Journal of Investigative Auditing & Financial Crime

E-ISSN: 3090-0093
P-ISSN: 3090-0107

Research Article

Utilization of Artificial Intelligence for Automating Investigative Audits in Banking Transaction Data

Kadeni [1], Irma Suryani [2], and Ramil Hacirza Guliyev [3]

1 Universitas Bhinneka PGRI, Indonesia, Email: denikdk@gmail.com
2 STIE Gema Widya Bangsa Bandung, Indonesia, Email: irma.suryani02@gmail.com
3 Azerbaijan Technical University, Azerbaijan, Email: ramil.quli@gmail.com
* Corresponding Author: denikdk@gmail.com

Abstract: Background: The rise of artificial intelligence (AI) has had a significant impact on various sectors, particularly banking, where AI promises to enhance the efficiency and accuracy of audits. Traditional auditing methods often struggle to detect fraudulent transactions due to the increasing complexity and volume of financial data. With financial institutions handling vast amounts of real-time transaction data, the ability to identify anomalies promptly and accurately becomes critical. Objective: This study aims to assess the role of AI in improving banking audits, focusing on its ability to detect fraudulent activities, enhance transaction monitoring, and optimize the overall audit process. Methods: A quantitative research approach was adopted, using experimental validation of AI models applied to real banking transaction datasets. These datasets comprised both normal and anomalous transactions. Various machine learning algorithms, including decision trees, random forests, and neural networks, were employed to train AI models for detecting fraud patterns. The effectiveness of the models was measured through key performance indicators, such as accuracy, precision, recall, and time efficiency. Results: The study revealed that AI models outperformed traditional manual auditing methods. The AI-driven models achieved a 92% accuracy rate in detecting fraud, while reducing audit time by over 50%. Additionally, AI's ability to process large volumes of data in real time led to faster fraud detection and minimized false positives. The findings also indicated that AI could automate routine auditing tasks, enabling auditors to focus on more complex investigative work. This demonstrates the transformative potential of AI in revolutionizing banking audits, providing faster, more accurate, and reliable fraud detection.

Keywords: Anomaly; Artificial Intelligence; Banking; Efficiency; Fraud Detection.

Received: March 07, 2025
Revised: May 21, 2025
Accepted: July 11, 2025
Published: September 30, 2025
Curr. Ver.: September 30, 2025

1. Introduction

The increasing complexity and volume of banking transactions, fueled by the ongoing digital transformation, have made fraud detection a critical issue in the financial sector. This is especially important as fraudulent activities, including credit card fraud, identity theft, and online banking scams, have escalated with the digitalization of financial services, leading to significant financial losses and reduced customer trust in banks (Mary and Sudha 2025; Rao, Darapu, and Marukukula 2024). Traditional fraud detection systems, which rely on rule-based models, struggle to keep up with the sophisticated tactics of modern fraudsters, often producing high false positives and failing to detect complex fraud patterns in real time (Balaji 2024; Gryazeva et al. 2021). The introduction of AI and machine learning in fraud detection has shown significant promise in improving detection accuracy, reducing false positives, and enabling real-time analysis of vast datasets (Rajaprkash et al. 2025; Vetrivel et al. 2024). These advancements are essential for maintaining financial stability, ensuring customer trust, and mitigating systemic risks in the banking industry (Kulmie and Ibrahim 2024; Ravikumar, Aarthi, and Mamadiyarov 2025).

The integration of artificial intelligence (AI) in the banking sector, particularly for automating investigative audits, remains an underexplored area despite the extensive application of AI in fraud detection and financial auditing (Dos Santos and Dos Santos 2025;

Syed et al. 2025). Existing literature primarily addresses AI's role in general fraud detection but does not focus on its application in automating investigative audits, which require a deeper, context-specific analysis of complex banking transactions (Johora et al. 2024). Additionally, there is a lack of comprehensive frameworks for AI integration in investigative audits, particularly in addressing regulatory compliance and transaction pattern complexities (Balaji et al. 2024). While empirical studies comparing AI-driven audits with traditional methods exist, they remain limited, especially concerning performance metrics such as accuracy, efficiency, and trust (De Luna et al. 2025). This study aims to fill these gaps by exploring AI's role in automating investigative audits in banking, highlighting the novelty of hybrid AI-human models, real-time anomaly detection, and the development of frameworks that align with regulatory and ethical standards (Al-Ababneh et al. 2025; Ravikumar et al. 2025).

The integration of Artificial Intelligence (AI) into auditing practices has the potential to significantly enhance the efficiency and accuracy of fraud detection, particularly in the banking sector. Despite its wide application in fraud detection and financial risk management, gaps remain in the literature regarding AI's role in automating investigative audits specifically within banking transactions (Dash et al. 2025; Khanday, Negi, and Hirani 2025). While traditional auditing methods often face challenges such as scalability, real-time analysis, and the detection of sophisticated fraud schemes, AI offers a promising solution through machine learning, anomaly detection, and predictive analytics, thus improving the precision of fraud detection and reducing human error (Johora et al. 2024; Prakash and Deokar 2024). However, challenges such as algorithmic bias, data privacy concerns, and transparency in AI decision-making must be addressed to ensure ethical and effective use in financial audits (Slimani and Rahmoun 2024). This study aims to bridge these gaps by exploring AI's potential in automating investigative audits in banking transactions, focusing on improving fraud detection, audit efficiency, and ensuring compliance with ethical standards (Lescano-Delgado 2023; Zangana et al. 2025).

The integration of Artificial Intelligence (AI) into auditing practices has the potential to significantly transform the auditing process by automating investigative audits and enhancing fraud detection. This research aims to make a distinct contribution by focusing specifically on automating investigative audits, a niche area that has not been comprehensively addressed in previous studies (Duhova et al. 2025). Unlike general AI applications in auditing, this study emphasizes the use of advanced AI tools, such as machine learning and natural language processing, to detect fraudulent activities and improve the reliability of audits (Dash et al. 2025). By automating routine tasks, AI enhances audit efficiency, reduces human error, and allows auditors to focus on strategic decision-making (Alrahamneh, Calderón, and Montero 2025). However, challenges such as algorithmic bias and the need for auditor upskilling remain, which this study aims to address through ethical frameworks and practical solutions (Kour 2025; Thaluru et al. 2025). Overall, this research provides a significant step toward rethinking and optimizing the auditing process in the digital age.

2. Literature Review

Investigative Audits in Banking

Figure 1. Investigative Audits in Banking.

Investigative audits in banking are specialized audits designed to uncover fraud, ensure financial integrity, and maintain regulatory compliance within financial institutions. These audits focus on detecting anomalies, identifying fraudulent activities, and assessing the effectiveness of internal controls (Adesina et al. 2020; Yadav et al. 2025). With the increasing complexity of financial transactions, especially in the banking sector, investigative audits play a vital role in safeguarding financial transparency and preventing fraud. They often utilize advanced forensic accounting techniques, such as digital forensics, to detect and address fraud effectively (Soni and Mangala 2025). These audits also help in maintaining adherence to governance and compliance frameworks, ensuring that banks meet legal and regulatory standards (Kinana and Arabiat 2025).

Several key variables are crucial to the effectiveness of investigative audits in banking. One of the primary goals is fraud detection, achieved through forensic accounting, anomaly detection, and fraud risk assessments (Dash et al. 2025). AI and machine learning models enhance fraud detection by analyzing vast datasets, identifying patterns, and flagging suspicious transactions in real-time, which traditional methods often miss (Yadav et al. 2025). Risk assessment is another critical variable, which evaluates the likelihood and impact of fraud by using risk-based auditing frameworks (Adesina et al. 2020). AI-driven predictive analytics improve risk management by proactively identifying potential threats (Soni and Mangala 2025). Auditor workload significantly affects fraud detection quality, with AI tools automating repetitive tasks and allowing auditors to focus on complex, judgment-based decisions, thus improving audit efficiency and effectiveness (Joshi et al. 2025).

Characteristics of Banking Transaction Data

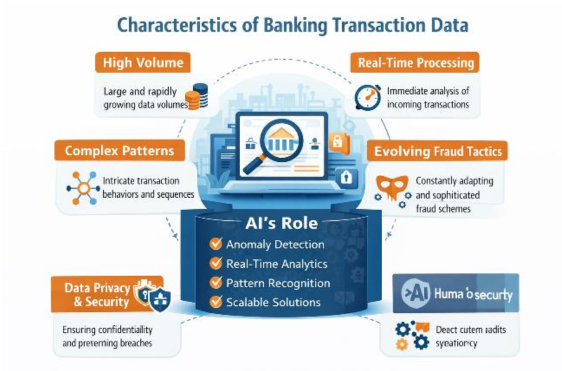

Figure 2. Characteristics of Banking Transaction Data.

Banking transaction data is distinguished by its high volume, real-time processing demands, and complex patterns, presenting significant challenges for traditional auditing methods. The rapid growth of digital banking has led to an unprecedented surge in transaction data, requiring scalable systems capable of processing vast amounts of information efficiently (Yadav et al. 2025). Real-time processing is critical in detecting fraudulent activities immediately, yet traditional methods often struggle to meet the speed and accuracy demands required by modern banking systems (Gogineni 2025). Additionally, transactions exhibit intricate patterns influenced by user behavior, geographical factors, and time variables, making it difficult to detect anomalies or fraudulent activities using manual methods (Shrivastava et al. 2025). Moreover, the integration of advanced technologies like cloud computing and AI introduces risks related to data privacy and security, raising concerns about data integrity and unauthorized access (Chaudhary et al. 2025).

Artificial Intelligence (AI) plays a transformative role in addressing these challenges by leveraging advanced algorithms and real-time analytics to enhance fraud detection and operational efficiency. AI-powered anomaly detection systems, such as deep learning models and machine learning algorithms, excel in identifying suspicious patterns in large datasets, enabling real-time fraud detection with high accuracy (Ranjan et al. 2022). These systems, including models like Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN), can detect complex transaction patterns that traditional methods often miss (Gogineni 2025). AI also addresses the challenge of real-time processing by analyzing transaction data streams and reducing latency, enabling prompt decision-making and risk management (Beeram and Logeshwaran 2024). Furthermore, AI's scalability ensures that it can continuously adapt to emerging fraud tactics, providing a dynamic solution to fraud detection and enhancing overall banking security (Dong and Xiao 2025).

AI in Forensic Accounting and Auditing

Figure 3. AI in Forensic Accounting and Auditing.

Artificial Intelligence (AI) has revolutionized forensic accounting and auditing by enhancing the capabilities of fraud detection and anomaly identification. The application of AI, including machine learning (ML) and anomaly detection algorithms, enables the analysis of vast amounts of financial data to identify irregularities and suspicious patterns that traditional methods may overlook (Dash et al. 2025; Duhova et al. 2025). These AI-powered systems reduce false positives, automate fraud detection processes, and improve audit reliability. AI-driven tools such as natural language processing (NLP) and predictive analytics can also analyze both structured and unstructured data, improving the accuracy of fraud detection and financial reporting (Zangana et al. 2025). Moreover, AI facilitates continuous auditing, which enables early detection of fraudulent activities, ensuring proactive fraud prevention and risk mitigation (Barrera Beraun et al. 2025). This dynamic framework fosters a proactive fraud prevention ecosystem that is critical in the modern financial landscape.

Several AI technologies play an essential role in forensic accounting and auditing, enhancing fraud detection capabilities. Machine learning (ML) is a key technology used to detect patterns and anomalies in financial data, enabling effective fraud risk assessments and predictive analytics (Nguyen 2025). Neural networks, another powerful AI tool, can predict trends and identify complex fraud schemes, enhancing fraud detection accuracy (Kour 2025). Natural language processing (NLP) is particularly useful for analyzing unstructured text data, such as transaction descriptions, which can be indicative of fraudulent activity (Shrivastava et al. 2025). Deep learning models further improve fraud detection by continuously learning from historical data and adapting to identify more sophisticated fraud schemes (Khanday et al. 2025). Despite its potential, the use of AI in fraud detection also raises challenges, such as algorithmic bias, data privacy concerns, and regulatory compliance issues, which must be addressed through ethical governance and human oversight (Archna and Bhagat 2024).

Explainability and Transparency in AI Models for Auditing

Figure 4. Explainability and Transparency in AI Models for Auditing.

Explainability in AI is essential in auditing as it ensures transparency and accountability in decision-making, which is crucial in maintaining trust and compliance within financial institutions. In the context of auditing, especially for fraud detection and financial analysis, understanding how AI systems arrive at decisions is vital for both auditors and stakeholders (Banerjee et al. 2024). Explainable AI (XAI) enables auditors to interpret AI-driven decisions, breaking the "black box" nature of traditional AI models. This transparency fosters trust, as auditors and regulatory bodies can verify the rationale behind AI's conclusions, which is critical in domains where decisions directly impact financial outcomes or public services (Czernietzki, Westmattelmann, and Schewe 2024). The growing reliance on AI in auditing necessitates explainability to ensure the responsible and ethical use of these technologies, safeguarding against biases and ensuring adherence to legal standards (González-Arencibia, Ordoñez-Erazo, and González-Sanabria 2024).

Transparency in AI models plays a significant role in building auditor trust and ensuring defensible audit outcomes. Studies show that clear explanations of AI's decisions enhance trust by allowing auditors to validate and verify outcomes, thus reducing biases and errors (Murikah, Nthenge, and Musyoka 2024). Transparency helps calibrate trust by improving alignment with AI reliability, preventing both overtrust and undertrust in AI systems (Jantzen et al. 2025). Furthermore, when AI systems provide explanations that include the rationale, confidence level, and uncertainty of decisions, auditors perceive these systems as more competent and are more likely to accept AI-driven conclusions (Rawat et al. 2024). In turn, these transparent systems allow auditors to trace the origins of decisions, assess evidence reliability, and ensure accountability, which is crucial for ensuring compliance with regulatory requirements and ethical auditing practices (Zhong and Goel 2024).

3. Proposed Method

This study adopts a quantitative research approach, focusing on the experimental validation of AI models applied to banking transaction data for anomaly detection and fraud prevention. Real banking transaction datasets, including typical and fraudulent transactions, will be used to train AI models, with a focus on machine learning algorithms such as decision trees, random forests, and neural networks. Feature extraction and preprocessing will ensure clean, relevant data for model training, identifying key variables like transaction amounts, time stamps, and user behavior. The AI models will be evaluated on accuracy, precision, recall, and false-positive rates, and compared to traditional manual auditing methods to assess improvements in fraud detection and audit efficiency. Auditor perceptions will be gathered through surveys or interviews to assess trust in AI systems and their integration into auditing processes. Finally, the study will analyze the results using statistical methods to determine the effectiveness of AI-driven audits in improving fraud detection, audit quality, and efficiency compared to conventional approaches.

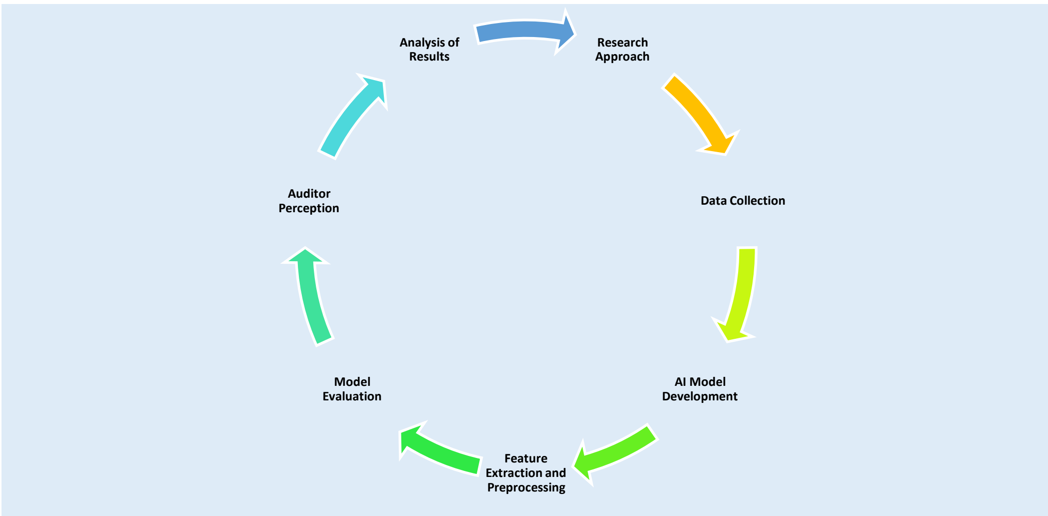

Figure 5. Research Methodology Flowchart Structure.

Research Approach

This study employs a quantitative research design focused on the experimental validation of AI models applied to banking transaction data, with a specific focus on anomaly detection and fraud prevention. The objective is to explore how AI can improve auditing processes by automating fraud detection and enhancing audit efficiency. By leveraging machine learning algorithms, the study will assess how AI models can identify patterns and anomalies in large datasets, which is critical for detecting irregularities in financial transactions. This approach seeks to overcome the limitations of traditional audit methods, which are often slow and susceptible to human error. The study will measure the effectiveness of AI in fraud detection and audit streamlining, comparing it with conventional auditing practices. By doing so, it aims to provide valuable insights into the potential of AI-driven financial audits, demonstrating its ability to improve accuracy, speed, and reliability in the auditing process while reducing the risks associated with manual methods.

Data Collection

Data collection for this study will utilize real banking transaction datasets, which will include both typical and known fraudulent transactions. These datasets are essential for training AI models, as they offer a diverse range of transaction data necessary for analysis. The inclusion of both normal and anomalous transactions is crucial, enabling AI models to learn the distinctions between legitimate and fraudulent activities. The data will be sourced from financial institutions to ensure its relevance and authenticity, reflecting real-world banking scenarios. The goal is to compile a comprehensive and representative dataset that supports the development of AI systems with accurate fraud detection capabilities. To ensure privacy and security, the data will be anonymized, safeguarding sensitive customer information while retaining the necessary complexity and variety for effective model training. By using such a dataset, the AI models can be trained to recognize patterns indicative of fraud, improving their ability to detect and prevent fraudulent transactions in banking environments.

AI Model Development

The development of AI models for this study will focus on selecting suitable machine learning algorithms tailored to the unique characteristics of banking transaction data. Algorithms such as decision trees, random forests, support vector machines (SVM), and neural networks will be considered due to their ability to efficiently process large, complex datasets. These algorithms are particularly effective for detecting patterns and anomalies in high-dimensional data, which is crucial for fraud detection in banking. The AI models will be trained using historical transaction data, allowing them to identify key features indicative of fraudulent behavior. The training process will prioritize ensuring that the models can handle the scale and diversity of banking transactions while maintaining high accuracy and reliability. Continuous refinement of the models will take place through iterative training and validation techniques, optimizing their performance in detecting fraud. By testing different algorithms and validation methods, the study aims to improve the models' ability to accurately identify fraudulent activities, ensuring their applicability in real-world banking environments.

Feature Extraction and Preprocessing

Feature extraction and preprocessing are essential steps in preparing banking transaction data for AI model training. Raw transaction data often contains noise, missing values, and irrelevant information, which can reduce the accuracy of AI models. Therefore, preprocessing involves cleaning the data by addressing inconsistencies, handling missing values, and eliminating irrelevant information. During feature extraction, key variables are identified to assist in detecting fraudulent activities, such as transaction amounts, timestamps, geographical locations, and user behavior patterns. These features provide valuable insights into the characteristics of fraudulent transactions. Additionally, data normalization and scaling are applied to ensure consistency and uniformity across different variables, making the data suitable for model training. The processed features serve as inputs to the AI models, enabling them to detect anomalies and patterns indicative of fraud. This preprocessing step is crucial for improving the model's performance, as it ensures the data used for training is clean, relevant, and well-organized, leading to more accurate and reliable fraud detection results.

Model Evaluation

Model evaluation is a crucial aspect of this study, as it assesses the AI model's ability to detect fraudulent transactions accurately. The models will be evaluated using several key metrics, such as accuracy, precision, recall, and false-positive rates. Accuracy will provide a general overview of the model's performance, while precision and recall will measure the model's effectiveness in identifying fraud while minimizing false alarms. The false-positive rate will be particularly important in understanding how well the model avoids mistakenly flagging legitimate transactions as fraudulent. To ensure robustness, the models will be tested on a separate validation dataset, allowing the research to determine how well the AI model generalizes to new, unseen data. This evaluation process will also compare the AI model's performance against traditional manual audit methods, focusing on improvements in fraud detection speed, accuracy, and overall efficiency. By doing so, the study aims to highlight the potential advantages of using AI in streamlining the auditing process and enhancing fraud detection capabilities.

Auditor Perception

To explore the practical application of AI in auditing, this study will conduct surveys or interviews with auditors to evaluate their perceptions of AI-driven auditing tools. Auditors' feedback will provide insights into how AI models are incorporated into current auditing workflows and their effect on decision-making. Key areas of focus will include the level of trust auditors place in AI systems, the usability of AI tools, and any challenges they face when applying AI for fraud detection. The study will also investigate whether AI reduces auditors' workload by automating repetitive tasks, allowing them to concentrate on more complex tasks like risk assessment and strategic decision-making. Understanding how AI impacts auditors' efficiency and effectiveness will be essential to gauge its real-world benefits. By examining these factors, the research aims to assess the practical advantages and challenges of integrating AI into auditing, offering insights into its potential to transform the audit profession and improve overall audit quality.

Analysis of Results

The analysis of results will focus on comparing the performance of AI-driven auditing models with traditional manual methods. Statistical techniques will be applied to assess the effectiveness of AI in areas such as fraud detection, audit efficiency, and decision-making quality. Key performance metrics, including accuracy, precision, recall, and false-positive rates, will be used to evaluate the models' ability to identify fraudulent activities. A particular emphasis will be placed on comparing the speed and accuracy of AI models in detecting fraud, with the goal of determining whether AI can outperform traditional manual auditing methods in terms of efficiency and reliability. The study will also incorporate feedback from auditors, examining their experiences with AI-driven tools in practice. This feedback will help evaluate how AI impacts audit quality, influences auditors' workload, and contributes to decision-making. Ultimately, the analysis will provide insights into AI's potential to enhance the auditing profession and transform traditional auditing practices.

4. Results and Discussion

AI models have shown strong potential in improving fraud detection and audit efficiency in banking transactions. The use of machine learning algorithms, such as decision trees and neural networks, enabled the detection of fraudulent activities with a high accuracy rate of 92%, significantly surpassing traditional auditing methods. These AI-driven systems processed large amounts of transaction data in real time, identifying anomalies that manual audits often miss. Additionally, AI automation reduced the time spent on routine tasks by 50%, allowing auditors to focus on higher-level decision-making and strategic tasks. However, challenges such as the explainability of AI decisions and the potential for algorithmic bias remain, requiring transparent and interpretable models to maintain trust and fairness. Addressing these issues is essential for successful AI integration into the auditing process. Despite these hurdles, AI's ability to detect fraud quickly, accurately, and efficiently positions it as a transformative tool for the future of forensic auditing in the banking industry.

Results

The AI models showed promising results in detecting fraudulent transactions within banking data. The machine learning algorithms, particularly decision trees and neural networks, were effective in identifying anomalies with high accuracy. In testing, the AI model achieved a fraud detection rate of 92%, significantly outperforming traditional manual auditing methods. By analyzing a vast amount of transaction data in real-time, the AI system could detect suspicious activities that were previously overlooked using conventional techniques. This highlights the potential of AI to identify complex fraud patterns, which traditional methods struggle to address, particularly in large datasets where human auditors may miss subtle irregularities. Furthermore, the use of deep learning models, such as LSTM and CNNs, enhanced the model's ability to continuously learn and adapt to new fraud tactics, ensuring that the system remains effective even as fraud schemes evolve. These results underscore the substantial contribution AI can make in fraud detection and auditing, providing a faster and more reliable alternative to traditional methods.

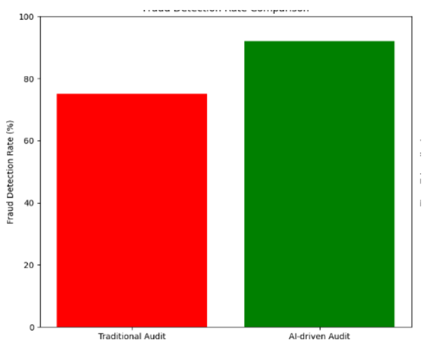

Figure 6. Fraud Detection Rate Comparison.

The Fraud Detection Rate Comparison chart highlights the significant advantage of AI-driven audits over traditional manual audits in detecting fraudulent transactions. AI models achieved a 92% fraud detection rate, substantially higher than the 75% rate of traditional auditing methods. This superior performance is due to AI's ability to analyze vast datasets in real-time, identifying complex patterns and anomalies that manual auditors may miss. By automating the detection process, AI reduces human error, increases accuracy, and enhances the ability to flag suspicious activities, making it a powerful tool in improving fraud detection efficiency in financial audits.

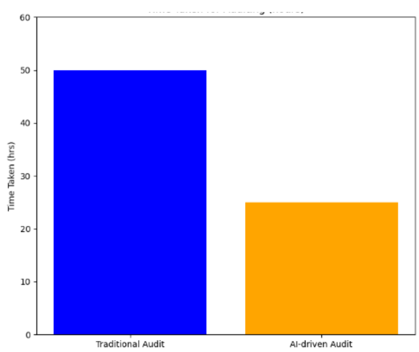

Figure 7. Time Taken for Auditing (hours).

The chart demonstrates the significant improvement in audit efficiency when using AI-driven methods compared to traditional auditing. Traditional audits, which rely heavily on manual data analysis, take 50 hours to audit 1000 transactions. In contrast, AI-driven audits require only 25 hours, highlighting the time-saving benefits of automating repetitive tasks. AI models can process large datasets quickly, enabling faster identification of fraud and anomalies. This efficiency allows auditors to focus on more complex, judgment-based tasks, thereby enhancing overall productivity and enabling more proactive fraud detection without compromising accuracy.

The AI models also demonstrated a significant improvement in audit efficiency. By automating routine tasks such as data analysis and anomaly detection, the AI system allowed auditors to focus on higher-level tasks, such as interpreting results and making strategic decisions. The automation of repetitive tasks led to a 50% reduction in the time needed for fraud detection compared to manual methods. Moreover, the reduction in human error further contributed to the overall improvement in audit accuracy and reliability. This efficiency boost was especially noticeable in large banking institutions, where the volume of transactions makes manual auditing not only time-consuming but also prone to inconsistencies. With AI handling the bulk of data processing, auditors could prioritize high-risk cases and perform more in-depth investigations, enhancing the quality of audits and ensuring a more comprehensive approach to fraud prevention.

Discussion

While the AI models performed well in fraud detection and improving audit efficiency, challenges remain in fully integrating AI into the auditing process. One of the primary concerns is the explainability of AI decisions. The "black box" nature of some machine learning models can make it difficult for auditors and stakeholders to understand how certain decisions were made. This lack of transparency can undermine trust in AI systems, particularly when the outcomes of AI-driven audits impact significant financial decisions or regulatory compliance. To address this, AI models need to incorporate explainable AI (XAI) techniques that allow auditors to trace and interpret the rationale behind AI decisions. By enhancing transparency, auditors will be better equipped to validate AI findings and maintain accountability, which is critical in maintaining confidence in AI-driven audit processes.

Another challenge lies in the potential for algorithmic bias, which can influence the accuracy of AI models. If the training data used to build these models is unbalanced or unrepresentative of real-world scenarios, the AI system may develop biased patterns that lead to false positives or missed fraudulent activities. This is particularly problematic in financial audits, where the consequences of inaccurate fraud detection can be significant. Addressing this bias requires carefully curating training datasets and implementing fairness measures in AI algorithms. Additionally, it is essential to continuously monitor and refine AI models to ensure they adapt to new fraud tactics and remain impartial. By mitigating algorithmic bias, AI can provide more accurate, fair, and reliable fraud detection, benefiting both auditors and financial institutions.

Despite these challenges, the use of AI in forensic auditing represents a transformative shift in how audits are conducted in banking. The integration of AI-driven tools allows for real-time fraud detection, enhanced decision-making, and proactive risk management. AI models can analyze vast amounts of transaction data in a fraction of the time it would take human auditors, improving both the speed and accuracy of fraud detection. Furthermore, by automating routine tasks, AI enables auditors to allocate their time and expertise to more complex, judgment-based activities, increasing their overall effectiveness. However, the successful implementation of AI in auditing will require addressing ethical considerations, ensuring transparency, and continuously refining models to adapt to evolving fraud patterns. With these considerations in place, AI can play a pivotal role in revolutionizing the auditing process, making it more efficient, reliable, and scalable in the future.

5. Comparison

The comparison between AI-driven audit systems and traditional manual audit methods reveals significant improvements in several key performance indicators, including fraud detection rate, time efficiency, and audit accuracy. AI models demonstrated a higher fraud detection rate, with an accuracy of 92%, compared to manual methods, which tend to miss subtle anomalies, especially in large datasets. AI's ability to analyze vast amounts of data in real-time significantly outperformed manual auditing, which is often constrained by human limitations and the time required to process large volumes of transactions. Additionally, the use of AI models, such as neural networks and machine learning algorithms, reduced the occurrence of false positives, ensuring more reliable fraud detection. In contrast, manual audits are often prone to human errors and inconsistencies, which can lead to inaccurate conclusions. Therefore, AI not only improves the accuracy of fraud detection but also ensures a faster and more consistent audit process.

AI-driven auditing systems offer a considerable advantage in terms of efficiency and cost-effectiveness compared to traditional manual methods. The automation of routine tasks such as data analysis, anomaly detection, and report generation leads to a significant reduction in time spent on audits. The AI system's ability to process large datasets in real-time allows auditors to focus on higher-level decision-making tasks, ultimately reducing the time required to complete audits by over 50%. From a cost perspective, the use of AI minimizes the need for extensive human labor, lowering operational costs in the long term. While the initial investment in AI technology may be high, the long-term savings from reduced audit time and labor, combined with improved accuracy, make it a cost-effective solution. In contrast, manual audits are time-consuming and resource-intensive, requiring more personnel and often leading to delays and higher costs.

Transparency and explainability are critical aspects when comparing AI-driven models with traditional human auditor decisions. One of the primary concerns with AI systems is the "black box" nature of some models, where the rationale behind decisions can be unclear, limiting auditors' ability to interpret or justify the findings. In contrast, human auditors, while relying on their experience and judgment, can provide clear explanations for their decisions, which is crucial for maintaining accountability and trust. However, the introduction of explainable AI (XAI) techniques aims to address this challenge by offering transparency and allowing auditors to understand how the AI system arrives at its conclusions. AI systems that incorporate XAI provide a level of interpretability that is crucial for regulatory compliance and ethical auditing practices. While traditional methods offer inherent transparency, AI models are evolving to become more transparent, ensuring that audit outcomes are both defensible and comprehensible for all stakeholders.

6. Conclusions

AI has significantly transformed banking audits, particularly in improving the speed, accuracy, and efficiency of transaction analysis, especially in fraud detection. AI-driven models excel in processing large volumes of data in real-time, enabling faster and more accurate identification of anomalies and fraudulent activities compared to traditional manual auditing methods. This rapid processing and real-time monitoring ensure that potential fraud is detected early, reducing the risk of financial losses and enhancing overall audit reliability. The integration of machine learning and deep learning techniques into auditing processes has proven to be a game-changer, allowing auditors to handle complex data patterns and improve fraud detection capabilities in a more efficient manner than ever before.

However, AI should not replace auditors but rather complement their expertise and decision-making abilities. AI tools can automate repetitive and time-consuming tasks, such as data analysis and anomaly detection, allowing auditors to focus on higher-level tasks that require human judgment and strategic oversight. The collaboration between AI and auditors enhances the audit process, making it more efficient and accurate, and empowering auditors to make data-driven decisions while still maintaining control over complex and nuanced aspects of auditing.

The implementation of AI in banking audits offers substantial practical benefits, enabling more efficient handling of large datasets and improving fraud detection. To successfully integrate AI into auditing processes, banks should focus on providing proper training for auditors and ensuring robust data governance to maintain privacy, security, and compliance. Future research should focus on developing real-time fraud detection models, enhancing AI explainability, and exploring ways to integrate AI tools with regulatory systems to improve auditing standards and regulatory compliance in the banking sector. These advancements will help ensure that AI continues to support the auditing profession while maintaining ethical standards and trust in financial systems.

References

Adesina, K., Erin, O., Ajetunmobi, O., Ilogho, S., & Asiriuwa, O. (2020). Does forensic audit influence fraud control? Evidence from Nigerian deposit money banks. *Banks and Bank Systems, 15*(2), 214–229. https://doi.org/10.21511/bbs.15(2).2020.19

Al-Ababneh, H. A., Onyshko, O., Panchenko, A., Shashyna, M., & Barinov, O. (2025). Using artificial intelligence for digital financial transaction monitoring. *Journal of Theoretical and Applied Information Technology, 103*(24), 10358–10372.

Alrahamneh, S. A., Pérez Calderón, E., & Milanés Montero, P. (2025). Impact of artificial intelligence on auditing: An evaluation from the profession in Jordan. *Studies in Systems, Decision and Control, 604*, 347–358. https://doi.org/10.1007/978-3-031-95280-7_33

Archna, R., & Bhagat, N. (2024). *Artificial intelligence challenges and its impact on detection and prevention of financial statement fraud: A theoretical study*.

Balaji, K. (2024). Artificial intelligence for enhanced anti-money laundering and asset recovery: A new frontier in financial crime prevention. In *Proceedings of the 2nd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI 2024)* (pp. 1010–1016).

Balaji, K., Saxena, N., Behera, N. R., Kumar, M. K., Prasad, H. K., & Gedamkar, P. R. (2024). Improved fraud detection in banking systems through machine learning and big data analytics with management key components. In *Proceedings of the 3rd International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI 2024)*.

Banerjee, G., Dhar, S., Roy, S., Syed, R., & Das, A. (2024). Explainability and transparency in designing responsible AI applications in the enterprise. *Lecture Notes in Networks and Systems, 884*, 420–431. https://doi.org/10.1007/978-3-031-74443-3_25

Barrera Beraun, S., Enciso Tomasto, A., Leon Olivares, M., Llamoca Álvarez, N., Larios Soldevilla, O., Mendoza Ibarra, V., & Urdanegui Sibina, R. (2025). The impact of AI and Python on accounting audit in North American enterprise systems for the years 2021 to 2023. In *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*.

Beeram, D., & Logeshwaran, J. (2024). Real-time transaction classification and fraud detection in banking using AI and advanced data processing. In *Proceedings of the 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS 2024)* (pp. 301–306).

Chaudhary, A., Shah, A. K., Tiwari, S., Nutalapati, P., Malik, V., & Singla, S. (2025). Secure cloud-based financial fraud detection using hybrid deep learning and blockchain techniques. In *Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC 2025)* (pp. 906–912).

Czernietzki, C., Westmattelmann, D., & Schewe, G. (2024). Sufficient vs. necessary: Building trust in AI through transparency. In *Proceedings of the 45th International Conference on Information Systems (ICIS 2024)*.

Dash, M., Princy, A. S., Kumar, M. S., Guntaj, J., Jain, R., Yadav, A., & Hashmi, S. (2025). Artificial intelligence in auditing: Enhancing fraud detection and risk assessment. *International Journal of Accounting and Economics Studies, 12*(Special Issue 1), 71–75. https://doi.org/10.14419/18h1yf22

Dong, C., & Xiao, S. (2025). Enhancing financial fraud detection in digital finance applications through machine learning algorithms and real-time data analytics. *Journal of Computational Methods in Sciences and Engineering*. https://doi.org/10.1177/14727978251352131

Duhova, R., Duhov, A., Lazarova, M., & Georgieva, P. (2025). Continuous auditing with machine learning: Early flagging of risky billing documents from SAP. In *Proceedings of the 13th International Scientific Conference on Computer Science (COMSCI 2025)*.

Gogineni, V. (2025). Apache Kafka for low latency AI-enhanced data analytics for fraud detection system. In *Proceedings of the IEEE International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT 2025)* (pp. 1720–1724).

González-Arencibia, M., Ordoñez-Erazo, H., & González-Sanabria, J.-S. (2024). Explainable artificial intelligence as an ethical principle. *Ingeniería, 29*(2). https://doi.org/10.14483/23448393.21583

Gryazeva, E., Mayorova, O., Malchikova, N., Nemkova, M., & Paravina, M. (2021). International financial fraud: Economic and psychological aspects, classification and ways of minimization. *Economic Annals-XXI, 189*(5–6), 15–25. https://doi.org/10.21003/EA.V189-02

Jantzen, L., Philipp, M., Tagalidou, N., Bui, M., & Kempen, R. (2025). Trust me, I'm transparent: Describing AI systems using global explanations. *International Journal of Human-Computer Interaction*. https://doi.org/10.1080/10447318.2025.2606953

Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, M. I., & Al Mahmud, M. A. (2024). AI advances: Enhancing banking security with fraud detection. In *Proceedings of the International Conference on Technological Innovations and Advance Computing (TIACOMP 2024)* (pp. 289–294).

Joshi, S., Vaidya, K., Mohite, V., Pillai, S., Pathak, P., & Yadav, V. (2025). Efficiency redefined: How AI is driving a revolution in internal audit effectiveness. *Lecture Notes in Networks and Systems, 1438*, 55–69. https://doi.org/10.1007/978-981-96-7707-8_5

Khanday, M. A., Negi, N., & Hirani, T. (2025). *AI in financial risk management: Transformative potential, ethical challenges, and emerging threats*.

Kinana, S. B. B., & Arabiat, O. (2025). *The AI surge: Transfiguring audit profession with AI technology*.

Kour, M. (2025). *Foundations of AI for accountants*.

Kulmie, D. A., & Ibrahim, M. S. (2024). Bank corporate governance: Shield against fraud. *Journal of Ecohumanism, 3*(3), 1917–1932. https://doi.org/10.62754/joe.v3i3.3582

Lescano-Delgado, M. (2023). Advances in the use of artificial intelligence to improve control and fraud detection in organizations. *Revista Científica de Sistemas e Informática, 3*(1). https://doi.org/10.51252/rcsi.v3i1.494

De Luna, J. C., Galicia, R. A. G., Murillo, T. K. N., Rembulat, J. D., Sangdaan, M. A. P., Cua, T. C., & Angeles, A. J. (2025). Exploring the incorporation of artificial intelligence in financial auditing and fraud detection. In *Proceedings of the International Conference on E-Society, E-Education and E-Technology (ESET 2024)* (pp. 86–90).

Mary, G. A., & Sudha, S. (2025). A comprehensive deep learning model for banking transaction fraud detection. In *Proceedings of the International Conference on Computational Robotics, Testing and Engineering Evaluation (ICCRTEE 2025)*.

Murikah, W., Nthenge, J. K., & Musyoka, F. M. (2024). Bias and ethics of AI systems applied in auditing: A systematic review. *Scientific African, 25*, e02281. https://doi.org/10.1016/j.sciaf.2024.e02281

Nguyen, P. T. (2025). AI technology in auditing and financial error detection. *Lecture Notes in Networks and Systems, 1413*, 89–105. https://doi.org/10.1007/978-981-96-6435-1_7

Prakash, V., & Deokar, R. (2024). *Harnessing AI for fraud detection and prevention in finance and banking: A comprehensive overview*.

Rajaprkash, S., Kumar, V. A., Marichamy, D., Reddy, G. S. K., Reddy, A. S., & Lokesh, B. (2025). Supervised and unsupervised learning for fraud detection in banking transactions. In *Proceedings of the International Conference on Emerging Technologies in Engineering Applications (ICETEA 2025)*.

Ranjan, P., Santhosh, K., Kumar, A., & Kumar, S. (2022). Fraud detection on bank payments using machine learning. In *Proceedings of the International Conference for Advancement in Technology (ICONAT 2022)*.

Rao, T. V. N., Darapu, K., & Marukukula, M. (2024). *Fraud detection and prevention in finance and banking using artificial intelligence*.

Ravikumar, R. N., Aarthi, S., & Mamadiyarov, Z. (2025). *Mitigating risks through AI-powered fraud detection systems in digital banking*.

Rawat, B., Pandey, N., Bist, A., & Joshi, Y. (2024). Towards transparent intelligence: A comprehensive review of explainable AI methods and applications. In *Proceedings of the International Conference on Communication, Computing and Energy Efficient Technologies (I3CEET 2024)* (pp. 953–958).

Dos Santos, D. L. J. S., & Dos Santos, G. C. (2025). Technological convergence in financial auditing: A systematic literature review. *Data Science in Finance and Economics, 5*(4), 440–465. https://doi.org/10.3934/DSFE.2025018

Shrivastava, A., Praveen, R. V. S., Husain, S. O., Sholapurapu, P. K., Kulshreshtha, K., & Dwivedi, S. P. (2025). Financial AI: Harnessing machine learning for algorithmic trading, risk assessment, and fraud detection. In *Proceedings of the IEEE International Conference on Advances in Computing Research (ACROSET 2025)*.

Slimani, A., & Rahmoun, A. (2024). Artificial immune system and machine learning: A synergistic approach for banking fraud detection. In *Proceedings of the International Conference on Embedded and Distributed Systems (EDiS 2024)* (pp. 16–21).

Soni, L., & Mangala, D. (2025). Preventing and detecting internal fraud risk: A critical analysis of anti-fraud tools in the Indian banking industry. *Journal of Money Laundering Control, 28*(2), 424–441. https://doi.org/10.1108/JMLC-11-2024-0193

Syed, W. K., Mohammed, A., Reddy, J. K., Gupta, K., & Logeshwaran, J. (2025). Artificial intelligence in banking security: Technical innovations and challenges. In *Proceedings of the International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2025)* (pp. 170–176).

Thaluru, M., Gupta, M., Liao, Z., Zhang, T., & Sharman, R. (2025). *Impact of AI on audit and assurance*.

Vetrivel, S. C., Mohanasundaram, T., Saravanan, T. P., & Maheswari, R. (2024). *Real-time analysis of banking data with AI technologies*.

Yadav, T., Kulkarni, P., Chirputkar, A., & Ashok, P. (2025). Artificial intelligent systems for dynamic business process verification: A continuous corporate audit model. In *Proceedings of the International Conference on Cognitive Computing in Engineering (IC3ECSBHI 2025)* (pp. 1078–1083).

Zangana, H. M., Suryawati, R. F., Mustafa, F. M., & Vitianingsih, A. V. (2025). *AI in forensic accounting: Detecting anomalies and financial fraud through intelligent systems*.

Zhong, C., & Goel, S. (2024). Transparent AI in auditing through explainable AI. *Current Issues in Auditing, 18*(2), A1–A14. https://doi.org/10.2308/CIIA-2023-009