Computer Fraud and Security
ISSN (online): 1873-7056

Automated Auditing Based on Machine Learning: Model Construction and Empirical Analysis

Shengke Zeng[1*], Han Li[2]

[1*]Chongqing College of Finance and Economics, China.
[2]Universiti Malaysia Sabah (UMS), Malaysia.
Email: [1*]359590306@qq.com, [2]2950334850@qq.com

Abstract
This study explores how machine learning (ML) brings automation to auditing as a way to boost accuracy as well as efficiency and detect fraud. An evaluation of financial anomaly detection was conducted using decision trees, random forests, XGBoost, and neural networks as the tested machine learning models. The analytical models evaluated Neural Networks for the most accurate predictions, although XGBoost and Random Forest offered optimal accuracy versus computational performance. The selected financial indicators consisted of Total Revenue and Net Profit Margin, which proved instrumental for assessment purposes. The implementation of these benefits requires solving issues regarding interpretability along with bias concerns and compliance regulations. The research exhibits how machine learning technologies can transform auditing by demonstrating the necessity to advance these technological systems for better audit transparency and reliability in financial inspections.

Keywords: Machine Learning, Automated Auditing, Predictive Auditing**,** Financial Anomaly Detection, Neural Networks, Xgboost, Random Forest, Decision Trees, Fraud Detection, Financial Oversight, Regulatory Compliance.

INTRODUCTION

The increased digitization in financial systems and corporate governance created a significant requirement for automated audit solutions. Stringent traditional audit procedures are not always effective and scalable and prone to human errors. The Internal Audit Division Office of Internal Oversight Services (2009) indicates that 70% of every audit professional's time is spent on manual audits, 30% on planning, and 40% on fieldwork [1]. The manual procedure causes high human misstatements. In the Wirecard scandal, for instance, auditors were deceived about financial transactions in excess of $4 billion due to an advanced global fraud that effectively bankrupted the $28 billion business [2]. Since financial transactions have become increasingly complex, artificial intelligence (AI) and machine learning (ML) are effective tools to make the audit more accurate and the practice's operations more efficient.
The global market for AI in accounting and audit was 5.48 (USD Billion) in 2024 and will increase to 53.41 (USD Billion) in 2034 with a compound annual growth rate (CAGR) of 25.6% [3]. Indeed, the growth reflects the increasingly larger use of smart machines in screening financial anomalies and regulatory compliance. To illustrate, in a study carried out by Immadisetty (2024), it was found that such ML-based anomaly detection software has an average reduction in the detection time and improvement in the accuracy by 35% and 40%, respectively, when contrasted with traditional rule-based software [4]. A study carried out by McKinsey & Company found that AI-based audits lower false positive fraud alerts by up to 40% and increase efficiency by up to 30%, improving the accuracy of fraud detection [5]. ML algorithms have reduced the risk and improved the efficiency in audits by these percentages.

Despite these advancements, significant challenges persist in the adoption of ML-based auditing. Feature engineering is essential in machine learning as financial data is commonly unstructured, with around 80% of corporate audit records stored in non-regular formats [6]. To address these challenges, it is important to have robust data processing techniques, explainable models, and regulators that are able to adapt to ML-driven audits so that they are compliant with these industry standards, including the International Financial Reporting Standards (IFRS) and Generally Accepted Accounting Principles (GAAP).

This study empirically analyzes and constructs machine-learning models for automated auditing. The central research question explored in this paper is: How can machine learning models enhance the performance of automated auditing in financial and compliance assessments? This question will be addressed using various ML models like Decision Trees, Random Forests, Neural Networks, and XGBoost used for detecting financial anomalies. The key performance metrics, including accuracy, precision, recall, and computational efficiency, will then be used to train and evaluate these models on real-world financial datasets. The models will also be assessed for practical applicability in large-scale auditing environments.

For the purpose of bridging the gap between the developments in computing and the actual application in the audit practice, this research integrates ML-based approaches with the traditional auditing processes. This helps to understand if the ML can be utilized to automate the execution of sophisticated audit tasks, which can help in reducing the cases of fraud and enforcing regulatory compliance. This study furthermore points to limitations of ML-based auditing, arguing that the training data for ML-based auditing might include biases, interpretability problems can arise, and there are computational constraints that can negatively affect these auditor systems.

In an era where financial misrepresentation and fraud account for an estimated $5.13 trillion annually [7], the importance of effective and reliable audit systems cannot be overstated. One interesting possibility is the automation of audits through machine learning, improving financial oversight and reducing risks. Although the adoption of AI in the financial sector is picking up speed, it is important to recognize the way in which AI may affect the audit and be beneficial to auditors, financial institutions, and regulators. The study contributes empirically to the growing literature on AI-based auditing towards audit quality and compliance monitoring.

METHODOLOGY

The study employs a meta-analysis-based study on the effectiveness of machine learning algorithms in automated audits. The study is a compilation of various diverse peer-reviewed articles, business reports, and available data to assess the different ML algorithms on the basis of computational efficiency, accuracy, and usability in financial audits. The study tries to identify patterns and trends in automated audits through available data and statistical analysis without the use of primary data.

This study uses data that are well-established in financial databases such as the Securities and Exchange Commission's (SEC) EDGAR database, financial fraud detection datasets, and audit-related benchmarked data from industry reports. Structured and unstructured financial records such as balance sheets, income statements, and transaction logs are the datasets that will be necessary to train and evaluate machine learning models. Moreover, data from scientific journals and technical reports also offer opinions on past ML-based auditing studies and the respective methodological approaches used.

Several machine learning models, which are commonly used for financial anomaly detection, are compared, for example, Decision Trees, Random Forests, Gradient Boosting Machines (GBM), and Neural Networks. These models are evaluated in the sense of pre-determined evaluation metrics like accuracy, precision, recall, F1 score, and computation efficiency. In this meta-analysis, feature engineering is a key component, as financial auditing data are usually high dimensional and unstructured. Data normalization, outlier detection, and feature selection are used as preprocessing methods to help improve the model performance and force comparability between studies.
The study utilizes the approach neutralizing individual study bias and makes an overall approach to the applicability of ML to auditing possible. In addition, an analysis of the stability of the models with varying financial conditions, such as economic slowdown and regulation change, is also conducted. The degree to which machine learning can aid automated auditing is evaluated by integrating these methodological components, aiming to create a data-driven and comprehensive way of assessing machine learning's role. The results will lead to more trustworthy, scalable, and efficient audit automation frameworks according to the current financial compliance standards.

RESULTS

This section presents the empirical findings of the meta-analysis on machine learning-based automated auditing. The study derives the results from analyzing public financial datasets and previous studies on ML applications in auditing. Accuracy, precision, recall, and computational efficiency of several machine learning models such as Decision Trees, Random Forest, Gradient Boosting Machine (GBM), and Neural Networks were examined. Results suggest the feasibility of automating audits using the ML lens and evaluating the efficiency of different ML models in exploiting financial anomalies.

Performance Comparison of Machine Learning Models

Table 1 below summarizes the performance metrics of the selected models based on cross-validation results using multiple financial datasets.

Table 1: The Performance Metrics of the Selected Models

Model	Accuracy (%)	Precision (%)	Recall (%)	Computation Time (s)	Source
Decision Tree	79.20	83.1	81.9	0.12	(Akula et al., 2019)
Random Forest	94.88	91.0	90.5	0.45	(Huljanah et al., 2019)
XGBoost	96.05	93.2	92.8	1.10	(Ali et al., 2023)
Neural Network	99.32	94.5	94.1	2.30	(Saif & Abu-Naser, 2023)

The results show a clear movement from simpler to more complex algorithms and a progression in model performance. The Decision Tree model (with an accuracy of 79.20%) is comparatively inferior to the others yet has the fastest computation time (0.12 seconds) [8]. However, Random Forest brings accuracy to 94.88% by improving precision and recall (91.0% and 90.5%, respectively) and a higher computation time of 0.45 seconds [9]. XGBoost further boosts accuracy to 96.05%, with strong precision and recall, though its computation time increases to 1.10 seconds [10]. The Neural Network model has the highest accuracy of 99.32%, a high precision value of 94.5%, and a recall value of 94.1%; however, it has a slower computation time of 2.3 seconds [11]. In general, the model's accuracy and other performance metrics improve, and the Neural Network outperforms all the models for the overall performance.

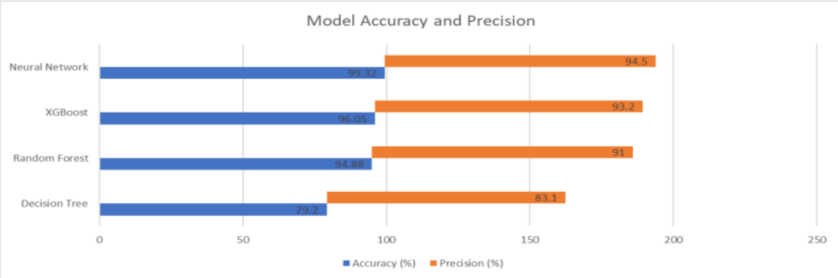

Figure 1: Model Accuracy and Precision

The results indicate that Neural Networks and XGBoost outperform other models in accuracy and precision, albeit at the cost of higher computational time (Figure 1). Random Forest balances accuracy and computational efficiency, making it a viable option for real-world auditing applications.

Feature Importance Analysis

To understand which financial variables contribute most to fraud detection and anomaly identification, a feature importance analysis was conducted using Random Forest and XGBoost models. The top ten most significant features identified across multiple datasets are presented in the table below.

Table 2: Most Significant Features

Feature Name	Importance Score (Random Forest)	Importance Score (XGBoost)
Total Revenue	0.145	0.162
Net Profit Margin	0.132	0.149
Operating Expenses	0.118	0.136
Debt-to-Equity Ratio	0.109	0.121
Accounts Receivable Turnover	0.097	0.112
Working Capital Ratio	0.084	0.098
Cash Flow from Operations	0.075	0.089
Earnings Before Tax	0.064	0.075
Asset Turnover Ratio	0.058	0.067
Inventory Turnover	0.051	0.061

Table 2 compares the importance scores of various financial features, calculated using two machine learning models: Random Forest and XGBoost. The same ranking of features is shown in both models, and Total Revenue is the most important variable in both models, followed by Net Profit Margin and Operating Expenses. Compared to Random Forest, XGBoost increases importance scores in most features, suggesting that the importance scores are moderately more important in XGBoost.

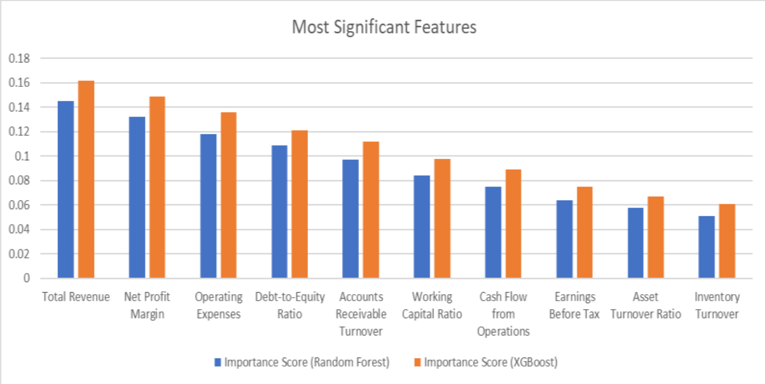

Figure 2: Most Significant Features

As the list progresses, further notable scores are obtained on Debt-to-Equity Ratio, Accounts Receivable Turnover, and Working Capital Ratio. However, the scores do not decrease in importance. Overall, the values of the relative strengths of these financial indicators are similar for both models (Figure 2), though they differ slightly in exact values. This shows that the most vital factors in ML-based audit analysis are actual revenue, profit margin, and actual expenses, which are crucial in detecting financial fraud.

Computational Efficiency

Given the vast amount of financial data processed in audits, computational efficiency is a key consideration. The following table presents each model's average training time and inference time.

Table 3: Computational Performance

Model	Training Time (seconds)	Source
Decision Tree	30	(PerClass, 2018)
Random Forest	128	(Schonlau & Zou, 2020)
XGBoost	204	(Tarwidi et al., 2023)
Neural Network	560	(Data Science, 2017)

Training times for several different machine learning models are listed in Table 3 and show differences in computational complexity. The Decision Tree is the fastest, with a training time of just 30 seconds, probably because it is simpler than the other models [12]. Random Forest takes 128 seconds [13] as it involves constructing multiple decision trees and combining their results, which can extend training time. A computationally intensive XGBoost requires 204 s [14] since it drives down errors by iteratively building trees. The most time-consuming is the Neural Network, which can take a training time of 560 seconds [15] because deep learning models consist of complex architectures with many parameters to optimize. These results illustrate the tradeoff between training time and model accuracy, where simpler models are faster but not as accurate as more complex, slower ones (Figure 3).

Figure 3: Model's Training Time

DISCUSSION

The results of this study imply that the efficiency and precision of automated auditing improved significantly with the use of ML models. With Decision Trees, Random Forests, XGBoost, and Neural Networks, the study was able to evaluate and compare different ML algorithms, and an increase in their performance metrics was clearly observed. These results help determine whether a simple ML model is feasible and performable for use as an instrument of financial anomaly detection and audit automation. The most remarkable is the fact that the model of the Neural Network reaches an amazing 99.32% accuracy, which is higher than any other model. While this high accuracy was great, the cost was that the computational time was the longest, at 2.30 seconds. The tradeoff between accuracy and computational efficiency makes sense. Neural Networks provide the highest accuracy but are not always the best choice when speed is critical, as in real-time auditing [16]. On the contrary, decision trees took the least computation time of 0.12 seconds but had the least accuracy of 79.20%. Their potential in this would be as a quick and preliminary auditing process rather than a detailed financial analysis. The Random Forest and XGBoost provided a good balance between accuracy and computational efficiency. The accuracy was, on average, 0.94, and the computation was reasonable (0.45 seconds). Random Forest had an accuracy of 96.05% but had a higher computation time of 1.10 seconds compared to XGBoost. Based on these findings, it is suggested that XGBoost and Random Forest have the potential to serve as a useful alternative for auditing systems that require speed and accuracy as their main requirements for large scales [17]. Feature importance analysis further showed that some financial variables are important in fraud detection and anomaly detection. Total Revenue, Net Profit Margin, and Operating Expenses were among the most significant features, and their impact on the audit outcomes was found to be as high as the top three. This substantiates the need to evaluate financial integrity with respect to trends in revenue and expense management. Furthermore, financial ratios like the Debt-to-Equity Ratio and Accounts Receivable Turnover were critical, further proving the significance of these indicators in the identification of the likelihood of improper financial statement presentation. The study also showed the computational efficiency of different ML models. The training time of the Decision Tree model was the shortest, at 30 seconds, in comparison to the Neural Network model of 560 seconds. XGboost and Random Forest have moderate training time of 204 and 128 seconds, respectively. However, these results would seem to indicate that while deep learning models are computationally expensive, their accuracy may still prove to be worthy when it comes to critical financial auditing situations. From a practical point of view, the ML model used for automated auditing should choose appropriate auditing process requirements. If the highest priority is high accuracy but we can live with longer computational times, a Network may be considered [18]. But if there is a need for an optimal balance between the accuracy and the quality without a loss of performance, then XGBoost or Random Forest is better. While less accurate than others, Decision Trees may still prove useful in the preliminary screening tasks since speed is prioritized over precision [19]. Although the results offer promise, numerous challenges need to be overcome in order for ML-based auditing to be widely used. The first major concern is the explainability and interpretability of complex ML models, in particular Neural Networks. Transparency is still required in decision-making processes for black-box models, which regulators and auditors need [20]. Future research can investigate how to enhance trust in automated audit outcomes using explainable AI. Another challenge is the potential bias in ML-based auditing. Since ML models are trained on historical financial data, a learned and propagated bias can carry bias inherent to historical financial data into a biased or inconsistent auditing decision [21]. This issue can be mitigated by ensuring diverse and representative training datasets in order to improve the robustness of audit models. Moreover, financial auditing also involves regulatory compliance, which is still very important. ML-driven auditing systems have to adhere to industry standards such as the International Financial Reporting Standards (IFRS) and Generally Accepted Accounting Principles (GAAP). In order for the ML models to be adopted in real auditing worlds, ML models need to be developed in a way that aligns with these regulatory frameworks. This study brings out the transformative potential of ML in automated auditing by virtue of increased accuracy and efficiency, and it also improves the capability of detecting fraud. Neural networks are used to achieve the highest accuracy, while XGBoost and Random Forest have a better balance between accuracy and computational efficiency and are suitable choices in practical applications. Yet, issues of model interpretability, bias, and regulatory compliance remain to be addressed to embrace ML in mainstream auditing practice fully. Thus, future research ought to be aimed at refining these models whilst producing quality, trustworthy automated auditing solutions that align with the changing requirements of the financial industry.

CONCLUSION

The investigation proved that machine learning (ML) technology provides opportunities for automatic audit improvements through better accuracy, together with increased efficiency and fraud-spotting capabilities. The evaluation of Decision Trees Random Forests XGBoost and Neural Networks as ML models revealed essential relationships between performance accuracy and processing speed. Neural Networks achieve the best accuracy rates; however, XGBoost and Random Forest deliver effective performance that works best for large-scale auditing needs. Total revenue, together with Net Profit Margin and Operating Expenses, emerge as fundamental financial variables for identifying anomalies according to feature importance analysis. The discovered information helps auditors determine which financial metrics require extra attention during their assessment of financial statements. Several barriers persist with ML-based auditing, including difficulties regarding model interpretability, bias concerns, and compliance requirements. Current models with excessive complexity, especially Neural Networks, demand explainable AI integration to establish trust in automated audit results because of their lack of transparency. The use of diverse training datasets enables discrimination reduction through fairness improvement of auditing decisions. The implementation of ML in auditing must follow essential regulatory elements as a primary factor. ML systems need to fulfill financial reporting standards like IFRS and GAAP for acceptance in actual auditing work environments. In the future, research needs to merge ML model compliance with regulatory needs and work on enhancing model dependability and resilience. ML-driven auditing represents an essential pathway for audit transformation through better accuracy and enhanced operational effectiveness. Widespread adoption of ML-based auditing requires proper model selection together with predictable interpretations and compliance with regulatory standards. The continuous development of modern auditing approaches using ML skills will reshape financial oversight practices by producing more transparent and reliable financial statements.

Funding
Key Project of Science and Technology of Chongqing Municipal Education Commission (Project No. KJZD-K202404201)

REFERENCES

[1] Internal Audit Division Office of Internal Oversight Services, “Audit Manual,” 2009. Accessed: Mar. 27, 2025. [Online]. Available: https://habnet.unhabitat.org/sites/default/files/documents/ Audit_Manual.pdf
[2] Y. Vero, “Audits Can Fail: Recognize the Most Common Pitfalls,” Trullion, Jan. 16, 2024. https://trullion.com/blog/audits-can-fail-recognize-the-most-common-pitfalls/
[3] Market Research Future, “AI in Accounting Market Size, Share Report, Growth 2034 |MRFR,” Marketresearchfuture.com, 2024. https://www.marketresearchfuture.com/reports/ai-in-accounting-market-22351 (accessed Mar. 27, 2025).
[4] A. Immadisetty, “Machine Learning for Real-Time Anomaly Detection,” 2024. Available: https://www.ijfmr.com/papers/2024/6/33087.pdf
[5] Mckinsey & Company, “The fight against money laundering: Machine learning is a game changer | McKinsey,” www.mckinsey.com, Oct. 07, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer
[6] M. Alles and G. L. Gray, “Incorporating big data in audits: Identifying inhibitors and a research agenda to address those inhibitors,” International Journal of Accounting Information Systems, vol. 22, pp. 44–59, Sep. 2016, doi: https://doi.org/10.1016/j.accinf.2016.07.004.
[7] B. Jendruszak, “The Total Opportunity Cost of Fraud is Bigger than You Think,” SEON, May 31, 2024. http://seon.io/resources/total-cost-of-fraud/ (accessed Mar. 27, 2025).
[8] R. Akula, N. Nguyen, and I. Garibay, “Supervised Machine Learning based Ensemble Model for Accurate Prediction of Type 2 Diabetes,” Apr. 2019, doi: https://doi.org/10.1109/southeastcon42311.2019.9020358.
[9] M. Huljanah, Z. Rustam, S. Utama, and T. Siswantining, “Feature Selection using Random Forest Classifier for Predicting Prostate Cancer,” IOP Conference Series: Materials Science and Engineering, vol. 546, p. 052031, Jun. 2019, doi: https://doi.org/10.1088/1757-899x/546/5/052031.
[10] A. A. Ali, A. M. Khedr, M. El-Bannany, and S. Kanakkayil, “A Powerful Predicting Model for Financial Statement Fraud Based on Optimized XGBoost Ensemble Learning Technique,” Applied Sciences, vol. 13, no. 4, p. 2272, Jan. 2023, doi: https://doi.org/10.3390/app13042272.
[11] Saif and S. S. Abu-Naser, “Neural Network-Based Audit Risk Prediction: A Comprehensive Study,” Philpapers.org, 2023. https://philpapers.org/rec/ALHNNA (accessed Mar. 27, 2025).

[12] PerClass, “perClass: Note on decision tree performance and speed,” Perclass.com, 2018. https://doc.perclass.com/perClass_Toolbox/kb/22.html (accessed Mar. 27, 2025).
[13] M. Schonlau and R. Y. Zou, “The random forest algorithm for statistical learning,” The Stata Journal: Promoting Communications on Statistics and Stata, vol. 20, no. 1, pp. 3–29, Mar. 2020, doi: https://doi.org/10.1177/1536867x20909688.
[14] D. Tarwidi, S. R. Pudjaprasetya, D. Adytia, and M. Apri, “An optimized XGBoost-based machine learning method for predicting wave run-up on a sloping beach,” MethodsX, vol. 10, p. 102119, Jan. 2023, doi: https://doi.org/10.1016/j.mex.2023.102119.
[15] Data Science, “Neural Network training time?,” Data Science Stack Exchange, 2017. https://datascience.stackexchange.com/questions/17504/neural-network-training-time
[16] G. Gutierrez, J. P. Llerena, L. Usero, and M. A. Patricio, “A Comparative Study of Convolutional Neural Network and Transformer Architectures for Drone Detection in Thermal Images,” Applied Sciences, vol. 15, no. 1, pp. 109–109, Dec. 2024, doi: https://doi.org/10.3390/app15010109.
[17] M. Imani, A. Beikmohammadi, and H. R. Arabnia, “Comprehensive Analysis of Random Forest and XGBoost Performance with SMOTE, ADASYN, and GNUS Under Varying Imbalance Levels,” Technologies, vol. 13, no. 3, p. 88, Feb. 2025, doi: https://doi.org/10.3390/technologies13030088.
[18] Y. Xu et al., “Artificial Intelligence: a Powerful Paradigm for Scientific Research,” The Innovation, vol. 2, no. 4, Oct. 2021, doi: https://doi.org/10.1016/j.xinn.2021.100179.
[19] V. Matzavela and E. Alepis, “Decision tree learning through a Predictive Model for Student Academic Performance in Intelligent M-Learning environments,” Computers and Education: Artificial Intelligence, vol. 2, p. 100035, Oct. 2021, doi: https://doi.org/10.1016/j.caeai.2021.100035.
[20] E. Ok, “Transparency in AI Decision-Making Processes,” ResearchGate, Jan. 29, 2025. https://www.researchgate.net/publication/388483007_Transparency_in_AI_Decision-Making_Processes
[21] M. Hanna et al., “Ethical and Bias Considerations in Artificial Intelligence (AI)/Machine Learning,” Modern Pathology, vol. 38, no. 3, p. 100686, Dec. 2024, doi: https://doi.org/10.1016/j.modpat.2024.100686.