied to it. This constitutes the primary obstacle. The detection accuracy suffers potentially when the dataset information shows biases or inadequacies in representation. Studies demonstrate that combining blockchain technology with AI produces powerful data security combined with

DOI: 10.51903/jmi.v4i1.168

transparency that leads to superior fraudulent transaction detection (Sets, 2024). Artificial intelligence models' "black box" operation creates difficulties for auditors to understand their decision-making processes, which represents an extra barrier to understanding analytical results. Explainable AI (XAI) has advanced as a solution to promote transparency within AI decision systems because Awosika et al. (2024) developed the technology. The application of AI technology within forensic auditing faces challenges because auditors need to demonstrate readiness related to technological infrastructure and data security, and have the background knowledge needed to work with this technology. AI acceptance by auditors relies heavily on organizational readiness to implement technological progress (Anh et al., 2024). The successful implementation of artificial intelligence-based fraud detection requires technology innovators to work together with audit researchers to achieve both acceptance and success.

According to the research conducted by Olubusola Odeyemi et al. (2023), AI systems can assess large datasets, identify complex patterns, and detect irregularities that conventional methods could overlook, enhancing the overall audit procedure. Algorithms, data integrity, and the model's ability to decrease detection errors impact its reliability. Regulatory frameworks, templates, transparency, and auditor trust are among factors that impact the use of AI in audits (Brown et al., 2021).

Based on Rashid et al. (2023), AI will assess data in real-time and swiftly identify fraud. According to another study that examined Random Forest, Neural Networks, and support vector machines, deep learning performs better in terms of accuracy than other machine learning models (Rashid et al., 2023). The lack of clarity and transparency in the auditors' deception. However, an important barrier to the application of AI is the detection of data (Brown et al., 2021). Additional studies using a mixed-methods approach are projected to fully investigate the effects of adding AI into financial audits, particularly the difficulties auditors experience when implementing this technology into practice.

The review of academic work identifies three main research gaps: inadequate studies that use mixed methodologies for AI evaluation, unclear algorithms, and a lack of expertise in blockchain integration with AI auditing systems (Han et al., 2023). The research establishes three propositions, which state that AI-based machine learning demonstrates better results than traditional auditing, while model perceptibility affects auditor acceptance of AI systems, and trust depends on algorithmic elements and data reliability. Integrated systems of blockchain with artificial intelligence technology will enhance fraud detection by improving accessibility as well as reliability, according to current beliefs.

The AI fraud detection examination consists of using machine learning algorithms to test past data, as well as qualitative assessments of implementation barriers and auditor acceptance strategies, along with data quality and accuracy testing. Additionally, this study explores the integration of blockchain technology and artificial intelligence to improve the transparency of financial audits. By demonstrating that AI can successfully identify fraud, this research greatly enhances the field of forensic accounting (Daneshmand, 2024). Additionally, it suggests utilizing blockchain technology alongside artificial intelligence to enhance transparency in the audit process (Arham, 2025). Moreover, this research highlights several implementation challenges for AI, particularly concerning model transparency and regulatory issues that require further investigation (Maxwell Nana Ameyaw et al., 2024). Therefore, to evaluate the extent of artificial

intelligence (AI) integration in the auditing field, this research merges technological methods with qualitative assessment.

## II. LITERATURE REVIEW

### *A. Fraud in Financial Statement Audits*

The fraud in financial statements was categorized into three headings by the International Association of Certified Fraud Examiners (ACFE, 2022): asset misappropriation, corruption, and fraudulent financial reports. Considerable relevance concerning audit work and the official supervisory authorities is associated with these types of fraud. Asset misappropriation is one of the very few general types that is most commonly heard. For example, theft of cash, manipulation of inventories, and misuse of company resources are among the commonest types that come under asset misappropriation. As regards the categories of corruption, fraud related to purchases, conflict of interest, and bribery can all be directly classified under corruption. By contrast, financial statements resulting from data manipulation, such as inflated revenues or hidden liabilities, are also deceptive. Conventional techniques mostly fail to measure up when it comes to the identification of more sophisticated fraud patterns. (Ejike and Okolie, 2023) These financial statement anomalies have been verified by forensic specialists to be very good indicators of economic fraud. Artificial intelligence (AI) technology is gaining popularity in terms of ensuring that anomaly detection capability stands high, especially in improving audit efficiency.

### *B. The Role of Artificial Intelligence in Fraud Detection*

Machine Learning and deep learning algorithms can pinpoint atypical patterns in financial transactions through the characterization of massive data. Artificial Intelligence encompasses a wide range of fields such as intelligent frameworks, expert systems, natural language understanding, and smart robotics (Sarker, 2021). Among the several AI algorithms, various stand out for detecting fraud in finance. One of such states is Machine Learning (ML), which supports various ideas relating to data science for the study and development of algorithms to induce unusual patterns or suspicious behavior in financial data (Ali et al. 2022). In addition, Natural Language Processing (NLP) is applied in sentiment analysis and automated document processing, two important areas for human language comprehension and processing, such as chatbots (Vyas et al., 2024). Neural networks, on the other hand, bring out complex relationships among financial variables that are normally difficult to catch by conventional means (Kim, 2022).

### *C. Blockchain as a Complement to AI in Forensic Auditing*

The decentralized ledger structure inherent in blockchain is immutable and unsupervised, which decreases data manipulation chances and increases transparency and security in accounting record audits (Georgiou et al., 2024). It thereby helps ensure that security is maintained with improved clarity for data in information systems. The varied aspects of business processes have been successfully enabled by smart contracts to most accurately function in their field capacities (Marcelletti et al., 2024). The Blockchain view can always help in real time regarding the detection of irregular actions (Brown et al., 2021). The research of (Hossain, M.Z., Johora, F.T. et al., 2024) suggests that using smart contracts can improve efficiency and fortify the security concerning financial transactions in accounting. The holistic approach of Blockchain, coupled

with AI to detect and prevent fraud, build confidence in accounting choices, and clarify asset ownership and obligations, helps to augment the efficiency of the audit (Han et al., 2023).

### *D. Mixed-Method Study in Evaluating AI and Blockchain in Auditing*

The approach adopted in this study is a mixed-method approach for an in-depth assessment of the efficacy of AI in fraud detection and its correlation with blockchain. This approach utilizes both quantitative and qualitative methods for a more thorough analysis rather than relying on a singular isolation method (Bieńkowska & Sikorski, 2024). Whereas quantitative methods engage historical financial transaction data in evaluating the accuracy and efficiency of AI algorithms concerning anomaly detection, Pratto et al. (2022) argue that machine learning algorithms can improve fraud detection with efficiency and reduce manual reconciliation. The qualitative method relies on conversations with auditors and financial and regulatory professionals to gain deeper insights into barriers to AI adoption in financial auditing engagements and how reliable AI can be in carrying out audit procedures (Hu et al., 2023). Such mixed methods are relevant because fraud detection requires an understanding of business context and financial regulations, in addition to some quantitative assessment. By the immutability and append-only nature of blockchain data, experts can rely on this data for decisions, as noted in a study by Han et al. (2023), and underline how blockchain engenders trust and transparency in financial processes.

This study draws upon two interrelated theoretical foundations to support the integration of artificial intelligence (AI) and blockchain in financial auditing: the Technology Acceptance Model (TAM) and the Audit Innovation Adoption Framework. TAM posits that perceived usefulness and ease of use influence an individual's intention to adopt a technology. In the context of auditing, explainability and perceived reliability of AI systems influence auditors' trust and willingness to incorporate AI into their workflows (Awosika et al., 2024).

Complementing this, the Audit Innovation Adoption Framework suggests that innovation adoption within audit firms is shaped by perceived audit quality improvement, organizational readiness, and regulatory compliance (Leocádio et al., 2024). Accordingly, this study hypothesizes that the effectiveness and acceptance of AI in audit fraud detection is determined by three key factors: (1) model performance (accuracy and interpretability), (2) integration with transparent frameworks such as blockchain, and (3) auditor trust built upon ethical use and explainable AI outputs. By grounding the study in these frameworks, this research not only investigates technical performance but also contextualizes findings within the behavioral and organizational dimensions of auditing practice.

## III. RESEARCH METHOD

### *A. Research Approach*

The main area of research involves a mixed-methods approach involving quantitative and qualitative techniques to determine AI competence and reliability in fraud detection in financial audit reports. The quantitative method of this research relies on ML and DL algorithms to study previously done historical financial report data toward extracting unusual patterns indicative of possible fraud. The effectiveness of the developed AI model in detecting fraud signals will be assessed using metrics like Neural Network, Random Forest, Support Vector Machine (SVM), and Decision Tree. Furthermore, the quantitative technique requires the assessment of AI-produced signals by evaluating fraud with the help of human skill to get to the bottom of the issue

of how well a machine can detect bad accounting behavior. The papers highlight the issue in detail by addressing various issues that arise when AI technology is implemented for auditing. Some of these issues are matching the traditional audit approaches to AI and the accuracy of the assessments, which are the result of AI. In contrast, the release of the qualitative approach entails going through one-on-one interviews with professionals from the finance industry, auditors, and even forensic experts to extract information in terms of their perception of AI incorporation into financial audits. Through these interviews, an attempt is made to find out whether the auditors have the required knowledge of getting involved in the AI technology, the barriers to its implementation, and the chances for reinventing AI-augmented forensic audits. To guarantee an organized examination, the insights obtained from the conversations will be recorded and evaluated using thematic analysis.

The methodology set in the study provides a clear view of how the Fraud Detection Framework is implemented, which has been organized into five basic stages as showcased in Figure 1. The first stage includes Data Collection and Preparation for collecting and processing financial statements with transaction logs and public databases by applying cleansing methods to remove noise and duplicates and irrelevant entries ahead of data transformation and normalization. The second phase, Feature Engineering and Selection, will statistically examine some of the most predictive variables and implement techniques such as PCA or RFE for refining the model inputs. The third phase is Model Development, wherein various machine learning and deep-learning algorithms like Random Forest, Support Vector Machines (SVMs), Neural Networks, Gradient Boosting Machines (GBM), and Extreme Gradient Boosting (XGBoost) are trained on legitimate and fraudulent data with hyperparameter tuning to ensure their robustness. Fourth is Evaluation and Validation, where key model metrics and performance tests are linked with interviews with auditors regarding real applicability and professional challenges. The last, most important point is Interpretation and Reporting, which interprets model decisions using other techniques like SHAP and LIME, whereby auditors and forensic analysts lend their knowledge to attest to the reliability of AI in Financial Auditing.

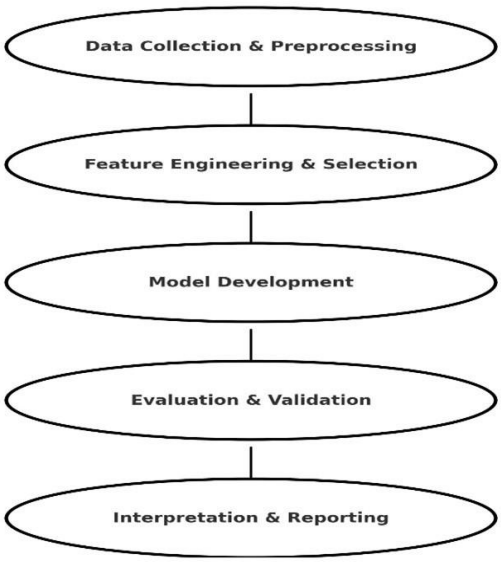


**Figure 1. Research Framework**

B. Software and Tools Utilized

In this work, various software applications are used for manipulating the AI models and data. The primary programming language is Python, and a variety of import libraries, such as TensorFlow and Scikit-Learn, are being utilized in development and training deep learning and machine learning models. Financial report datasets are stored and organized in an SQL-based database. Power BI and Tableau are utilized for data visualization, presenting analytical findings through interactive dashboards and charts. NVivo is also used in qualitative analysis to perform thematic analysis of in-depth interviews. To improve data security and privacy in digital transactions, this study integrates blockchain-based technologies like Hyperledger Fabric.

*C. Data and Sampling Techniques*

Qualitative as well as quantitative information is used in this research. A historical financial report dataset comprising both routine and possibly fraudulent transactions makes up the quantitative data. The study also includes classification outcomes using artificial intelligence (AI) models, which are assessed based on accuracy, F1 score, and AUC-ROC. In the meantime, auditors are interviewed to get qualitative data about how they evaluate the use of AI in financial audits, specifically about transparency, effectiveness, and the possible decrease in human bias in AI-based auditing. This study uses stratified random sampling for quantitative data processing to guarantee that the dataset's fraudulent and non-fraudulent transactions are allocated proportionally. To guarantee a more representative data distribution, systematic sampling is also used to choose audit data at predetermined intervals. For example, it might be used to choose every nth transaction in a company's financial report. Purposive sampling is employed to choose AI models for analysis; models like Neural Networks, Random Forest, SVM, and Decision Tree are selected according to how well they detect fraud. Similar to this, Purposive Sampling is used to select auditors for interviews based on their experiences utilising AI in financial audits, with a minimum of five years of professional experience, to gather qualitative data.

Furthermore, Snowball Sampling is employed to expand the scope of interviews, allowing interviewed auditors to suggest other auditors who possess similar knowledge in AI-driven auditing. For quantitative data, the sample size of the study varies from 1,000 to 10,000 financial transactions, ensuring an even distribution of both fraudulent and non-fraudulent transactions to maintain the accuracy of the AI model. Between ten and twenty skilled auditors with knowledge in AI auditing are interviewed to gather qualitative data. These sampling techniques were selected considering critical factors in the methodology for the study. Stratified random sampling is used here, carefully ensuring that each category of transaction or event has a good representation in the dataset. This method includes systematic sampling, ensuring that the transactions captured for the final selected sample are from different periods. Purposive Sampling is used for selecting effective AI models since it concentrates only on well-performing models. Concurrently, snowball sampling is going to be used in aggregating experts who have working knowledge of AI-driven auditing. This method shall yield what is considered accurate-representative-reliable data against which AI can be evaluated on its effectiveness to detect fraud.

*D. Data Analysis Techniques*

The quantitative and qualitative data analysis methods are utilized in this study. The capability of AI models to detect fraud in financial audit reports is numerically evaluated through various data analysis techniques. The main approach evaluates model performance using classification metrics, where accuracy and F1 score are a few of the important performance indicators for a model. Models like Random Forest, Neural Networks, SVM, and Decision Trees are further compared in the research to determine which AI model can effectively detect anomalies in financial accounts. For further analysis, the AUC-ROC metric is used to assess the models in their ability to discriminate between fraudulent and legitimate transactions. The performance of the more robust models is compared against traditional systems by using the deep learning approaches of Long Short-Term Memory (LSTM) and Artificial Neural Networks (ANN). This study further employs thematic analysis to explore data acquired through interviews with auditors and forensic financial specialists to highlight trends and factors influencing AI usage in auditing. An analysis of indicators of fraud typically derived from financial reports is carried out via content analysis, contrasted against audit trails and forensic documents. It goes into full detail on the reliability of AI in fraud detection, combining the quantitative and qualitative evaluations of AI with shining praises upon it.

*E. Validity and Reliability of the Research*

The most current studies have come up with ambiguous results concerning the dependability and authenticity of the AI systems about fraud detection, as such studies have tried to analyze and find out how much effective AI methodology would be in the possible detection of fraud through a Critical Systematic Literature Review (SLR) study which consisted of 16 articles from reputed journals published from 2018 to 2024. Accordingly, for the considered output, AI is determinant for fraud detection in financial audits. Furthermore, some studies have been done to jointly use blockchain technology with AI to ensure the security and transparency of audit processes. However, issues of using AI models on the one hand and threats of manipulating data on the other hand have raised two constant challenges. This study views the auditors' and companies' experiences in using AI for fraud detection through a mixed-methods approach, with emphasis on changes in the auditors' roles and continuing professional development needs.

*F. Ethical Consideration*

This study was conducted in adherence to established ethical guidelines. Before participating in interviews, all respondents were informed about the purpose of the research, their right to withdraw at any time, and the confidentiality of their responses. Written informed consent was obtained from each participant. The research protocol and interview procedures received formal approval from the Research Ethics Committee.

## IV. RESULT

This study employs a mixed-methods approach to examine the possibility of artificial intelligence (AI) identifying fraudulent activities in financial statements. Therefore, a set of financial statements belonging to companies classified as fraudulent or non-fraudulent is employed to carry out a quantitative analysis on different AI models. Exploratory models include neural networks, random forests, SVMs, decision trees, etc. The performance capabilities of each of these AI models are summarized in terms of accuracy value and F1, which will introduce the result of the comparative study on models, as seen in Table 1.

**Table 1. Performance of AI Models in Fraud Detection**

| AI Model | Accuracy (%) | F1 score (%) |
|---|---|---|
| Neural Network | 95.1 | 93.5 |

| | | |
|---|---|---|
| Random Forest | 92.4 | 90.7 |
| Support Vector Machine (SVM) | 88.7 | 87.2 |
| Decision Tree | 84.3 | 82.1 |

Accuracy and F1 score are the most important attributes that can be employed to gauge the performance of AI algorithms in fraud detection. The Neural Network is the best-performing model when it has 95.1% accuracy and 93.5% F1 score. It is a deep learning model that can eliminate classification error by finding complex patterns in the data while maintaining equilibrium between recall and precision. These findings are the best evidence for the fact that the use of positive network is a good example, and standing as a way to handle the most chaotic data is truly a must. However, to run it efficiently, it requires a large amount of data and a high-speed computing machine. In addition to Neural Networks, with 92.4% accuracy and 90.7%, F1 Random Forest also delivers the same high-quality performance as Neural Networks. This model can gain a larger and more non-assembled approach and there will be less risk of overfitting to the model because it is an ensemble approach that consists of more than one Decision Tree. Its high accuracy and F1 score make it more trustworthy for fraud detection.

Despite its enhanced performance over Decision Tree, Random Forest is not only more accurate in fraud detection but also suitable for the detection of fraud in complex and unknown to the user a new areas of the data. On the other hand, the Support Vector Machine (SVM) achieves an F1 score of 87.2% and an accuracy of 88.7%. In the scenario where income data needs to be analyzed to find the pattern in a financial line, such as multiple dimensions, the SVM algorithm will be the best option. However, its precision is not the highest among the mentioned models. Computation efficiency is a crucial issue, especially when managing large datasets. Random Forest outperforms SVM in classification accuracy for predicting mitigation and disaster preparedness indices. Decision Tree achieves the lowest performance with an accuracy of 84.3% and an F1 score of 82.1%.

Although this model is easy to understand and analyze, it often overfits, particularly in complex architectures. Its inability to identify intricate patterns is shown by its lower accuracy. These analytical findings are also backed by the observation that Decision Tree does not perform as well in stock price prediction compared to Random Forest and SVM. Neural networks are the most effective choice for identifying fraud due to their excellent accuracy and F1 score. Nonetheless, Random Forest serves as an excellent alternative for clients seeking interpretability while maintaining efficiency. Although decision tree methods are more effective for initial assessments or when included in ensemble approaches, Support Vector Machines (SVM) are suitable for analyzing datasets with high dimensions..

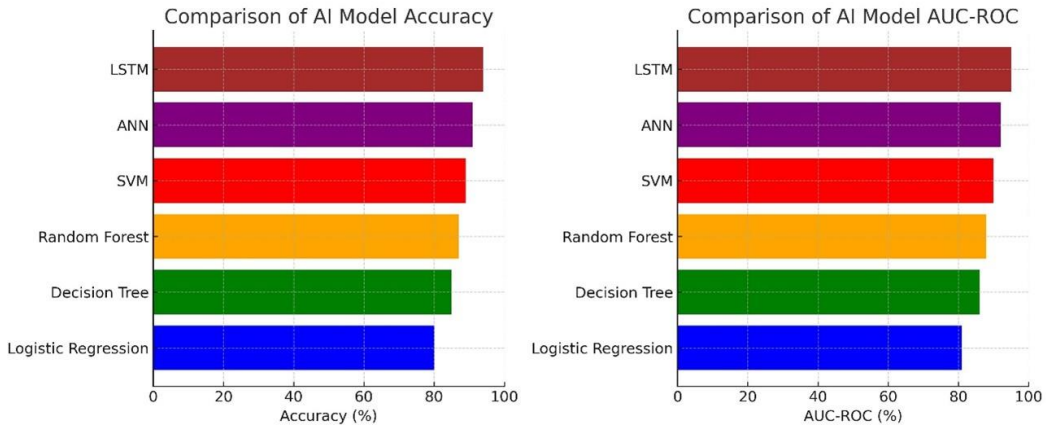


**Figure 2. Comparison of AI Model Accuracy and AUC-ROC in Fraud Detection**

As per the Figure 2 report, the Long Short-Term Memory (LSTM), Artificial Neural Network (ANN), and Support Vector Machine (SVM) models are the ones that score the highest in the area of fraud detection. The fact that deep learning models such as LSTM and ANN can recognize intricate financial data patterns vastly increases their fidelity in abnormality and fraud detection. On the contrary, SVM and Random Forest display a level of competitiveness, and also the fact that they are the least resource-demanding options in the era of deep learning models. The problem with a range of AI model methods in financial fraud detection is that the SVM and Random Forest recognizers perform better in terms of precision among the models. However, as they cannot find the nonlinear relationship between complex financial data, models like Decision Tree and Logistic Regression are the ones that always lag. These results are in harmony with what other studies have shown, which is that AI models relying on deep learning and ensemble techniques are more effective than traditional methods in fraud detection. As a result, the introduction of AI into forensic audits could improve fraud detection and help auditors find and understand the details of the transaction that are under suspicion more accurately.

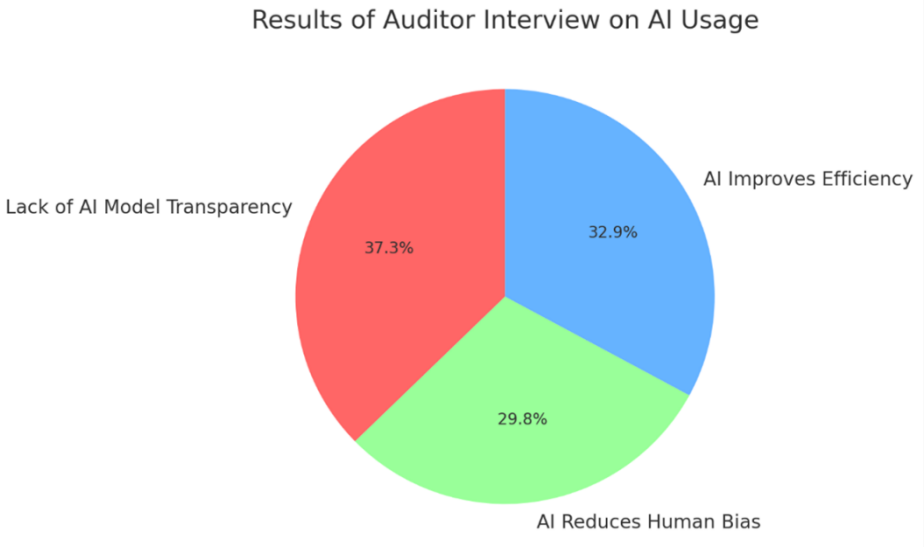


**Figure 3. Interview Results of Auditors Regarding the Use of AI in Auditing**

**Table 3. Thematic Findings from Auditor Interviews**

| Theme | Example Quote | Interpretation |
|---|---|---|
| Transparency Concerns | "AI systems often don't show how they reached their conclusions." | Indicates distrust due to AI's black-box nature |
| Improved Efficiency | "AI helps reduce our audit duration significantly." | Supports practical value in real-time analysis |
| Bias Reduction | "Data-driven patterns are less subjective than human judgment." | Suggests AI can improve audit objectivity |
| Need for XAI | "We want to understand the reasons behind flagged anomalies." | Auditors require explainability for validation and trust |

The results of auditor interviews regarding the use of artificial intelligence (AI) in finance Audits are shown in Figure 3. The pie chart illustrates three primary perspectives: reduced human bias (29.8%), improved audit effectiveness (32.9%), and insufficient AI transparency (37.3%). Realising that AI frequently functions as a "black box," making the decision-making process hard to understand, the majority of auditors (37.3%) voice worries about its lack of openness. That issue affects auditors' confidence in AI's fraud detection capacity as well as regulatory concerns. The findings of 32.9% of auditors, artificial intelligence (AI) improves audit efficiency by speeding up data analysis, automating anomaly detection, and decreasing labour expenses, allowing auditors to concentrate on more complicated studies. Furthermore, according to 29.8% of respondents, AI can lessen human bias in audits through offering statistically based patterns and data-driven analysis that are more objective than manual methods. According to other research, machine learning algorithms are more efficient than human auditors at manually analysing audit data for patterns. These are nonetheless significant challenges in an area where others have widely recognized the strong strengths of AI in performance from proper implementation and neutrality in recommending. As a result, creating more interpretable and understandable algorithms is crucial for enhancing AI's appeal in the auditing sector. Table 2 shows the comparison of performance between manual and AI-driven assessments.

**Table 2. Comparison of Manual Audit and AI in Auditing**

| Aspect | Manual Audit | AI in Audit |
|---|---|---|
| Completion Time | Approximately 2 months | Approximately 2 weeks |
| Accuracy | 60-75% | 85-95% |
| Efficiency | Low | High |
| Interpretability | Easily understood | Still requires further development (XAI) |

A comparison between AI-driven auditing and traditional auditing shows that the use of AI greatly improves the accuracy and efficiency of audits. AI has the potential to cut audit completion durations by as much as 75%, allowing for quick analysis of large datasets. Moreover, artificial intelligence demonstrates greater reliability than human auditors since it can detect patterns that may be difficult for auditors to observe. Nonetheless, even with the improved accuracy of AI, comprehending AI models entirely continues to be difficult. Stakeholders and auditors often struggle to understand how AI models operate and the rationale for their decisions. Enhancing transparency and confidence in AI-supported audits depends on progress in Explainable AI (XAI). Table 3 emphasizes the benefits of AI in detecting fraud.

**Table 3. Advantages of AI in Fraud Detection**

| Factor | AI Advantages |
|---|---|

| | |
|---|---|
| **Anomaly Pattern Detection** | AI surpasses traditional methods in identifying complex patterns in financial reports. Deep learning models can detect suspicious transactions that were previously difficult to identify. |
| **Transparency** | Combining AI and blockchain is already making for great improvements in transparency, both in creating an immutable audit trail. The technology enables tracing any 'suspect' transaction from its original point to the present instance without any possibility of data alteration. |
| **Explainable AI (XAI)** | More needs to be done to instill greater confidence in AI among auditors and stakeholders. As things stand, many AI models operate as black boxes, making it impossible for the auditors to understand the rationale behind fraud predictions. |

What the results indicate is the improvement in fraud detection skills compared to the old ways, but AI for fraud detection has some constraints related to model explainability. To advance the understanding and acceptability of AI-based analytics results by auditors and other stakeholders, it is recommended to further investigate developing advanced analytical capabilities in an explainable AI (XAI). By using deep learning models, it is possible to identify transactions that normally would not be observed by standard manual detection. Also, integrating AI into auditing by utilizing blockchain technology that increases transparency through its unalterable records of transactions will do much more.

These techniques suggest employing artificial intelligence (AI) to improve efficacy in fraud detection and that this study would advance forensic auditing. The findings of this research concur with previous studies emphasizing the ability of AI to assist auditors in identifying unusual patterns that are often difficult to pick up through human judgment. Furthermore, AI may ease the auditors' workload while increasing the accuracy of detecting financial irregularities. However, precise and comprehensive public regulations are vital to ensure the proper integration of AI into the traditional financial audit system.

This research has various limitations, despite the significant contributions it made. A restricted dataset was used to assess the AI model, and therefore, it could not encompass all possible fraud situations that would have been encountered in real cases. Besides, auditors generally see it as a major impediment in that they find it very difficult to follow the reasoning behind the AI system's fraud detection outputs. Thus, improving model transparency will require more effort on Explainable AI (XAI). Furthermore, due to the study's focus on a limited number of companies that have applied AI in the auditing profession, it is possible that the findings may not be generalized across other industry sectors. Future studies should concentrate on creating more transparent AI models, employing supplementary datasets, and exploring AI implementations across different industries to tackle these limitations.

## V. DISCUSSION

The study establishes that artificial intelligence detection of financial account fraud has three major impacts, which include better accuracy alongside enhanced operational efficiency and superior capability to detect suspect transaction patterns. Deep learning models with neural networks reach the highest levels of efficiency according to quantitative examination because they achieve optimal accuracy and F1 score for identifying fraud indicators. The detected ability of AI demonstrates its competency in recognizing normal payment systems from risky ones. A Neural Network model surpasses Random Forest, Support Vector Machine (SVM) and Decision

Tree models to achieve 95.1% accuracy and 93.5% F1 score in the analysis of Table 1 information. Complex transaction recognition becomes achievable through the main benefit of neural networks. The implementation faces major hurdles because it requires large amounts of processing power, together with sufficient data for achieving the best possible performance.

The Random Forest model achieved remarkable outcomes with 92.4% accuracy along with a 90.7% F1 score. Wang et al. (2023) showed that by being less standard in structure than a stand-alone Decision Tree, the model predicts more consistently and limits overfitting. The SVM model, on the other hand, can mainly be used to detect problematic transaction patterns, especially where high-dimensional datasets are concerned, because of its low 88.7% accuracy. In contrast, the Decision Tree has the lowest accuracy at 84.3% and is one that can easily be over-fitted, but is very interpretable. The models mentioned in fraud detection, as seen in Figure 2, are Long Short-Term Memory (LSTM), Artificial Neural Network (ANN), and Support Vector Machine (SVM). The ability of sophisticated deep-learning models like the LSTM and Artificial Neural Networks to detect anomalies and suspicious transactions rests on the fact that such complex patterns of financial data are also difficult to detect. This was further emphasized by Qatawneh (2024), who elaborated on the deep learning capacity for financial fraud detection.

Intelligent techniques for fraud detection, LSTM and ANN in this study, were found to outperform other models when it came to accuracy, as they also proved as distinguished models in nonlinear pattern recognition and temporal relationships found in financial data. Despite this, SVM has demonstrated commendably excellent performance and thus can be a serious contender in that accuracy parameter, making it suitable for fraud detection. Random Forests also performed quite comparably with others, especially in cases where computational efficiency is a high concern. (Mohaimin et al., 2023) assessed various artificial intelligence-based techniques in fraud detection intelligence models in identifying financial irregularities, finding that Support Vector Machine (SVM) and Random Forest demonstrated a significant level of accuracy in fraud detection. Nonetheless, most of the time, these simpler models, such as Decision Trees and Logistic Regression, are unable to deliver their peak performance due to their simple architectural design patterns, which, by nature, consider the way a pattern can be recognized in complex financial data (Wen 2023).

Research findings confirm that artificial intelligence aids financial audit fraud detection through deep learning models, which include LSTM and ANN. Audit professionals achieve better questionable transaction pattern recognition through an AI model. Enhanced transparency combined with decreased risks of financial reporting fraud becomes possible when AI is applied for forensic auditing purposes.

The incorporation of AI into auditing faces significant challenges, as per the findings from extensive discussions between AI experts and forensic auditors. Auditors who took part in these discussions showed strong reservations about AI model opacity because these systems remain mysterious. XAI technology requires development since it will provide auditors with explanations about how AI systems make decisions. AI technology increases audit performance through fast data set analysis and reduces auditors' work-related tasks, as reported by 32.9% of participating professionals. Per 29.8% of survey participants, AI presents a solution for audit bias reduction since data models provide more objective outputs when compared to manual auditing methods. Traditional auditing proves less efficient than AI-enabled auditing according to the data presented

in Table 2, which supports the research conclusions. AI shortens the auditing duration, which amounts to two weeks, while each audit process requires two months (Leocádio et al., 2024). The accuracy rate AI-powered auditing provides contrasts with manual audits since manual audits offer about 60–75% accuracy, whereas AI-powered auditing reaches 85 to 95% accuracy rates. (Sapiens, 2020). The main obstacle of AI models involves their inability to explain their decisions because organizations need improvements in Explainable AI (XAI) to build trustworthy analytical outputs. AI-powered financial audits achieve better implementation when blockchain technology increases the transparency level of operations. The evaluation process using AI takes approximately two weeks to finish (Leocádio et al., 2024), though some steps need up to two months to complete. The accuracy level of AI-driven auditing surpasses manual auditing at 85 to 95% since it reaches a better accuracy rate. The particular phrase "Sapiens, 2020" cannot be paraphrased because it refers to both a book title and the publication year instead of being a text fragment.

The following studies need to study regulatory frameworks in addition to developing full-scale Artificial Intelligence implementation strategies while honoring legal and ethical concerns. The research significantly promotes forensic auditing through its proof that AI enhances fraud detection precision. It is significant to recognize some limitations during this stage. Current technology brings numerous benefits to fraud detection through AI, but auditors face difficulties when attempting to gain system explanations about which data features drive decision outcomes. Financial audit is inhibited by both technical obstacles and official restrictions related to the implementation of AI systems. Owing to ambiguous legislation and a lack of comprehensive guidelines, numerous organisations are still hesitant to deploy AI for audits Humanize Text. AI models used in this work operated on a particular dataset that makes their testing results unusable for all possible fraud detection scenarios within actual settings. Results from this research apply only to organizations using AI based on the topology and they cannot be used to predict other industries. Future research should concentrate on developing better understandable AI models that need large data sets to ensure effective industry-wide implementation of financial audit AI applications.

## VI. CONCLUSION

It has been shown that the assessed AI models, particularly Random Forest and Neural Networks, produce predictions that are more accurate than those produced by conventional methods. The main obstacles to the extensive adoption of AI technology remain the lack of transparency in model decision-making, the high processing power requirements, and regulatory challenges. To improve the transparency of AI-generated assessments, organizations and auditors ought to utilize Explainable AI (XAI) to create clearer AI structures. In addition, the integration of blockchain technology with artificial intelligence (AI) has the potential to enhance the credibility and lucidity of financial audits. It is suggested that future studies use a larger dataset to guarantee that the findings accurately reflect circumstances in different economic sectors.

To support the advancement of AI in auditing, this study recommends three key actions: (1) developing interpretable AI models through Explainable AI (XAI) frameworks, (2) expanding cross-industry datasets for model generalizability, and (3) establishing regulatory guidelines that ensure ethical, secure, and transparent AI integration. These steps are essential to promote AI adoption while maintaining professional standards and stakeholder trust.

## REFERENCES

Alenizi, A., Mishra, S., & Baihan, A. (2024). Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence. *Ain Shams Engineering Journal*, *15*(6), 102733. https://doi.org/10.1016/j.asej.2024.102733

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences (Switzerland)*, *12*(19). https://doi.org/10.3390/app12199637

Anh, N. T. M., Hoa, L. T. K., Thao, L. P., Nhi, D. A., Long, N. T., Truc, N. T., & Ngoc Xuan, V. (2024). The Effect of Technology Readiness on Adopting Artificial Intelligence in Accounting and Auditing in Vietnam. *Journal of Risk and Financial Management*, *17*(1). https://doi.org/10.3390/jrfm17010027

Arham, M. W. (2025). *Transforming Auditing through AI and Blockchain : A Comprehensive Study on Adoption, Implementation, and Impact in Financial Audits*. *15*(2), 225–241. https://doi.org/10.4236/ajibm.2025.152011

Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. *IEEE Access*, *12*, 64551–64560. https://doi.org/10.1109/ACCESS.2024.3394528

Bieńkowska, J., & Sikorski, C. (2024). Integrating qualitative and quantitative methods: a balanced approach to management research. *Eastern Journal of European Studies*, *15*(1), 345–360. https://doi.org/10.47743/ejes-2024-0115

Brown, S., Davidovic, J., & Hasan, A. (2021). The algorithm audit: Scoring the algorithms that score us. *Big Data and Society*, *8*(1). https://doi.org/10.1177/2053951720983865

Daneshmand, M. (2024). *Financial Fraud Detection : A Comparative Analysis of AI and ML Techniques*. *4*(2), 138–142. https://doi.org/10.56472/25832646/JETA-V4I2P123

Georgiou, I., Sapuric, S., Lois, P., & Thrassou, A. (2024). Blockchain for Accounting and Auditing—Accounting and Auditing for Cryptocurrencies: A Systematic Literature Review and Future Research Directions. *Journal of Risk and Financial Management*, *17*(7). https://doi.org/10.3390/jrfm17070276

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1). https://doi.org/10.1186/s40537-024-01048-8

Han et al. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*(March 2021), 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hargyatni, T., Purnama, K. D., & Aninditiyah, G. (2024). Impact Analysis of Artificial Intelligence Utilization in Enhancing Business Decision-Making in the Financial Sector. Journal of Management and Informatics, 3(2), 282–296. https://doi.org/10.51903/JMI.V3I2.36

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*(April 2022), 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hossain, M.Z., Johora, F.T., R., Profound, T., research paper uses qualitative analysis to examine the, & M.R., & Hasan, L. (2024). The Impact of Artificial Intelligence and Blockchain

on the Accounting Profession. *IEEE Access*, *8*, 110461–110477. https://doi.org/10.1109/ACCESS.2020.3000505

Hu, K. H., Chen, F. H., Hsu, M. F., & Tzeng, G. H. (2023). Governance of artificial intelligence applications in a business audit via a fusion fuzzy multiple rule-based decision-making model. *Financial Innovation*, *9*(1). https://doi.org/10.1186/s40854-022-00436-4

Kim, H. (2022). Deep Learning. *Artificial Intelligence for 6G*, *22*(4), 247–303. https://doi.org/10.1007/978-3-030-95041-5_6

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. *Administrative Sciences*, *14*(10). https://doi.org/10.3390/admsci14100238

Marcelletti, A., Marangone, E., & Di Ciccio, C. (2024). *Balancing Confidentiality and Transparency for Blockchain-based Process-Aware Information Systems*. http://arxiv.org/abs/2412.05737

Maxwell Nana Ameyaw, Courage Idemudia, & Toluwalase Vanessa Iyelolu. (2024). The role of blockchain in auditing processes: A review and future perspectives. *International Journal of Scientific Research Updates*, *8*(1), 037–053. https://doi.org/10.53430/ijsru.2024.8.1.0045

Mohaimin et al. (2023). *Machine Learning in Business Analytics: Advancing Statistical Methods for Data-Driven Innovation*. *2023*, 104–111. https://doi.org/10.32996/jcsts

Okolie, P. I. P., & Ejike, S. I. (2023). *Using data analytics techniques for the detection of accounting fraud in financial statements*. 212–214. www.allmultidisciplinaryjournal.com

Olubusola Odeyemi, Kehinde Feranmi Awonuga, Noluthando Zamanjomane Mhlongo, Ndubuisi Leonard Ndubuisi, Funmilola Olatundun Olatoye, & Andrew Ifesinachi Daraojimba. (2023). The role of AI in transforming auditing practices: A global perspective review. *World Journal of Advanced Research and Reviews*, *21*(2), 359–370. https://doi.org/10.30574/wjarr.2024.21.2.0460

Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach. *IEEE Access*, *10*(August), 87115–87134. https://doi.org/10.1109/ACCESS.2022.3198956

Qatawneh, A. M. (2024). The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. *International Journal of Organizational Analysis*, *July 2024*. https://doi.org/10.1108/IJOA-03-2024-4389

Ramazan Cakali, K., Kurulu Başkanı, T., & Kalkınma ve Yatırım Bankası AŞ, T. (2023). Agency Problem in Corporate Governance: WorldCom Case. *İşletme | The Business Journal*, *2022*(1), 15. https://www.researchgate.net/publication/367166710_Agency_Problem_in_Corporate_Governance_Worldcom_Case_Kurumsal_Yonetimde_Vekalet_Sorunu_Worldcom_Vak'asi

Rasha Kassem. (2023). *Investigating the Black-box of External Audit Practice: The Paradox of Auditors' Failure in Detecting and Reporting Fraud*. *26*(4), 598–621.

Rashid, M., Luo, M., Ashraf, U., Hussain, W., Ali, N., Rahman, N., Hussain, S., Aleksandrovich Martyushev, D., Vo Thanh, H., & Anees, A. (2023). Reservoir Quality Prediction of Gas-Bearing Carbonate Sediments in the Qadirpur Field: Insights from Advanced Machine Learning Approaches of SOM and Cluster Analysis. *Minerals*, *13*(1).

https://doi.org/10.3390/min13010029

Sapiens, H. (2020). *AI in Auditing - An essential upgrade*.

Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 1–21. https://doi.org/10.1007/s42979-021-00592-x

Sets, F. (2024). *Utilization of Blockchain Technology to Improve Security and Transparency of Information Systems Pemanfaatan Teknologi Blockchain untuk Meningkatkan Keamanan dan Transparansi Siste ... Information Technology Studies Journal ( ITECH ) Pemanfaatan Teknologi*. *May*. https://doi.org/10.62207/qtds0397

Vyas, K., Vyas, K., & Arora, A. (2024). *INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING A Comparative Analysis of Natural Language Processing Techniques for Sentiment Analysis*. *12*, 903–908.

Wang, Y., Wu, H., & Nettleton, D. (2023). Stability of Random Forests and Coverage of Random-Forest Prediction Intervals. *Advances in Neural Information Processing Systems*, *36*(1), 1–28.

Wen, Z. (2023). Feature analysis and model comparison of logistic regression and decision tree for customer churn prediction. *Applied and Computational Engineering*, *20*(1), 55–61. https://doi.org/10.54254/2755-2721/20/20231073