Mantik Journal, 9 (1) (2025), ISSN 2685-4236 (Online)

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik

Enhancing fraud prevention with artificial intelligence in accounting systems: A case study of e-fishery

Nano Suyatna
Department of Computerized Accounting, Faculty of Computer, Ma'soem University, Indonesia

A R T I C L E I N F O

Article history:

Received Apr 23, 2025
Revised Apr 29, 2025
Accepted May 14, 2025

Keywords:

Accounting Systems;
Automated general journal;
Artificial Intelligence;
Fraud Detection;
Revenue Inflation.

ABSTRACT

Fraud in accounting records, particularly income inflation, poses a significant risk to companies, affecting credibility, investment decisions, and legal compliance. Despite using the double-entry system, financial statement manipulation can still occur, creating an illusion of higher profitability. This study explores how Artificial Intelligence (AI) in Accounting Information Systems can more effectively prevent income inflation and detect fraud than traditional methods. A case study of e-Fishery highlights AI's role in identifying fraud through anomaly detection and automated general journal verification. AI-based audits, such as those using Isolation Forest, significantly improve efficiency by automating repetitive tasks and enabling real-time data analysis, reducing the time and resources required for audits. The research results indicate that 68% of respondents preferred the automated audit approach. The Isolation Forest algorithm resulted in a detection accuracy of 26%, while Autoencoder improved the accuracy to 33.6%. These findings demonstrate that AI in Accounting Information Systems enhances fraud prevention, improves financial reporting accuracy, and addresses challenges traditional methods fail to identify.

Corresponding Author:

Nano Suyatna,
Department of Computerized Accounting/Faculty of Computer, Ma'soem University,
Griya Bandung Asri 2 Blok F5 No.20, Bandung, West Java, 40287, Indonesia.
Email: nanosuyatna@yahoo.com

1. INTRODUCTION

Fraud in accounting records, particularly revenue inflation, presents a significant risk for companies. Even though companies implement the double-entry bookkeeping system, financial statement manipulation can still occur, often creating the illusion that a company is more profitable than it actually is (Umi Zakiyatun Khasanah, 2025; Wanua.Id, 2025). This can impact investment decisions, the company's credibility, and legal compliance (Hardiantoro & Adhi, 2025). Inflating Feed Facilities (Assets) (Hakim, 2025) and manipulating losses into profits (Setyowati, 2025). further complicate the situation. While the Accounting Information System (AIS) is crucial for documenting financial transactions systematically, traditional systems often fail to detect fraud effectively (Meiryani et al., 2023). Optimizing AIS with Artificial Intelligence (AI) offers a promising solution for improving the accuracy, transparency, and security of transactions, as AI can automate fraud detection and payment verification. According to

Purrushottam((2025), Machine learning algorithms like CNN analyze transaction patterns to detect fraud in real-time, improving the accuracy of financial reports and spotting unauthorized transactions. This study explores how AI in Accounting Information Systems can better prevent income inflation and fraud compared to traditional methods. By integrating anomaly detection, automated journal verification, and stronger access controls, AI helps reduce fraud risks and ensure accurate financial records. The study offers valuable insights into how AI-driven accounting systems can enhance fraud prevention and the reliability of financial reporting in companies.

AI boosts accounting accuracy by automating data entry and bookkeeping, reducing human errors, and improving efficiency. By analyzing large data sets, AI can identify trends and risks that may lead to income inflation, helping with better financial planning and fraud detection(V. M. et al., 2024). AI enhances the reliability of accounting information by providing more accurate financial data, which can help reduce income inflation. It increases efficiency and reduces fraud, resulting in more accurate financial reporting. However, it also tackles challenges like technical risks and unclear accountability, which could impact overall accuracy(Liang & Wu, 2022).

AI is integrated into Accounting Information Systems (AIS) to address issues like income inflation and fraud, which are often overlooked by traditional methods. This study focuses on the accounting challenges caused by income inflation, affecting investment decisions and legal compliance, and shows how AI, particularly through machine learning, can better detect fraud. AI uses anomaly detection to identify unusual journal entries and transactions, along with automated verification to ensure only legitimate transactions are recorded. By using Convolutional Neural Networks (CNN), AI can analyze transaction patterns in real-time to spot fraud that traditional systems might miss. Additionally, AI improves system security with stricter access controls, ensuring that only authorized users can modify financial data, reducing the risk of financial manipulation. This makes AI not only faster at detecting fraud but also enhances the accuracy and transparency of financial reporting.

2. RESEARCH METHOD

This study uses a case study approach to examine how AI-integrated Accounting Information Systems (AIS) are used for fraud detection and account verification. The method focuses on identifying fraudulent accounts in financial statements, particularly through anomaly detection and automatic payment verification using AI. The main goal of the research is to assess the effectiveness of AI-enhanced AIS in detecting fraud and ensuring data accuracy by using anomaly detection, automated journal input verification, and controlled journal entry access. The research employs a case study and detection method to explore how AI in AIS helps detect fraud and verify accounts, improving the accuracy of financial data.

2.1 Research Type

This study adopts a case study approach to explore how an Accounting Information System (AIS) integrated with Artificial Intelligence (AI) is applied in an aquaculture company and a startup to detect fraud and verify relevant accounts. The main objective is to examine how AI integration enhances AIS's capability in fraud prevention and ensuring financial data accuracy, along with exploring the associated challenges and benefits (Roszkowska, 2020). (a) Detection Methodology: This approach identifies accounts showing signs of fraud in financial statements. It is important because many companies manipulate financial data in ways that adhere to accounting principles, making fraud detection difficult for those without forensic accounting expertise (Kim et al., 2008). (b) Anomaly Detection and Automatic General Journal Input Verification: This process identifies unusual patterns in financial transactions

within accounting systems, especially for standard accounts involved in transactions. AI-driven techniques detect anomalies and automatically verify the accuracy of journal entries, ensuring that they align with pre-established rules and account pairings. This improves the consistency and reliability of financial data, reducing errors and fraud (Chandola et al., 2009).

2.2 Case Selection

Criteria for selecting the case study: (a) Use of Advanced Accounting Information Systems: eFishery uses a tech-based platform to manage operational and financial data. The AI-integrated AIS is key in detecting fraud and ensuring accurate financial transactions. (b) Data Management and Financial Security: eFishery automates fish feeding and optimizes data for better results. It handles large volumes of data, making it relevant for studying AI's role in improving data security and detecting manipulation. (c) Effectiveness of AI in Fraud Detection: eFishery is an example of AI being used to detect fraud in financial management. The study will assess how well AI-integrated AIS identifies anomalies and ensures financial report accuracy. (d) Complexity of Financial System Management in Tech Companies: As a company blending advanced technology with the fisheries industry, eFishery faces complex financial management issues. This study will explore how AI-integrated AIS simplifies financial management and reduces errors or fraud.

2.3 Data Collection Techniques

Documentation: The study will gather documents related to AI-integrated AIS use, such as audit reports, transaction data, and fraud detection logs. Additionally, web-based sources like technology news websites (e.g., teknologi.id, CNBC Indonesia) will provide real-world applications and case studies for validation.

2.4 Data Analysis Techniques

For qualitative analysis, thematic analysis will categorize interview and observational data, identifying patterns in AI's use within AIS and fraud detection. (a) Quantitative analysis will include statistical tests on financial transaction data to assess AI's impact on financial report accuracy. Data triangulation will cross-verify interview, observational, and documentary information to ensure result validity. (b) Data Validation: Data from technology news websites will be cross-referenced with fraud detection reports and AI system logs to ensure credibility. Convergent validity will be tested by comparing fraud cases in the articles with actual audit reports from third-party auditors. Longitudinal reliability will be assessed by evaluating AI's performance across multiple business cycles.

2.5 Analysis of Results

The results from the anomaly detection and access restriction features will be analyzed for their effectiveness in fraud prevention. Success will be measured by comparing the number of fraud cases detected before and after AI implementation. Similarly, the effectiveness of the journal entry access control system will be measured by evaluating unauthorized changes to financial records.

The following is a scheme or visualization of the stages of AI integration into the AIS system:

Figure 1. A scheme or visualization of the stages of AI integration into the AIS system

Based on the flowchart you uploaded, the steps are as follows: a.Clear Entry and Bookkeeping Initiation: The first step involves entering data into the accounting system and initiating the bookkeeping process. This step establishes the foundation for accurate and systematic financial record-keeping, b. Process Detection and Initialization: AI is applied to process financial transactions, detect anomalies, and initialize the workflow. This step involves identifying unusual patterns or errors within the data and setting up the system for further analysis, c. Read from Monitoring and Databases:AI then reads data from various monitoring systems and databases to gather insights. This step ensures that real-time financial information is accessible for analysis, d. Access General and Sending Information: The system accesses general data and sends the processed information to authorized stakeholders. This step is crucial for transparency, ensuring that financial reports and data are available for decision-making, e. Improved Financial Buying: Finally, AI leads to improved financial buying decisions. By providing more accurate and timely financial information, AI enables better management of investments and financial resources.

3. RESULTS AND DISCUSSIONS

The Indonesian startup industry was rocked by claims of financial fraud involving eFishery, a unicorn company that raised US$200 million in a Series D funding round in 2023, as reported by CNBC Indonesia(Purwanti, 2025), eFishery kept two financial books: an external book with inflated figures for external parties like the board, shareholders, banks, and auditors, and an internal book showing the company's true financial status. This fraud, which started in 2018, involved several executives, making it a systemic issue with multiple parties involved.

Key Individuals Involved: (a) AHR joined eFishery in August 2020 to help with financial management. AHR was tasked with recording inflated revenue and profit figures in the external financial books, as instructed by Gibran Huzaifah. In January 2022, Gibran created five nominee companies to manage money flows, with AHR handling bank accounts and tokens for these companie. (b) TTA joined in January 2021 to manage the internal financial records, showing the company's true financial situation. He reported directly to Gibran Huzaifah.

3.1 WK joined eFishery in December 2021 as the division head. WK reported directly to AHR and helped manage the external books.

In addition to the three main individuals, around 10 other employees were aware of the existence of two different financial books. External audits revealed discrepancies, such as revenue figures being four times higher than actual numbers. For example, during the January-September 2024 period, eFishery claimed a revenue of Rp2.6 trillion in the internal book, while the external report showed Rp12.3 trillion. Fraudulent practices included revenue inflation, where the external report exaggerated revenue growth while the internal report showed significant losses; profit manipulation, where the external report indicated a pre-tax profit of Rp261 billion, while the internal report showed a loss of Rp578 billion; feed facilities misrepresentation, where Gibran Huzaifah falsely claimed the company owned over 400,000 feed facilities, when the actual number was only about 24,000; and the creation of nominee companies, where Gibran set up five companies under different names to falsely inflate both revenue and expenses, including fabricating invoices, contracts, and fake bookkeeping in 2023. The manipulation aimed to inflate the company's financial figures and deceive investors and auditors. Transparency is essential for clear and accurate financial reporting, as it ensures information is accessible and understandable. Without transparency, it can lead to bad decisions, misinterpreted data, and hidden negative information(Gheorghe & Pirnau, 2009). Poor management can allow individuals to manipulate financial data for personal or corporate benefit. AI is revolutionizing accounting by boosting performance and expanding services. Today, it is used in forensic accounting and financial services, with future trends aimed at improving problem-solving abilities.(Lutfiati Rohmah et al., 2022).

AI-based audits, such as those using Isolation Forest, significantly improve efficiency by automating repetitive tasks and enabling real-time data analysis. This reduces the time and resources required for audits compared to traditional methods. The research results indicate that 68% of respondents preferred the automated audit approach over the conventional method(Budiandru et al., 2023). The AI autdit has great potential to improve overall audit practices(Lidiana, 2024).

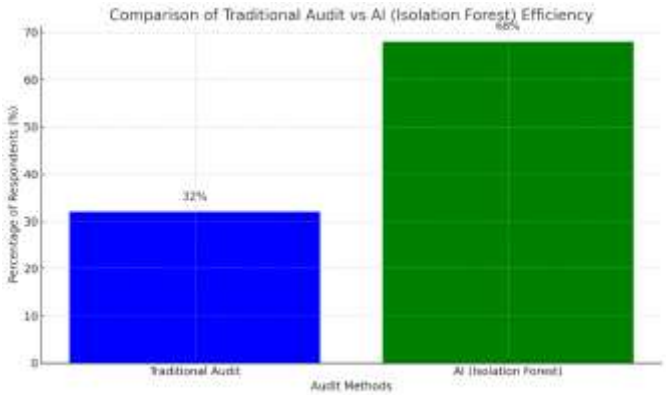

Figure 2. A comparison of the efficiency between Traditional Audit and AI

The chart compares the efficiency of Traditional Audit versus AI (Isolation Forest) in terms of preference by respondents :Traditional Audit (Blue Bar): 32% of respondents preferred the traditional audit method. This method typically involves manual reviews and checks, which can be time-consuming and prone to human error. AI (Isolation Forest) (Green Bar): 68% of respondents preferred the AI-based audit method, particularly Isolation Forest, a machine learning algorithm that detects anomalies and fraud patterns in data more efficiently. AI methods are able to automate

the detection process, significantly speeding up the audit and increasing accuracy. The chart clearly shows a higher preference for AI-based auditing over traditional methods, with a significant 68% preference, indicating that AI is seen as more efficient in detecting fraud. The 32% preference for traditional audits suggests that, while still widely used, manual auditing methods are less favored for their time-consuming nature and susceptibility to error compared to the automated capabilities of AI. This visual comparison highlights how AI can transform traditional auditing practices, improving both efficiency and effectiveness in detecting fraud. Based on the facts presented in the eFishery fraud case, here are several fraud prevention measures in the general journal that can be implemented using Artificial Intelligence (AI) technology.

AI can be applied to ensure that the general journal only records valid account pairs, such as sales with cash for cash sales, or sales with receivables for credit sales, preventing incorrect account pairings. AI can code transactions based on their type and ensure that journal entries only occur for valid account pairs by using techniques such as Natural Language Processing (NLP) or Deep Learning to automatically verify entries. This helps prevent errors or manipulation in the entry of mismatched account pairs, which could lead to inaccurate financial reports. For automatic coding of journal entries based on account pairs, we can use a basic NLP model or rule-based logic. This example assumes we have some journal entries in textual format and we want to check if the account pairs are valid (e.g., Sales with Cash or Sales with Receivables).

```
import re
# Define valid account pairings
valid_pairs = [
    ("Sales", "Cash"),
    ("Sales", "Accounts Receivable"),
    ("Purchases", "Accounts Payable"),
    ("Expenses", "Cash"),
    ("Revenue", "Bank")
]
# Sample journal entries (for testing purposes)
journal_entries = [
    {"description": "Sale of goods for cash", "debit_account": "Sales", "credit_account": "Cash"},
    {"description": "Sale of goods on credit", "debit_account": "Sales", "credit_account": "Accounts
Receivable"},
    {"description": "Payment for office supplies", "debit_account": "Expenses", "credit_account": "Cash"},
    {"description": "Sale of equipment", "debit_account": "Revenue", "credit_account": "Bank"},
    {"description": "Incorrect entry", "debit_account": "Sales", "credit_account": "Inventory"}
]
def check_valid_entry(entry):
    """
    Function to check if the journal entry has a valid account pair.
    """
    for pair in valid_pairs:
        if (entry["debit_account"] == pair[0] and entry["credit_account"] == pair[1]) or \
           (entry["debit_account"] == pair[1] and entry["credit_account"] == pair[0]):
            return True
    return False
# Check each journal entry
for entry in journal_entries:
    if check_valid_entry(entry):
        print(f"Valid entry: {entry}")
    else:
        print(f"Invalid entry: {entry}")
```

Figure 3. Automatic Coding in Journal Bookkeeping

Explanation: (a) Valid Account Pairings: A list of valid debit and credit account pairs (Sales with Cash, Sales with Accounts Receivable, etc.). (b) Sample Journal

Entries: A few sample journal entries to test the validation. (c) Check Function: The function check_valid_entry checks if the debit and credit accounts in the journal entry match any of the valid pairs. (d) utput: For each journal entry, the system prints whether the entry is valid or not based on the predefined rules.

3.2 Real-Time Reporting and Fraud Alerts

AI can be used to send real-time alerts if there is potential fraud or manipulation in the general journal. If the system detects transactions that do not align with normal patterns, AI can issue automatic alerts to managers or auditors for further action. This enables a quick response to potential fraud or errors in the general journal and reduces the time needed to detect such issues. For Real-Time Fraud Alerts, we can set up a basic anomaly detection system based on patterns or predefined thresholds. Here, we'll simulate a simple anomaly detection system that sends alerts if a transaction deviates significantly from expected values.

```
import random
# Simulated journal entry data (for testing purposes)
journal_entries = [
    {"transaction_id": 1, "amount": 5000, "debit_account": "Sales", "credit_account": "Cash"},
    {"transaction_id": 2, "amount": 1000000, "debit_account": "Sales", "credit_account": "Cash"},  #
Suspicious entry
    {"transaction_id": 3, "amount": 20000, "debit_account": "Expenses", "credit_account": "Cash"},
    {"transaction_id": 4, "amount": 1500, "debit_account": "Sales", "credit_account": "Accounts
Receivable"}
]
# Define a threshold for suspicious amounts (e.g., any transaction above 100,000 is suspicious)
threshold = 100000
def detect_anomaly(entry):
    """
  Function to detect anomalies based on predefined threshold (e.g., large transactions).
    """
    if entry["amount"] > threshold:
        return True
    return False
def send_alert(entry):
    """
    Function to send a fraud alert for suspicious transactions.
    """
    print(f"ALERT: Suspicious transaction detected: Transaction ID {entry['transaction_id']} with amount
{entry['amount']}")
# Check each journal entry for anomalies
for entry in journal_entries:
    if detect_anomaly(entry):
        send_alert(entry)
```

Figure 4. Automatic Coding in Real-Time Reporting and Fraud Alerts

Explanation: (a) Simulated Journal Entries: A list of journal entries with different transaction amounts. (b) Threshold: A threshold value for detecting large or suspicious transactions (e.g., any transaction above $100,000 is flagged as suspicious). (c) Detect Anomaly Function: Checks if a transaction exceeds the threshold, flagging it as an anomaly. (d) Alert System: If an anomaly is detected, an alert message is sent.

3.3 Combining Both Features (Full Implementation)

Let both automatic coding in journal bookkeeping and real-time fraud detection and alerts be combined into a single script.

```
import re
import random
# Define valid account pairings
valid_pairs = [
    ("Sales", "Cash"),
    ("Sales", "Accounts Receivable"),
    ("Purchases", "Accounts Payable"),
    ("Expenses", "Cash"),
    ("Revenue", "Bank")
]
# Sample journal entries (for testing purposes)
journal_entries = [
    {"transaction_id": 1, "description": "Sale of goods for cash", "debit_account": "Sales", "credit_account": "Cash", "amount":
5000},
    {"transaction_id": 2, "description": "Sale of goods on credit", "debit_account": "Sales", "credit_account": "Accounts
Receivable", "amount": 1000000},  # Suspicious entry
    {"transaction_id": 3, "description": "Payment for office supplies", "debit_account": "Expenses", "credit_account": "Cash",
"amount": 20000},
    {"transaction_id": 4, "description": "Sale of equipment", "debit_account": "Revenue", "credit_account": "Bank", "amount":
1500},
    {"transaction_id": 5, "description": "Incorrect entry", "debit_account": "Sales", "credit_account": "Inventory", "amount":
10000}
]
# Define a threshold for suspicious amounts (e.g., any transaction above 100,000 is suspicious)
threshold = 100000
def check_valid_entry(entry):
    """
    Function to check if the journal entry has a valid account pair.
    """
    for pair in valid_pairs:
        if (entry["debit_account"] == pair[0] and entry["credit_account"] == pair[1]) or \
           (entry["debit_account"] == pair[1] and entry["credit_account"] == pair[0]):
            return True
    return False
def detect_anomaly(entry):
    """
    Function to detect anomalies based on predefined threshold (e.g., large transactions).
    """
    if entry["amount"] > threshold:
        return True
    return False
def send_alert(entry):
    """
    Function to send a fraud alert for suspicious transactions.
    """
    print(f"ALERT: Suspicious transaction detected: Transaction ID {entry['transaction_id']} with amount {entry['amount']}")
# Process each journal entry
for entry in journal_entries:
    # Check if the journal entry is valid
    if check_valid_entry(entry):
        print(f"Valid entry: {entry}")
    else:
        print(f"Invalid entry: {entry}")
    # Detect anomalies and send alerts
        if detect_anomaly(entry):
        send_alert(entry)
        # Generate a summary report of valid and invalid entries
        valid_entries = []
        invalid_entries = []
        for entry in journal_entries:
            if check_valid_entry(entry):
                valid_entries.append(entry)
            else:
       invalid_entries.append(entry)
        print("\nSummary Report:")
        print(f"Total Valid Entries: {len(valid_entries)}")
        print(f"Total Invalid Entries: {len(invalid_entries)}")
        if invalid_entries:
            print("\nInvalid Entries:")
            for invalid_entry in invalid_entries:
```

Figure 5. Automatic Coding in Combining Both Features

Explanation of the Full Implementation. Step 1: Check Validity of Account Pairing: We check each journal entry against valid account pairs. Step 2: Detect Anomalies: The system checks if the transaction exceeds a predefined threshold for suspicious amounts. Step 3: Send Alerts: If an anomaly is detected, an alert is sent to notify the relevant parties (e.g., managers or auditors). Next Steps for Deployment: Integration with Real-Time Data: For actual use, you would integrate this code with real-time transactional data from your accounting system. Model Improvement: Use advanced machine learning models for more complex anomaly detection (e.g., Autoencoders, Isolation Forest) based on historical data. API Integration: For real-time reporting and fraud alerts, integrate with accounting software APIs like Xero or QuickBooks.

According to Kumari & Mittal (2024), machine learning algorithms are a great way to detect fraud in financial systems. These models can get better over time, learning to spot new types of fraud as they appear. This ability to adapt is key for keeping fraud detection effective in a constantly changing financial environment.

According to Xu et al. (2024), using the Isolation Forest algorithm achieved a detection accuracy of 26%, while the Autoencoder algorithm increased it to 33.6%. Isolation Forest is effective at detecting rare anomalies in streaming data(Kareem & Muhammed, 2024). Autoencoders are used to detect anomalies in transactions by training them on legitimate transactions and spotting differences in reconstruction to identify unusual activities.

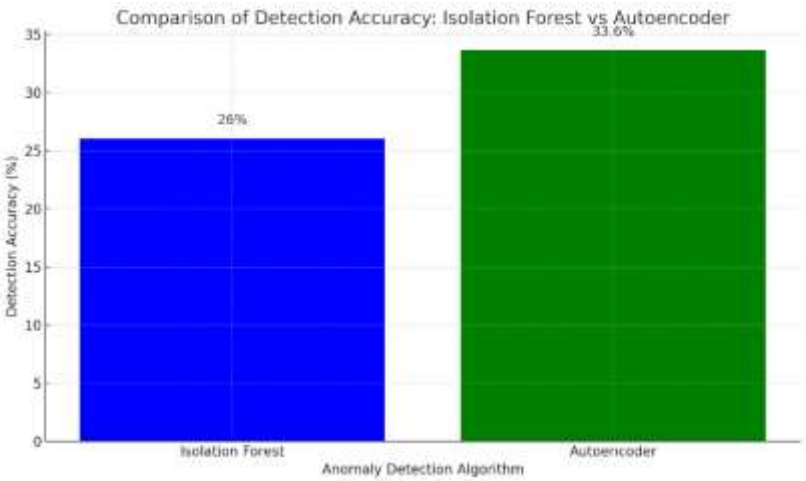

Figure 6. Comparison of Detection Accuracy: Isolation Forest vs. Autoencoder

The comparison results of Autoencoder provide better detection rates compared to Isolation Forest for the given use cases, improving the ability to identify fraudulent activities in financial transactions.

3.3 Access control and journal entry restrictions using Artificial Intelligence

In addition to detecting anomalies and verifying payments, controlling access to journal entries is vital in reducing fraud risk, especially by preventing unauthorized data manipulation. Limiting access to general journal entries ensures only authorized users can enter transactions into the system and that these transactions are recorded in valid accounts, like verified revenues. Access control in the accounting system is key to protecting assets and ensuring transactions align with management approval. Different methods, including preventive, detective, and corrective controls, address various risk factors. As systems grow more complex and face internal and external threats, strong management oversight is required to implement effective controls.

Failing to do so could lead to financial losses and data integrity issues(Rushinek & Rushinek, 1983).

According to Lakkshmanan et al. (2024), AI-based algorithms improve fraud detection in finance by identifying patterns and anomalies in transactions, boosting risk assessments, and streamlining customer service. These innovations lead to better fraud prevention strategies, enhancing security and trust. In accounting systems, AI improves efficiency, accuracy, and analysis. It automates tasks, improves financial reporting, and offers deeper insights, changing how organizations manage and analyze financial data for better decision-making(Muh. Fathir Maulid Yusuf et al., 2023).

3.4 Monitoring and Fraud Detection

AI can detect fraud by spotting unusual transaction patterns. Using machine learning algorithms, it can alert users to suspicious transactions early. Applying AI methods like Bagging, Random Forest, Support Vector Machine, and Bayesian techniques improves the management and intelligence of financial processing systems.(Song, 2024). The fraud detection system links payment accounts with user devices and analyzes location data to identify discrepancies. If the payment request location is outside the predefined range, payment authorization will be triggered(Lucy Ma Zhao, 2012).

3.5 Accuracy Improvement with Machine Learning

Fraud detection and prevention in finance are essential because fraud techniques are becoming more complex. Traditional methods often can't handle large data and lead to false positives. Deep Learning improves fraud detection by better recognizing patterns and extracting features(Miao, 2024).

3.6 Integration with Other Systems

AI-powered accounting systems must be connected with other systems like ERP and payment systems to link financial data with operations and payments. This integration improves efficiency, accuracy, real-time reporting, and helps with decision-making and data access throughout the organization(Lucy Ma Zhao, 2012).

3.7 Automatic Financial Report Preparation

AI can automatically create financial statements like income statements, balance sheets, and cash flow reports. Using predictive analysis, it can forecast future financial conditions based on transaction data. AI is also used to analyze financial reports, detecting anomalies and preventing fraud(Dheenadhayalan et al., 2025). AI is transforming accounting and auditing by automating routine tasks, improving efficiency, accuracy, and compliance. (Thanasas, 2024).

3.8 Security and Data Protection

Data security is essential in AI-driven accounting systems. AI can prevent unauthorized access and automatically detect threats, while helping with internal monitoring and access control. Machine learning algorithms like CNN-DenseNet and Random Forest can identify anomalies, improving cybersecurity, and can be used in accounting systems for real-time threat detection, ensuring security(Mohite & Ouarbya, 2024).

4 CONCLUSION

This research shows the effective use of AI in accounting systems, including anomaly detection, automated verification, and better access controls. These measures improve security, accuracy, and transparency in financial transactions while preventing fraud

like revenue inflation. The study highlights how AI reduces income inflation and enhances fraud detection, especially in large datasets.

The research found that 68% of respondents preferred the automated audit approach over traditional methods, highlighting the growing trust in AI-based auditing. The Isolation Forest algorithm achieved a detection accuracy of 26%, while Autoencoder improved this to 33.6%, demonstrating the effectiveness of machine learning in fraud detection. However, the study has limitations, including a small sample size and a focus on the e-Fishery case, which may not apply to other industries. Also, AI implementation depends on technical support, system integration, and management commitment, which may vary across organizations.

Future research could investigate the use of advanced AI models, like deep learning, to detect more complex fraud patterns. It should also assess AI's long-term effectiveness and scalability in accounting systems across industries. Additionally, exploring the combination of AI and human oversight could offer valuable insights into the best ways to manage fraud in Accounting Information System.

REFERENCES

Budiandru, B., Zakkiandri, Z., & Nur Basyiruddin, N. B. (2023). Unveiling the Potential of Computer-Based Audit Strategies: A Comparative Study between Conventional and Automated Approaches. *Account and Financial Management Journal*, *08*(08). https://doi.org/10.47191/afmj/v8i8.03

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection. *ACM Computing Surveys*, *41*(3), 1–58. https://doi.org/10.1145/1541880.1541882

Dheenadhayalan, K., Devapitchai, J. J., Surianarayanan, R., & Usha, S. (2025). *A Review of Current Applications of AI and Machine Learning Methods for Financial Statement Analysis* (pp. 211–230). https://doi.org/10.4018/979-8-3693-8186-1.ch008

Gheorghe, & Pirnau, M. (2009). Transparency in Financial Statements (IAS/IFRS). *EUROPEAN RESEARCH STUDIES JOURNAL*, *XII*(Issue 1), 101–108. https://doi.org/10.35808/ersj/212

Hakim, L. N. (2025). *eFishery Diduga Gelembungkan Pendapatan Hingga Rp9,7 Triliun*. CNBC Indonesia. https://teknologi.bisnis.com/read/20250122/266/1834010/efishery-diduga-gelembungkan-pendapatan-hingga-rp97-triliun?utm_source=chatgpt.com

Hardiantoro, A., & Adhi, I. S. (2025). *Berkaca dari Kasus eFishery, Bagaimana Cara Mengetahui Laporan Keuangan Akurat? Halaman all - Kompas.com*. Kompas.Com. https://www.kompas.com/tren/read/2025/01/26/180000565/berkaca-dari-kasus-efishery-bagaimana-cara-mengetahui-laporan-keuangan?page=all&utm_source=chatgpt.com

Kareem, M. S., & Muhammed, L. A. (2024). Anomaly Detection in Streaming Data using Isolation Forest. *2024 Seventh International Women in Data Science Conference at Prince Sultan University (WiDS PSU)*, 223–228. https://doi.org/10.1109/WiDS-PSU61003.2024.00052

Kim, Y., Savoldi, A., Lee, H., Yun, S., Lee, S., & Lim, J. (2008). Design and Implementation of a Tool to Detect Accounting Frauds. *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 547–552. https://doi.org/10.1109/IIH-MSP.2008.257

Kumari, P., & Mittal, S. (2024). Fraud Detection System for Financial System Using Machine Learning Techniques: A Review. *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–6. https://doi.org/10.1109/ICRITO61523.2024.10522197

Lakkshmanan, A., Seranmadevi, R., Sree, P. H., & Tyagi, A. K. (2024). *Engineering Applications of Artificial Intelligence* (pp. 166–179). https://doi.org/10.4018/979-8-3693-5261-8.ch010

Liang, P., & Wu, L. (2022). The Application of Artificial Intelligence in Accounting. *2022 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, 55–59. https://doi.org/10.1109/ICCNEA57056.2022.00023

Lidiana, L. (2024). AI and Auditing: Enhancing Audit Efficiency and Effectiveness with Artificial Intelligence. *Accounting Studies and Tax Journal (COUNT)*, *1*(3), 214–223. https://doi.org/10.62207/g0wpn394

Lucy Ma Zhao. (2012). Fraud detection system. *Patent Application Publication*.

Lutfiati Rohmah, K., Arisudhana, A., & Septa Nurhantoro, T. (2022). The Future of Accounting With Artificial Intelligence: Opportunity And Challenge. *International Conference on Information Science and Technology Innovation (ICoSTEC)*, *1*(1), 87–91. https://doi.org/10.35842/icostec.v1i1.5

Meiryani, M., Patricia, S., & Presillia, S. (2023). The Effect of Computerized Accounting Information Systems, Big Data Anaylsis, and Internal Audit in Accounting Fraud Detection. *2023 8th International Conference on Big Data and Computing*, 10–15. https://doi.org/10.1145/3624288.3624290

Miao, Z. (2024). Financial Fraud Detection and Prevention. *Journal of Organizational and End User Computing*, *36*(1), 1–27. https://doi.org/10.4018/JOEUC.354411

Mohite, R., & Ouarbya, L. (2024). Interpretable Anomaly Detection: A Hybrid Approach Using Rule-Based and Machine Learning Techniques. *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, 1–10. https://doi.org/10.1109/I2CT61223.2024.10543396

Muh. Fathir Maulid Yusuf, Ika Maya Sari, Ahmad Hamid, & Ilham Akbar Garusu. (2023). Integrasi Teknologi Artificial Intelligence Dalam Sistem Akuntansi Modern. *Journal of Trends Economics and Accounting Research*, *4*(1), 230–234. https://doi.org/10.47065/jtear.v4i1.902

Purrushottam, M. (2025). Fraud detection in financial transactons. *Indian Scientific Journal Of Research In Engineering And Management*, *09*(01), 1–9. https://doi.org/10.55041/IJSREM41105

Purwanti, T. (2025). *Fraud Sistemik efishery dan yang Terlibat di Dalamnya*. CNBC Indonesia. https://www.cnbcindonesia.com/news/20250201120230-4-607187/fraud-sistemik-efishery-dan-yang-terlibat-di-dalamnya

Roszkowska, P. (2020). Fintech in Financial Reporting and Audit for Fraud Prevention and Safeguarding Equity Investments. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3679816

Rushinek, A., & Rushinek, S. F. (1983). Access and communication controls in an accounting information system. *Proceedings of the Eighth Symposium on Data Communications - SIGCOMM '83*, 119–120. https://doi.org/10.1145/800034.800909

Setyowati, D. (2025). *Kronologi Dugaan Manajemen Startup eFishery Gelembungkan Dana Rp 9,8 Triliun - Startup Katadata.co.id*. Katadata.Co.Id. https://katadata.co.id/digital/startup/6791ae6f77b2a/kronologi-dugaan-manajemen-startup-efishery-gelembungkan-dana-rp-9-8-triliun?utm_source=chatgpt.com

Song, Y. (2024). Optimising the design of financial data processing models in accounting information systems based on artificial intelligence techniques. *Applied Mathematics and Nonlinear Sciences*, *9*(1). https://doi.org/10.2478/amns-2024-3603

Thanasas, G. L. (2024). *Transformation in Accounting Practices*. *10*, 1–16.

Umi Zakiyatun Khasanah. (2025). *Gibran Tersandung Skandal! eFishery Diduga Lakukan Manipulasi Keuangan Besar-besaran! - Teknologi*. Teknologi.Id. https://teknologi.id/startup/gibran-tersandung-skandal-efishery-diduga-lakukan-manipulasi-keuangan-besar-besaran

V. M., B., Dharmananda, M., M., M., Patel, S., Mohammed, M., & Reguraman, M. (2024). *Emerging Trends and Innovations of Artificial Intelligence in the Accounting and Financial Landscape* (pp. 575–598). https://doi.org/10.4018/979-8-3693-5380-6.ch023

Wanua.Id. (2025). *Startup eFishery Tersandung Skandal Fraud, Pendapatan Digelembungkan Rp 12 Triliun, CEO Diganti - WANUA.id*. Wanua.Id. https://wanua.id/startup-efishery-tersandung-skandal-fraud-pendapatan-digelembungkan-rp-12-triliun-ceo-diganti/?utm_source=chatgpt.com

Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). *AI-Based Financial Transaction Monitoring and Fraud Prevention with Behaviour Prediction*. https://doi.org/10.20944/preprints202407.1107.v1