Jurnal Akuntansi dan Bisnis
Vol 25, No. 1, Februari 2025: 65-86
https://jab.fe.uns.ac.id/

AI FOR FRAUD DETECTION AND ACCOUNTING SYSTEM SECURITY: IMPLEMENTATION IN INDONESIAN ISLAMIC BANKS

Deni Amin Sujana[1] (2307.Deni.002@student.tazkia.ac.id)
Sugiyarti Fatma Laela[2]

[1]Postgraduate Student, Islamic Accounting Department, Tazkia University, Indonesia
[2]Islamic Accounting Department, Tazkia University, Indonesia

ABSTRACT

This research study examines the impact of Artificial Intelligence (AI) on enhancing the security of Islamic banking accounting systems in Indonesia. Specifically, it focuses on AI's ability to accurately and efficiently detect fraud. The research used path analysis to investigate how AI's fraud detection capabilities affect accounting system security. The study involved 56 respondents, comprising IT professionals (55%), internal auditors (18%), and the rest (27%) were risk management staff from Islamic banking. A detailed questionnaire was developed to measure AI's role, revealing positive and significant effects on accounting system security. These effects were observed both directly and indirectly through fraud detection accuracy and efficiency. Interestingly, the study found that AI has a greater direct impact on security than its mediated effect, indicating that while AI improves fraud detection, its full potential in bolstering accounting system security has yet to be fully realized. The findings offer practical insights for Islamic banks, regulators, and stakeholders to implement and evaluate AI technology for fraud detection.

Keywords: Islamic Bank, Artificial Intelligence, Fraud Detection, Accounting System Security.

Penelitian ini meneliti dampak Artificial Intelligence (AI) dalam meningkatkan keamanan sistem akuntansi perbankan syariah di Indonesia. Secara khusus, penelitian ini memfokuskan pada kemampuan AI untuk mendeteksi kecurangan secara akurat dan efisien. Penelitian ini menggunakan analisis jalur untuk menyelidiki bagaimana kemampuan deteksi kecurangan AI mempengaruhi keamanan sistem akuntansi. Penelitian ini melibatkan 56 responden, yang terdiri dari profesional TI (55%), auditor internal (18%), dan sisanya (27%) adalah staf manajemen risiko di perbankan syariah. Kuesioner disusun secara rinci untuk mengukur peran AI, yang menunjukkan efek positif dan signifikan terhadap keamanan sistem akuntansi. Efek-efek ini diamati baik secara langsung maupun tidak langsung melalui akurasi dan efisiensi deteksi kecurangan. Menariknya, penelitian ini menemukan bahwa AI memiliki dampak langsung yang lebih besar terhadap keamanan daripada efek mediasinya, yang mengindikasikan bahwa meskipun AI meningkatkan deteksi kecurangan, potensi maksimalnya dalam meningkatkan keamanan sistem akuntansi belum sepenuhnya terwujud. Temuan ini menawarkan pemahaman praktis bagi bank syariah, regulator, dan pemangku kepentingan untuk mengimplementasikan dan mengevaluasi teknologi AI untuk mendeteksi kecurangan.

Kata kunci: Bank Syariah, Kecerdasan Buatan, Deteksi Kecurangan, Keamanan Sistem Akuntansi.

Received:
3 July 2024
Revised
3 March 2025
14 April 2025
10 June 2025
Received
20 June 2025

INTRODUCTION

The digitalization of the banking industry, including Islamic banking, has been rapidly growing. Since 2020, the number of physical offices of Islamic banks has slowed down due to changes in people's behavior after the COVID-19 pandemic and the increased digitalization of Islamic banking (OJKa, 2022). The technologies adopted include mobile and digital wallets, biometric authentication and artificial programming interface (Adewale et al., 2020). Widharto et al. (2020) explain that Islamic banks are now making digitalization a corporate policy to provide optimal service (Service Excellence). This is in line with the Islamic banking development roadmap of OJK (Otoritas Jasa Keuangan or Financial Services Authority) for 2020-2025, where one of the

programs is to make advanced Information Technology as a key of component Islamic Banking's new identity (OJKb, 2021).

The issue that emerges from this digital transformation is the problem of financial fraud which needs to be handled seriously. In 2022, there were 822 dispute complaint reports in the banking sector, and the largest complaints based on 5 types of banking problems were in the external fraud category, consisting of deception, account hacking, skimming, and cybercrime, totaling 145 complaints (LAPS-SJK, 2022). Banking losses in 2021 due to external and internal fraud reached Rp. 4.62 trillion (Republika, accessed 2021). Meanwhile in Islamic banks, based on GCG (Good Corporate Governance) reports, frauds occurred in 2021 and 2022. For example, at Bank Muamalat, there were reported internal fraud incidents of 10 cases in 2021 and 14 cases in 2022 (Muamalat, 2022). At Bank Syariah Indonesia (BSI), internal fraud was reported as 7 cases in 2021 and 14 cases in 2022 (BSI, 2022), and at Bank BTPN Syariah, 8 cases were reported in 2021 and 4 cases in 2022 (BTPN, 2022). Examples of fraud activities related to Islamic banking accounting systems include engineered recording of incoming funds in the form of savings, current accounts, and deposits, resulting in recording discrepancies in bank books; withdrawal of customer funds not by the owner that is not recorded in the books, causing physical discrepancies in cash; deposits or book transfers without accompanying fund flows; and others (POJK 39, 2019).

To overcome this challenge, Indonesian Islamic banking must continue to develop effective methods and tools to detect and prevent such fraud. One solution that has become a focus for Islamic banking is the use of Artificial Intelligence (AI) in fraud detection systems. AI is a field of computer science that aims to develop systems and machines that have the ability to perform tasks that require human intelligence (Russell et al., 2010). This intelligence includes understanding human language, pattern recognition, decision making, and self-learning. AI strives to create algorithms and mathematical models that enable computers to think, feel, and act as humans do (Russell et al., 2010). The application of AI in banking can be used in all sections. In the front office, examples of AI use are voice assistants and biometrics. In the middle office, AI can be used for anti -fraud risk monitoring and complex legal and compliance workflows. In the back office, an example of its use is credit underwriting with smart contract infrastructure (Fares, 2023).

AI technology can help Islamic banks detect suspicious transaction patterns, identify anomalies, and efficiently analyze financial data on a large scale. Mohamed (2021) describes the importance of applying artificial intelligence technology as a proactive step in mitigating fraud risk in the banking sector. According to POJK (Financial Services Authority Regulation) No. 39/POJK.03/2019, Banks are required to develop and implement an effective anti-fraud strategy, which must at least contain four pillars, including: first, prevention; second, detection; third, investigation, reporting, and sanctions; and fourth, monitoring, evaluation, and follow-up.

AI's ability to detect potential fraud will enhance security in the banking sector. AI provides several benefits in detecting fraud, including the ability to analyze large volumes of data with high accuracy, monitor and analyze user transactions and behavior in real time, and adapt to new fraud data and patterns (Takyar, accessed 2023). Strong security is one of the core elements of success and public trust in Islamic banking (Kartika et al., 2019). Based on the importance of AI in detecting potential fraud, this research empirically aims to analyze the role of AI in improving the security of Indonesia's Islamic banking accounting system through its ability to detect fraud more accurately and efficiently.

There have been quite several studies on the role of AI in detecting fraud, which are generally theoretical. Aysan et al. (2022) discuss how Islamic banks pay special attention to adopting information technology based on a survey conducted by

CIBAFI (General Council of Islamic Banks and Financial Institutions), one of which is artificial intelligence technology. However, Aysan et al. (2022) have yet to discuss how banks can implement this technology in detail. The importance of understanding the implications and impact of artificial intelligence applications in the context of Indonesian Islamic banks becomes the basis for further research. Previously, Abdulla et al. (2020) provided a more general view on the use of artificial intelligence in Islamic banking, particularly in Bahrain, but did not specifically discuss how artificial intelligence is implemented in other countries, particularly in Indonesia, and its application in fraud detection in accounting systems. Meanwhile, in the conventional banking sector, artificial intelligence has proven its effectiveness in improving accounting systems and fraud detection. For example, a study by Phua et al. (2010) highlights how artificial intelligence algorithms can identify suspicious patterns in financial transactions.

This research has three main points of focus. First, it aims to empirically test the role of AI in improving the security of Islamic banking systems through fraud detection. Second, the research specifically concentrates on fraud detection in Islamic banking accounting systems, which involves collecting, classifying, summarizing, and reporting financial statement information (Warren et al., 2018). All banking transactions, such as teller transactions, ATM, Mobile Banking, Payment & Purchase, Open Banking via API, Host to Host, and other system connections, are recorded in the accounting system and serve as a data source for fraud detection. Third, the research includes the development of a comprehensive questionnaire instrument related to indicators reflecting AI implementation, accuracy and efficiency of fraud detection, and security of accounting systems in Islamic banking, based on earlier conceptual studies.

The research method used in this study is the path analysis method to analyze the role of artificial intelligence (AI) in improving the security of Islamic banking accounting systems through its ability to detect fraud more accurately and efficiently. The accuracy and efficiency of fraud detection serve as mediating variables between the role of AI and the security of Islamic banking accounting systems. This research involves IT professionals in Islamic banking as respondents, who understand and/or have implemented fraud detection in accounting systems in Islamic banking. To measure the role of AI in detecting fraud to enhance the security of Islamic banking accounting systems, this study uses a questionnaire developed from previous concepts and research. The results of this study are expected to provide practical guidance for Islamic banks in determining policy direction and evaluation materials for AI implementation in Islamic banking accounting system fraud detection. For regulators, such as OJK, the results of this study can be used for comparison against the results of monitoring and supervision of fraud data in Islamic banking. Furthermore, this research can also be used by other stakeholders in facing challenges and opportunities in adopting artificial intelligence technology.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Fraud Theory

Fraud is the intentional act of misleading, deceiving, or manipulating the Bank, customers, or other parties, resulting in losses to the Bank, customers, or other parties, while the perpetrator gains financial benefits, directly or indirectly (POJK 39, 2019). Types of acts classified as Fraud include deception, fraud, asset embezzlement, information leakage, banking crimes, and other similar actions. Based on the Bank's business activities, Fraud occurrence activities are categorized as funding, credit or financing, use of identity and data of other parties, asset management, cyber use, financial statement presentation, and other activities (POJK 39, 2019). The fraud triangle theory suggests that fraud can occur due to three factors: pressure, opportunity, and

rationalization (Cressey, 1953). This foundational theory has evolved significantly, with the fraud diamond theory adding a fourth factor, capability, as a crucial cause of fraud (Wolfe, 2004). Further development led to the fraud pentagon theory by Crowe Howarth, which extends the fraud triangle by adding two more factors: competence and arrogance (Crowe, 2011). Recent research by Vousinas (2019) proposed the fraud hexagon model, incorporating stimulus as a sixth dimension to better explain fraudulent behavior in the modern digital environment. To prevent or reduce internal fraud, companies need to implement controls based on the Agency theory due to differences in interests between owners and managers (Ross, 1973). This occurs because agents act as management running the company and owners who are capital owners act as principals (Shoimah et al., 2021). Additionally, pressure among company owners must be minimized, as conflicts can also occur between company owners, namely, between majority shareholders and minority shareholders (Bebchuk et al., 2019). Fraud prevention has evolved from manual knowledge-based approaches to sophisticated proactive measures, with recent studies demonstrating the effectiveness of artificial intelligence and machine learning in detecting financial statement fraud patterns (Ozili, 2020). The integration of AI into fraud prevention frameworks represents a significant research gap in the literature, particularly in the context of Islamic banking systems where additional ethical and compliance considerations apply (Alrfai et al., 2023; Bose et al., 2023). While conventional banking has begun exploring AI-driven fraud detection extensively, there remains limited research on how these technologies can be tailored to address the unique requirements and challenges of Islamic banking systems.

Fraud from an Islamic Perspective

Fraud or cheating is an action that is prohibited in the Islamic religion, as explained in the Qur'an, Surah Al-Muthaffifin/83:1-3:

"Woe to those who give less [than due]. Who, when they take a measure from people, take in full. But when they give by measure or by weight to them, they cause loss."

In addition, we are forbidden to obtain wealth by false means, as explained in the Qur'an, Surah Al-Baqarah/2:188:

"And do not consume one another's wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you [to] consume a portion of the wealth of the people in sin, while you know [it is unlawful]."

In a hadith narrated by Muslim, it also illustrates how this fraud or cheating is described, as follows:

"The Messenger of Allah, peace and blessings be upon him, said: Whoever is given the responsibility by Allah to lead his people and then dies in a state of deceiving his people, surely Allah will forbid Paradise for him."

Al-Ghazali (1965) explains that in our efforts and search for livelihood, we are forbidden to commit oppression, dishonesty, and fraud because they are considered unlawful acts. In business activities, al-Ghazali classifies 8 business ethics to avoid fraud, as explained by Fitriani et al. (2022) as follows: 1. Business activities must be based on justice, kindness, and virtue, and the absence of oppression 2. There must be clarity between business actors 3. Foster good and trustworthy business relationships 4. Debts must be settled before the agreed time 5. Reduce margins by selling cheaper, and in turn increase profits 6. Business activities are not only pursuing worldly gains 7. Keep away from doubtful transactions 8. Achieve profits with consideration of existing risks. Imam Al-Haddad (2009) even obliges businesspeople to study Allah's law in the business world, which are obligatory, recommended, disliked, and forbidden before conducting business transactions. Moreover, to avoid fraud, businesspeople must constantly strengthen their faith and improve it because faith is the core of everything (Al-Haddad, 2012). Recent Islamic scholarly work has reinforced these principles in the context of modern financial systems. Rashid et al. (2024) emphasize the importance of corporate

governance in Islamic financial institutions as a means to prevent fraud and ensure compliance with Shariah principles. Yulisnawati et al. (2024) highlight the critical role of internal auditor independence and effectiveness in ensuring Shariah compliance, which inherently includes fraud prevention. Additionally, Mohamed (2021) discusses how Islamic financial risk management must adapt to new technological risks, including those introduced by AI implementation, while maintaining adherence to Shariah principles.

Artificial Intelligence (AI) and Its Role in Fraud Detection

Artificial Intelligence (AI) is a field of computer science focused on developing systems and machines capable of performing tasks that traditionally require human intelligence (Russell et al., 2010). In the banking sector, AI plays three key roles: 1. Front Office: This includes the implementation of chatbots, facial recognition, voice assistants, and biometrics. 2. Middle Office: AI is used for document digitization, loan processing, KYC/AML (Know Your Customer/Anti-Money Laundering), and legal compliance workflows. 3. Back Office: This involves the use of AI for credit underwriting, fraud detection, smart contract infrastructure, and risk monitoring (Bhattacharya et al., 2022).

Artificial intelligence (AI) plays a key role in fraud detection by automatically and in real-time monitoring transactions, recording relevant logs, and alerting the user when a transaction appears suspicious or may qualify as fraud. According to Umamaheswari et al. (2023) artificial intelligence (AI) can improve fraud detection accuracy and efficiency because, with the use of applied algorithms, it can process massive transaction data in banking without the need for human intervention. In order to investigate fraudulent transactions, humans are still involved in the final stage as decision-makers. However, choices may now be made directly without human oversight (Phua et al., 2010).

The use of AI in fraud detection at Islamic banks will strengthen the security of the accounting system. It will help in business and operational processes, including prevention against fraud, deception, asset embezzlement, information leakage, and other fraudulent actions (POJK 39, 2019). Ultimately, the security of the Islamic banking accounting system influences the trust and loyalty of Islamic banking customers (Kartika et al., 2019). Furthermore, according to Handinisari (2022), security, convenience, and trust influence the interest in transacting using Islamic bank services, particularly mobile banking services.

The Effect of AI on Accuracy and Efficiency in Detecting Potential Fraud

The Agency Theory (Ross, 1973) provides a fundamental theoretical framework for understanding the need for monitoring mechanisms in organizations. This theory addresses the inherent conflict of interest between principals (shareholders) and agents (management), which can lead to information asymmetry and potentially fraudulent activities. In Islamic banking, where ethical considerations are paramount, this agency problem is further complicated by the need to ensure compliance with Shariah principles (Rashid et al., 2024).

Artificial Intelligence emerges as a sophisticated monitoring tool that can significantly reduce these agency problems. The fraud detection capabilities of AI are grounded in the evolution of fraud theories, particularly addressing the "opportunity" element in the fraud triangle (Cressey, 1953), the "capability" element in the fraud diamond (Wolfe et al., 2004), and the "competence" factor in the fraud pentagon theory (Horwath, 2011). By continuously monitoring transactions and identifying patterns that humans might miss, AI restricts the opportunity for fraud and enhances detection of capability indicators.

AI is able to trace suspicious transactions quickly and accurately. The integration of AI in the banking sector creates opportunities for a financial

services revolution to increase the speed and accuracy of transactions, and reduce the risk of fraud (Panakaje et al., 2023). Bao et al. (2022) state that the implementation of AI and Machine Learning with algorithm application can increase accuracy and reduce errors in fraud detection. A fraud detection system with 24/7 automatic monitoring capabilities and specific anomaly detection capabilities makes fraud detection faster and more accurate. In addition, the AI feature in KYC (Know Your Customer) using NLP (Natural Language Processing) makes customer verification more accurate (Hasan et al., 2023). Similarly, in terms of handling big data, the use of AI provides advantages in efficiency and accuracy, allowing users to focus on other activities (Abdulla et al., 2020). Eneh et al. (2023) in a previous study stated that the implementation of AI (Facial recognition, Chatbot, and Digital Assistant) in Nigerian deposit banks has a positive and significant effect on transaction monitoring for fraud detection. This research will further investigate and empirically test the influence of AI, which is believed to be able to detect potential fraud more accurately and efficiently, by proposing hypothesis 1 as follows:

H1: Implementation of AI has a positive effect on Accuracy and Efficiency in Detecting Potential Fraud in the Islamic Bank Accounting system.

The Effect of Accuracy and Efficiency in Fraud Detection on the Security of Islamic Bank Accounting Systems

The concept of accounting system security is derived from Information Systems Security Theory, which emphasizes the protection of information assets from unauthorized access, use, disclosure, disruption, modification, or destruction (Hall, 2011). In accounting systems, security is particularly crucial as it safeguards financial information integrity, confidentiality, and availability.

The fraud hexagon theory (Vousinas, 2019) introduces "stimulus" as a critical factor in modern digital fraud environments. Efficient and accurate fraud detection systems can act as negative stimuli by creating an environment where potential fraudsters perceive a high risk of being caught. This theoretical perspective explains why enhanced fraud detection capabilities contribute to overall system security.

A secure accounting system is a system that is free from fraud and can prevent unwanted things such as data leakage or loss of data integrity (Hall, 2011). Research by Donepudi (2017) emphasizes the importance of implementing Machine Learning technology to increase efficiency and accuracy in fraud detection in Islamic banking. In line with this, Hashemi et al. (2023) present evidence that Machine Learning with enhanced algorithms can increase fraud detection capabilities in Islamic banking. Bose et al. (2023) provide in-depth insights into Big Data analysis strategies where AI that is continuously trained to improve accuracy and programmed to follow accounting rules will result in a more secure and consistent Islamic banking accounting system. Big Data Analytics can process large data from various sources, such as transaction data, customer data, and historical data, making it more efficient in detecting fraud and can improve the security of Islamic banking accounting systems (Dhone et al., 2023). The application of NLP (Natural Language Processing) algorithms in artificial intelligence for fraud detection is also highlighted in Boulieris et al. (2023) research as it improves accuracy in Islamic banking accounting systems both online and offline. Thus, integrating a more efficient and accurate fraud detection system can make a positive contribution to the security and reliability of the Islamic banking accounting system. This research will empirically test the impact of accuracy and efficiency in fraud detection due to AI implementation on improving the security of the accounting system by proposing hypothesis 2 as follows:

H2: Accuracy and Efficiency in Fraud Detection have a positive effect on the Security of Islamic Bank Accounting Systems.

The Effect of AI Implementation on the

Security of Islamic Bank Accounting Systems

The Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) provide theoretical frameworks for understanding how technological innovations like AI are adopted and influence organizational outcomes. These theories suggest that perceived usefulness and ease of use, along with performance expectancy, are key determinants of technology adoption success (Widharto et al., 2020).

From an Islamic perspective, the implementation of technology must align with maqasid al-shariah (objectives of Islamic law), which includes the protection of wealth (hifz al-mal). AI implementation that strengthens security systems directly contributes to this fundamental Islamic principle by protecting financial assets from fraudulent activities (Mohamed, 2021).

Research by Kaur et al. (2023) offers in-depth perspectives on AI implementation in addressing security challenges in Islamic financial institutions, namely by applying AI techniques through: Identify, protect, detect, respond, and recovery. Then Solikin et al. (2023) depict the positive impact of artificial intelligence implementation on the effectiveness of automating Islamic banking accounting systems. These findings are reinforced by studies from Alrfai et al. (2023) and Almustafa et al. (2023), which highlight the important role of AI in detecting fraud and improving the efficiency of Islamic banking accounting systems, particularly in Jordan. Similar conclusions are also found in Vinoth et al. (2022) research, which highlights the vital role of AI in enhancing information security in Islamic banking, in addition to improving efficiency and customer experience.

Thus, the use of artificial intelligence technology may have a direct influence on improving the security of Islamic banking accounting systems, by proposing hypothesis 3 as follows:

H3: AI implementation has a positive effect on Islamic Bank Accounting System Security

RESEARCH METHODS

The respondents in this study are professionals who work in Islamic banks and have worked or are currently working in the Information Technology (IT), Internal Audit, or Risk Management departments. These three functional units are the main functions in Information Technology governance by Commercial Banks (POJK 11, 2022). The study employs a purposive sampling method to ensure respondents possess specific expertise and experience relevant to the research objectives (Etikan et al., 2016). These three sections or fields of work are different but have a connection in the implementation of fraud detection in Islamic banking, either as implementors, end-users, or as supervisors and monitors of fraud detection.

The selection of respondents follows specific criteria to ensure they possess the necessary knowledge and experience in AI implementation for fraud detection in Islamic banking. Respondents must meet at least one of the following minimum criteria : 1) Has worked in the Information Technology department and has implemented AI products. They are expected to understand the technical implementation of AI, assess the capabilities of infrastructure and technology, and the technical challenges of AI implementation. 2)Has worked in the internal audit department and has implemented AI products. They will be able to independently assess the reliability and effectiveness of AI fraud detection systems or as users of AI products, fraud detection systems. 3).Has worked in the risk management department and has implemented AI products. They have the ability to analyze the impact of AI implementation on strategic and operational risks of Islamic banks.

The questionnaire is structured into four main sections to facilitate comprehensive data collection (Krosnick et al., 2018). The first section captures demographic information including respondents' professional background, years of experience, educational qualifications, and specific roles in AI

implementation projects. The second section assesses respondents' knowledge and experience with AI implementation in Islamic banking, focusing on technical understanding, implementation challenges, and perceived benefits. The third section explores the effectiveness of AI in fraud detection based on respondents' direct experience with such systems. The fourth section evaluates the impact of AI implementation on accounting system security and operational risk management.

Data collection is conducted through an electronic survey platform using a 4-point Likert scale to measure respondents' agreement with statements related to each research variable (Joshi et al., 2015). The research instrument underwent content validation through expert review and pilot testing with a small sample of Islamic banking professionals prior to full deployment (Bolarinwa, 2015). This ensured clarity, relevance, and comprehensiveness of the questionnaire items.

The research variables consist of ten latent variables, namely AI implementation and its three latent indicator variables; accuracy and effectiveness of fraud detection as well as accounting system security and its four latent indicator variables. Each latent variable is measured by observed variables totaling 28 questions. The conceptual figure below presents the complete research model.

AI implementation is an exogenous variable, to assess the extent to which AI has been implemented by respondents. The AI referred to in this research includes AI applications in the front office (chatbots, facial recognition, voice assistants, biometrics), middle office (document digitalization, loan processing, KYCP/AML, legal compliance workflows), and back

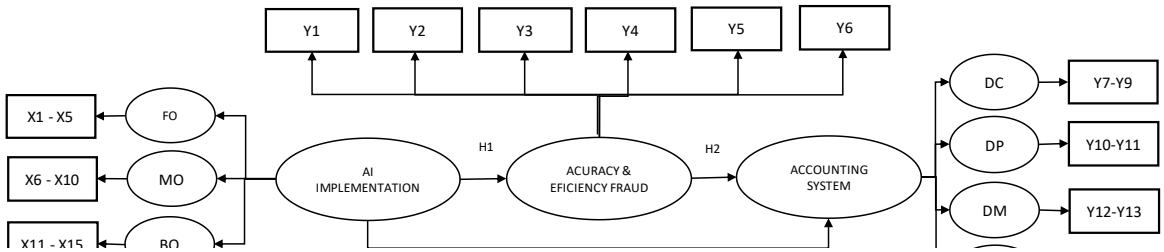

Figure 1.
Conceptual Research Model

FO	:	Front Office	MO	:	Midle Office	BO	:	Back Office
X1	:	Chatbots	X5	:	Document Digitalization	X9	:	Credit Underwriting
X2	:	Facial Recognition	X6	:	Loan Processing	X10	:	Fraud Detection
X3	:	Voice Assistant	X7	:	KYC/AML	X11	:	Smart Contract Infrastructure
X4	:	Biometric	X8	:	Legal Compliance Workflows	X12	:	Risk Monitoring
Y1	:	Real time detection	Y3	:	More Cost Saving	Y5	:	Less Time Processing
Y2	:	Reducing Manual Intervention	Y4	:	Improved Fraud Prevention	Y6	:	Reduce False Positives
DC	:	Data Collection	DP	:	Data Processing	IG	:	Information Generation
Y7	:	Data Valid	Y10	:	Free Program Fraud	Y14	:	Secure Data Information
Y8	:	Data Completed	Y11	:	Free Operational Fraud	Y15	:	Appropiate Information
Y9	:	Free Data Error	DM	:	Database Management	Y16	:	Authorized Access Information
			Y12	:	Secure Financial Data	Y13	:	Secure Non Financial Data

office (credit underwriting, fraud detection, smart contract infrastucture, risk monitoring) that have functions in fraud detection, either directly or indirectly (Bhattacharya et al., 2022). The questionnaire uses a 4-point Likert scale, where a score of 4 will fully represent the statement, conversely, a score of 1 will least represent the statement. In the front office, the AI analyzed is in the form of chatbots: AI-powered conversational interfaces that simulate human-like interactions to provide customer service, answer queries, and facilitate fraud reporting without human intervention, facial recognition: Biometric technology that identifies or verifies a person's identity using facial features by mapping facial geometry and comparing it against stored templates for authentication purposes, voice assistants: Speech recognition systems that interpret verbal commands, process natural language, and execute banking transactions or provide information through voice-based interactions, and biometrics: Authentication technologies that use unique physiological characteristics (fingerprints, iris patterns, palm veins) to verify customer identity, providing enhanced security for banking transactions (Tamrakar et al., 2021; Boldea et al., 2021; Memis et al., 2021; Marani et al., 2023). In the Middle office, AI includes Document Digitalization: The conversion of physical documents into digital formats using optical character recognition (OCR) and machine learning to extract, categorize, and process data automatically, reducing manual handling and improving information accuracy (Mejia, 2019), Loan Processing: AI-driven platforms that automate credit application analysis, risk assessment, and approval workflows by processing large volumes of financial data to expedite decision-making while maintaining consistency in underwriting standards (Mejia, 2019), KYC/AML (Know Your Customer/Anti-Money Laundering): Verification Tools: Intelligent systems that verify customer identities and monitor transactions using pattern recognition algorithms to detect suspicious activities that may indicate money laundering, terrorist financing, or other financial crimes (Faggella et al., 2023), and Legal compliance workflows: Automated processes that continuously monitor banking operations against evolving regulatory requirements, flagging potential compliance issues, generating required reports, and adapting to new regulations through machine learning capabilities (Faggella et al., 2023). While in the Back Office, AI includes Credit Underwriting: Credit Underwriting: AI-based systems that evaluate borrower creditworthiness using advanced statistical models, alternative data sources, and machine learning algorithms to predict repayment behavior and optimize lending decisions (Dessain et al., 2023), Fraud Detection: Intelligent systems that analyze transaction patterns, user behaviors, and account activities to identify anomalies and suspicious activities indicative of fraudulent transactions in real -time or near-real-time (Boulieris et al., 2023), Smart Contract infrastructure: Blockchain-based programmable agreements that automatically execute, control, and document legally relevant events according to predetermined terms, ensuring transaction transparency and reducing manual verification requirements (Abdulla et al., 2020), and Risk Monitoring: Predictive analytics platforms that continuously assess operational, credit, and market risks using AI algorithms to identify emerging threats, provide early warnings of potential issues, and enable proactive intervention before problems escalate (Joni et al., 2024).

The Accuracy and Efficiency of Fraud Detection variable is intended to assess AI's ability to correctly and quickly identify fraud cases with minimal errors (Bao et al., 2022). This variable includes real-time detection, reducing manual intervention, more cost saving, improved fraud prevention, less time processing, and reduce false positives (West et al., 2021). The security of an accounting system is crucial to prevent fraud. It encompasses control over processes such as data collection, data processing, database management, and information generation.

This security extends to all aspects including funding, financing, identity and data usage, asset management, cyber security, and the presentation of financial reports (POJK 39, 2019). The Data Collection variable will be measured based on the validity, completeness, and accuracy of input data. Control over Data Processing entails freedom from fraudulent programs and operations. Database Management security involves protecting both financial and non-financial data. Finally, for the Information Generation variable, it includes control over data theft, misuse, and appropriate data access (Hall, 2011).

This research uses a quantitative approach using path analysis method to analyze the role of AI in improving the security of Islamic banking accounting systems through its ability to detect fraud more accurately. The tool used for technical analysis is SmartPLS, which allows testing complex relationships between variables (one-way or two-way). Additionally, SEM is also a hybrid technique that combines aspects of regression analysis, path analysis, and confirmatory factor analysis. The initial stage will involve testing the measurement model/outer model and structural model. In the measurement model test, it will measure the validity test to assess whether the instruments/indicators truly measure what should be measured, where when the instrument is valid, the research results are valid (Sugiyono, 2019). Next, it will test the model's convergent validity to see the correlation between scores/indicators and their construct scores (LF), where a minimum score of 0.5 - 0.6 is still accepted for the development stage (Ghozali, 2021). Then, the Average Variance Extracted (AVE) will also be calculated, where the requirement for a good model is if the AVE of each construct is greater than 0.50 (Ghozali, 2021). In the structural model test, the R-Square value will be calculated to see how much influence the exogenous variables have on the endogenous ones, where R-Square values of 0.67, 0.33, and 0.19 mean strong, moderate, and weak models, respectively (Chin, 1988). From the above measurement results, it can then be continued to test whether this hypothesis can be accepted and how much influence it has by conducting a coefficient test (path coefficient) and significance test using the Bootstrapping method or by increasing the sample simulation to > 1000. Using SmartPLS, the sample used is 5000 samples (Sugiyono, 2019). The hypothesis result is declared accepted if the T Test value > T

Table 1.
Distribution of Respondent Based on Place of Work

No.	Bank Type	Bank Name	Total Respondent
1	BUS	PT. Bank Aceh Syariah	10
2	BUS	PT BPD Riau Kepri Syariah	-
3	BUS	PT BPD Nusa Tenggara Barat Syariah	6
4	BUS	PT. Bank Muamalat Indonesia	2
5	BUS	PT. Bank Victoria Syariah	-
6	BUS	PT. Bank Jabar Banten Syariah	7
7	BUS	PT. Bank Syariah Indonesia, Tbk	1
8	BUS	PT. Bank Mega Syariah	9
9	BUS	PT. Bank Panin Dubai Syariah, Tbk	-
10	BUS	PT. Bank Syariah Bukopin	-
11	BUS	PT. BCA Syariah	2
12	BUS	PT. Bank Tabungan Pensiunan Nasional Syariah, Tbk	1
13	BUS	PT. Bank Aladin Syariah, Tbk	1
14	UUS	UUS (Unit Usaha Syariah or Sharia Business Unit)	8
15	BPRS	BPRS (Bank Perkreditan Rakyat Syariah or Sharia Rural Bank)	9
		Total	56

Table. If the significance level is 5%, then the T Table value is 1.65, while for P Values < 0.05 if significant at 5%.

ANALYSIS AND DISCUSSION

Respondent Profile

A Google form questionnaire was distributed online through the WhatsApp application to be filled out by professionals in the fields of IT, Audit, and Risk Management at Islamic Banks for research purposes. A total of 90 questionnaires were sent out based on the researcher's connections at Islamic Banks, WhatsApp Group networks, and mediator relation. Out of these, 56 complete questionnaires were obtained for further processing. Among the 13 Islamic Commercial Banks, 9 or 70% participated in the research, with 39 represented respondents. Out of the 20 Sharia Business Units, 5 UUS (Unit Usaha Syariah or Sharia Business Units) or 25% participated, with 8 represented respondents. The remaining 9 respondents were from BPRS (Bank Perkreditan Rakyat Syariah or Sharia Rural Bank) also involved in the research. Based on the distribution of respondents, it can be concluded that this research adequately represents the implementation of AI in Islamic banking in Indonesia. The total number of respondents and their distribution are presented in Table 1.

The majority of respondents, which is 55%, work in the IT department, dominated by men aged 31-40 years old and have a bachelor's degree. As many as 10 people or 18% are internal auditors, and 7 people hold positions in risk management. The involvement of these three fields in filling out the questionnaire affects the accuracy of the results of this research, as all three are directly involved technically with AI applications, system security, and accounting business process flows. There are 3 respondents over the age of 41, and the remaining 22 respondents are over 41 years old. Based on education, there are 2 respondents with a diploma, 44 respondents with a bachelor's degree, and the remaining 10 respondents have a master's or doctoral degree. This shows, in general, the relatively good quality of human resources in Islamic banks, and in particular, they are able to understand not only the technical practice of AI but also its substantive impact on the quality of accounting information produced. Figure 2 provides the details of the respondent distribution, showing the complete profile distribution of the respondents.

Research Instrument Validity Test

Testing the validity of the questionnaire using the SmartPLS version 4.0.9.6 tool involves assessing convergent validity and discriminant validity. Convergent validity ensures that the questions or statements in the questionnaire accurately represent the

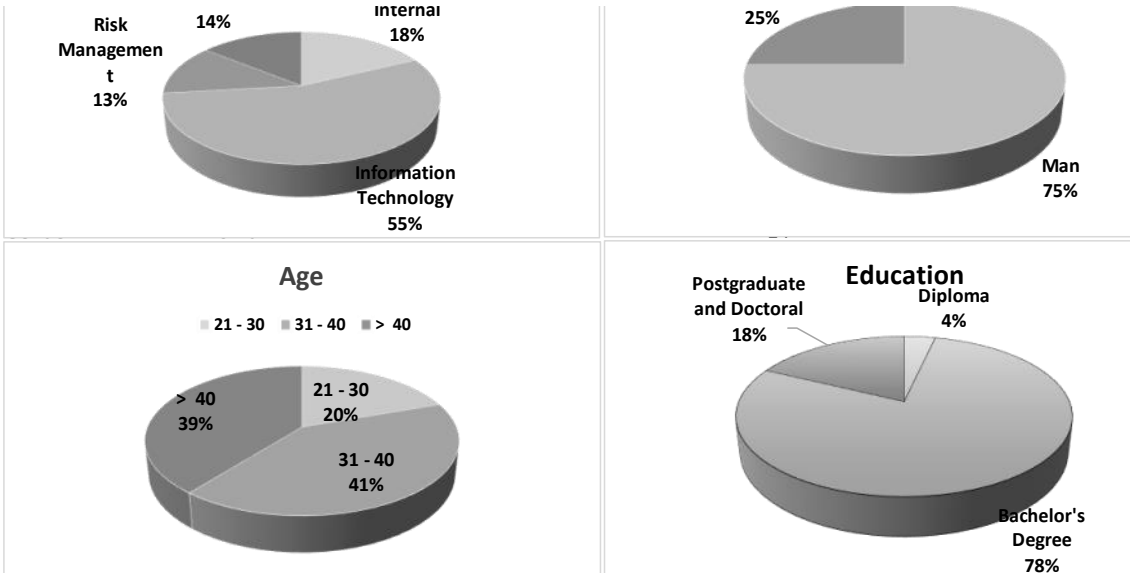

Figure 2.
Detail Respondent Distribution

underlying variable being measured. In other words, the questionnaire is considered valid if all the observed variables effectively and accurately measure their respective underlying variables. Convergent validity is measured by ensuring that the loading factor values are above 0.6 and that the Average Variance Extracted (AVE) values are above 0.5 (Ghozali, 2021). The initial model in SmartPLS is displayed in Figure 3, while the final model is shown in Figure 4, which is the outcome of testing convergent validity. Additionally, Table 2 presents the AVE values from the SmartPLS output.

Figure 3 shows the initial model of the test results for all variables. Several formative variables from the latent variables generally already have outer loading values greater than 0.6, but there are still some values below 0.6. Therefore, it is necessary to remove some variables in order to meet the convergent validity and model reliability testing stages.

After re-testing, all factor loading values in Figure 4 are greater than 0.6, thus meeting convergent validity. Similarly, the Average Variance Extracted (AVE) values in Table 2 show that all constructs of the latent variables have AVE > 0.5, or more than 50% of the variance from the measurement items has been absorbed by their respective latent variables. Therefore, overall this model is valid in terms of convergent validity.

The results of the discriminant validity testing based on the Fornell-Larcker criterion state that if the square root of the AVE on a construct is higher than the correlation of the construct with other latent variables, then it is considered valid. The assessment of validity using cross-loadings states that if the cross-loading value of an indicator is higher than

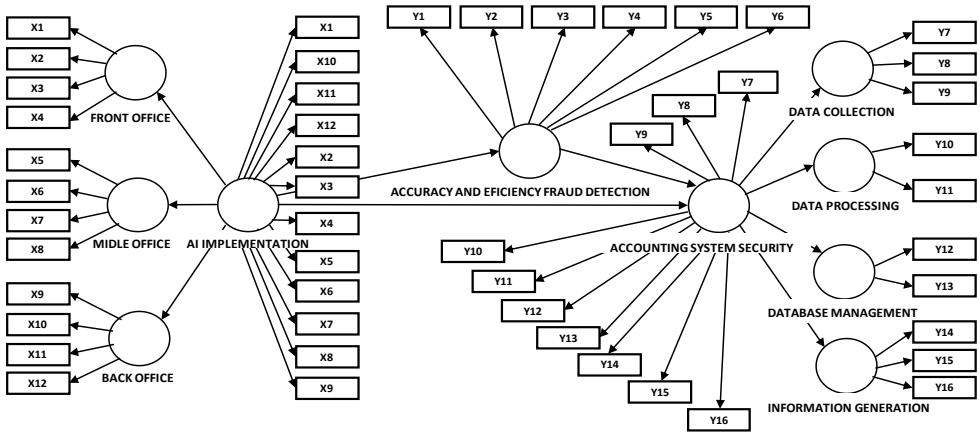

Figure 3.
Initial Model Estimation

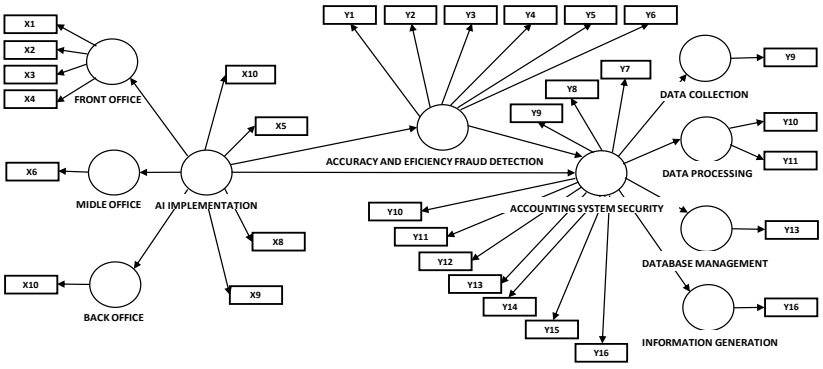

Figure 4.
Final Model Estimation

other constructs (Sekaran et al., 2016). The test results are presented in Table 3.

From Table 3, it can be seen that the square root of the AVE on the construct variables is higher than the correlation of the construct with other latent variables, so this construct model can be said to have discriminant validity. In addition to using the Fornell-Larcker criterion, according to Henseler et al. (2015) and Hair et al. (2021), an alternative approach based on the multitrait-multimethod matrix can also be used to assess discriminant validity, known as the heterotrait-monotrait ratio of correlations (HTMT), where the discriminant validity correlation value must be <0.85 or <0.90 (Hair et al., 2021) to depict good discriminant validity. The HTMT test results can be seen in Table 4.

Table 4 shows that all correlation values for discriminant validity are less than 0.9, indicating that the construct model has strong discriminant validity. Each concept is distinct from the others, meaning that there is no overlapping association.

Research Instrument Reliability Testing

Reliability testing is used to measure the consistency of respondents' answers. Reliability indicators can use composite reliability and Cronbach's alpha values. Composite reliability measures the true value of a construct's reliability, while Cronbach's alpha measures the minimum

Table 2.
AVE Values

	Cronbanch's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	AVE
Accuracy And Eficiency Fraud Detection	0.950	0.955	0.961	0.807
Data Processing	0.869	0.882	0.938	0.884
Front Office	0.754	0.750	0.845	0.580
Ai Implementation	0.781	0.828	0.852	0.591
Accounting System Security	0.942	0.948	0.951	0.665

Table 3.
Fornel Lacker Values

	Accuracy And Eficiency Fraud Detection	Back Office	Data Collection	Data Processing	Database Management	Front Office	Ai Implementation	Information Generation	Accounting System Security	MO
Accuracy And Eficiency Fraud Detection	0.898									
Back Office	0.32	1								
Data Collection	0.303	0.186	1							
Data Processing	0.355	0.409	0.503	0.94						
Database Management	0.464	0.452	0.447	0.617	1					
Front Office	0.2	0.268	-0.01	0.189	0.318	0.761				
Ai Implementation	0.411	0.818	-0.015	0.389	0.398	0.465	0.769			
Information Generation	0.591	0.427	0.467	0.589	0.666	0.197	0.442	1		
Accounting System Security	0.562	0.481	0.643	0.794	0.86	0.249	0.408	0.86	0.815	
Midle Office	0.269	0.365	-0.04	0.102	0.12	0.286	0.393	0.263	0.169	1

limit of a construct's reliability value. An indicator is considered reliable if the composite reliability and Cronbach's alpha values are > 0.7 (Ghozali, 2021). The test results in Table 5 show the composite reliability and Cronbach's alpha values.

From Table 5, it can be seen that all Cronbach's alpha and composite reliability values are greater than 0.7, so it can be said that all indicators are reliable and respondents are consistent in answering the questions.

Evaluation of Model Quality

To assess the quality of a model, according to Hair et al. (2019), if the R-Square value is 0.75, 0.50, and 0.25, it means the model is substantial/strong, moderate, and weak, respectively. Meanwhile, an R-Square value of 0.90 or higher is considered a typical indicative or overfit model.

From Table 6, we can see that the Fraud Detection Accuracy and Efficiency variable has an R-Square value of 0.169 or falls into the weak category, meaning that 16.9% of fraud detection accuracy and efficiency is influenced by the AI implementation variables (Front Office, Middle Office, Back Office), and the remaining 83.51% is influenced by other variables. For the Accounting System Security variable, it has an R-Square value

Table 4.
HTMT Values of SmartPLS Result

	Accuracy And Eficiency Fraud Detection	Back Office	Data Collection	Data Processing	Database Management	Front Office	Ai Implementation	Information Generation	Accounting System Security	Midle Office
Accuracy And Eficiency Fraud Detection										
Back Office	0.328									
Data Collection	0.311	0.186								
Data Processing	0.386	0.435	0.534							
Database Management	0.472	0.452	0.447	0.658						
Front Office	0.251	0.299	0.039	0.24	0.365					
Ai Implementation	0.482	0.815	0.209	0.438	0.403	0.616				
Information Generation	0.605	0.427	0.467	0.626	0.666	0.223	0.475			
Accounting System Security	0.589	0.49	0.68	0.878	0.879	0.298	0.466	0.877		
Midle Office	0.276	0.365	0.04	0.103	0.12	0.312	0.422	0.263	0.18	

Table 5.
Construct Reliability and Validity Values

	Cronbanch's Alpha	Composite Reliability (Rho_A)	Composite Reliability (Rho_C)	Average Variance Extracted (Ave)
Accuracy And Eficiency Fraud Detection	0.950	0.955	0.961	0.807
Data Processing	0.869	0.882	0.938	0.884
Front Office	0.754	0.750	0.845	0.580
Ai Implementation	0.781	0.828	0.852	0.591
Accounting System Weakness	0.942	0.948	0.951	0.665

of 0.353 or falls into the moderate category, which means that 35.3% of accounting system security is influenced by the Fraud Detection Accuracy and Efficiency and AI Implementation variables, and the remaining 64.7% is influenced by other variables.

Hypotesis Testing

To test whether these hypotheses can be accepted and how significant their effects are, coefficient testing (path coefficient) and significance testing were performed using the bootstrapping method or sample simulation. The hypothesis is stated as accepted if the T-test value > T-table value, and the P-Values < 0.05 with a 5% significance level. The data was then expanded to 5,000 data points, and calculations were performed using SmartPLS, (Figure 5).

Based on the results shown in Figure 4 and Table 7, the path coefficient analysis show that all T-test values for the latent variables are above the threshold of 1.65, with P-Values consistently below 0.05. The strongest relationships were observed between AI Implementation and Back Office (coefficient = 0.818, t-statistic = 19.906), and between Accounting System Security and both Database Management and Information Generation (coefficients = 0.860, t-statistics = 12.318 and 20.132 respectively). This indicates strong predictive relationships between these constructs.

The relationship between AI Implementation and Accuracy and Efficiency Fraud Detection, though

Table 6.
R-Square Valuest

	R-Square	R-Square Adjusted
Accuracy And Eficiency Fraud Detection	0.169	0.151
Back Office	0.670	0.662
Data Collection	0.413	0.400
Data Processing	0.631	0.623
Database Management	0.740	0.734
Front Office	0.216	0.198
Information Generation	0.739	0.734
Accounting System Security	0.353	0.324
Midle Office	0.154	0.136

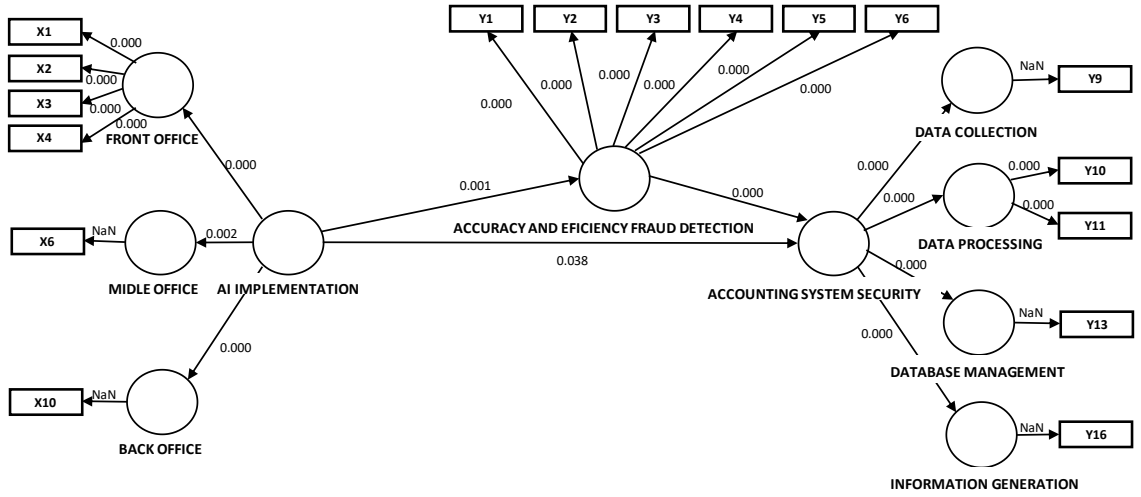

Figure 5.
Final Model and Bootstraping Result

significant (p = 0.001), showed a moderate effect size (coefficient = 0.411, t-statistic = 3.105). Similarly, Accuracy and Efficiency Fraud Detection demonstrated a moderate predictive effect on Accounting System Security (coefficient = 0.475, t-statistic = 3.755, p < 0.001). The weakest, though still statistically significant, relationship was between AI Implementation and Accounting System Security (coefficient = 0.212, t-statistic = 1.780, p = 0.038).

Based on these comprehensive statistical results, all proposed hypotheses can be accepted as they demonstrate positive and statistically significant effects. The descriptive statistics provide context for these relationships, allowing for more nuanced interpretation of the strength and practical significance of each relationship tested in the model.

H1: AI implementation has a positive effect on the accuracy and efficiency in detecting potential fraud in the accounting system of Islamic banks. The T-test value is 3.105 > 1.65, and the P-Value is 0.001 < 0.05, so the hypothesis is accepted and has a significant positive effect. H2: The accuracy and efficiency in fraud detection have a positive effect on the security of the accounting system of Islamic banks. The T-test value is 3.755 > 1.65, and the P-Value is 0.000 < 0.05, so the hypothesis is accepted and has a significant positive effect. H3: AI implementation has a positive effect on the security of the accounting system of Islamic banks. The T-test value is 1.780 > 1.65, and the P-Value is 0.038 < 0.05, so the hypothesis is accepted and has a significant positive effect.

Analysis and Discussion

The first hypothesis states that implementing AI has a positive impact on the accuracy and efficiency in Islamic banks' accounting systems is strongly supported by our findings, The positive correlation between AI implementation and fraud detection capabilities demonstrates that artificial intelligence technologies are enhancing the fraud detection landscape in Islamic banking. This technological advancement allows for real-time detection, faster data processing, reduced

Table 7.
Patch Coefficient Values Bootstraping Result

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/ STDEV|)	P values
Accuracy And Efficiency Fraud Detection -> Accounting System Security	0.475	0.476	0.126	3.755	0.000
Ai Implementation -> Accuracy And Efficiency Fraud Detection	0.411	0.426	0.132	3.105	0.001
Ai Implementation -> Back Office	0.818	0.826	0.041	19.906	0.000
Ai Implementation-> Front Office	0.465	0.487	0.100	4.657	0.000
Ai Implementation -> Accounting System Security	0.212	0.214	0.119	1.780	0.038
Ai Implementation -> Midle Office	0.393	0.392	0.134	2.932	0.002
Accounting System Security -> Data Collection	0.643	0.645	0.101	6.377	0.000
Keamanan Sistem Akuntansi -> Data Processing	0.794	0.796	0.053	14.988	0.000
Accounting System Security -> Database Management	0.860	0.858	0.070	12.318	0.000
Accounting System Security -> Information Generation	0.860	0.859	0.043	20.132	0.000

false positives, and enhanced fraud prevention through automation.

These findings align with Eneh et al. (2023), who identified similar positive effects when implementing AI technologies (facial recognition, chatbots, digital assistants) in Nigerian deposit banks, specifically in transaction monitoring for fraud detection. The consistency between our results and previous research strengthens the conclusion that AI technology significantly improves the accuracy and efficiency of fraud detection systems regardless of banking context. In other words, AI makes transaction monitoring more accurate and efficient. The results of this study also support the theory that AI provides several benefits in detecting fraud, including the ability to analyze large amounts of data with high accuracy, monitor and analyze transactions and user behavior in real-time, and adapt to new data and fraud patterns (Takyar, accessed 2023). The results of this study also support the research concept by Panakaje et al. (2023) that the integration of AI in the banking sector creates opportunities for a revolution in financial services to improve the speed and accuracy of transactions and reduce the risk of fraud.

The relatively low R-square value of 17% for AI's explanatory power on fraud detection accuracy suggests several practical challenges in the Indonesian Islamic banking sector. This likely stems from suboptimal utilization of AI-generated data across front, middle, and back offices. Furthermore, the unique nature of Islamic banking products creates implementation challenges, as application developers must thoroughly understand Islamic banking business models when developing fraud detection systems. This explanation is consistent with Roh et al. (2021), who identified bottlenecks in machine learning data collection processes, and Zheng et al. (2022), who emphasized the importance of domain-specific business knowledge in developing effective fraud detection systems.

The second hypothesis is that the accuracy and efficiency in fraud detection have a positive effect on the security of the accounting system of Islamic banks. In other words, the more accurate and efficient the fraud detection, the more secure the accounting system of Islamic banks. This indicator can be seen in how respondents describe the security of the accounting system in banks, observed from how data is inputted or received (data collection), data is processed (data processing), data is stored (database management), and how data is informed (generate information). This finding empirically validates the conceptual insights from Bose et al. (2023) regarding Big Data analysis strategies in which AI systems continuously trained for improved accuracy and programmed to follow accounting regulations create more secure and consistent accounting systems. Our results also provide quantitative evidence supporting Donepudi's (2017) emphasis on machine learning implementation for enhanced fraud detection in Islamic banking, as well as Hashemi et al.'s (2023) findings regarding enhanced algorithms improving fraud detection capabilities.

The third hypothesis exploring AI implementation's direct effect on accounting system security is also supported by our research. The implementation of various AI technologies across Islamic banks' operational divisions demonstrated a positive, albeit modest, direct effect on accounting system security. This modest direct effect (coefficient of 0.212) indicates that while AI implementations contribute positively to security enhancements, the relationship is complex and influenced by various factors..

This finding complement previous qualitative research by Solikin et al. (2023), which illustrates the positive impact of implementing artificial intelligence on the effectiveness of automating the accounting system of Islamic banks, as well as studies by by Alrfai et al. (2023) and Almustafa et al. (2023), which highlight the important role of AI in detecting fraud and improving the efficiency of the accounting system in Jordanian Islamic banks. A similar conclusion was also found in research by Vinoth et al. (2022), which highlights the

vital role of AI in enhancing information security in Islamic banking.

Based on the bootstrapping results obtained, it can be seen that AI implementation has a direct influence on the security of the accounting system with a value of 0.212. This indicates that the application of artificial intelligence (AI) technology in the accounting system contributes positively to improving the security of the system, although the influence is relatively small. This finding is in line with research by Kokina et al. (2017), which states that although AI has great potential, there are still challenges in its implementation, explaining why the direct influence of AI on the security of the accounting system is still relatively small.

Interestingly, our path analysis revealed that AI's direct impact on accounting system security (0.212) slightly exceeds its indirect impact through fraud detection accuracy and efficiency mediation (0.19). This suggests that while AI significantly improves fraud detection capabilities, which subsequently enhances system security, there are additional direct security benefits from AI implementation beyond fraud detection improvements. This finding supports Oladipo et al.'s (2024) assertion that accounting system security depends on multiple factors including human factors, governance structures (Rashid et al., 2014), internal audit processes (Yulisnawati, 2024), and management policies (Cahyadi et al., 2020), which may be directly influenced by AI implementation.

These findings collectively demonstrate that AI implementation in Islamic banking provides both direct security enhancements and indirect benefits through improved fraud detection capabilities, though the current implementation state suggests considerable room for optimization in the Indonesian Islamic banking sector.

CONCLUSION

Based on the results of this study, the implementation of AI in Islamic banks has been proven to affect the security of the accounting system both directly and indirectly through the mediation of fraud detection accuracy and efficiency. Another finding is that the role of AI in improving accuracy in fraud detection to enhance the security of the accounting system is still not optimal. However, the direct influence of AI implementation on improving the security of the accounting system is even greater. The implication of the significant influence of AI on the security of the accounting system can be a recommendation for Islamic banks and regulators. Islamic banks can consider implementing AI gradually, in the front office, middle office, and back office. In addition to customer experience purposes, AI can also be used for fraud detection purposes to be more accurate and efficient, thus indirectly making the accounting system of Islamic banks more secure. This finding provides input for regulators, in this case, the OJK (Otoritas Jasa Keuangan or Financial Services Authority), to assess and evaluate the extent to which Islamic Banks implement AI in their business activities, so that it becomes an input in designing the governance of Islamic Banks in the AI era.

LIMITATIONS AND SUGGESTIONS

This research provides valuable insights into AI implementation and its impact on accounting system security in Islamic Banks, though several limitations should be acknowledged. The questionnaires given to respondents from the Information Technology, Audit, and Risk Management departments at Islamic Banks were able to answer the research model that describes the implementation of AI and its impact on the security of the accounting system. While the research model successfully demonstrates AI's significant role in enhancing accounting system security through improved fraud detection, the relatively modest R-square value (17%) indicates that AI's potential is not yet fully optimized in this context.

Additionally, while the measurement instruments were generally reliable, several questionnaire items did not meet validity and reliability thresholds, indicating potential gaps in capturing the full

complexity of the variables under study. The sample size, though sufficient for statistical analysis, represents another limitation that could affect the generalizability of findings across the entire Islamic banking sector.

Future research could address these limitations by incorporating additional variables that influence accounting system security, such as human factors, internal control mechanisms, organizational policies, and governance structures. Expanding the conceptual dimensions of AI implementation beyond the front office, middle office, and back office classification to include customer experience, risk management, regulatory compliance, product development, and operational efficiency would provide more comprehensive insights.

To enhance generalizability, subsequent studies should aim to include representatives from all Islamic banks in the country with larger sample sizes. Furthermore, longitudinal studies tracking the evolution of AI implementation and its security impacts over time would provide valuable insights into the developmental trajectory of these technologies in Islamic banking.

REFERENCES

Abdulla, Y., Ebrahim, R., & Kumaraswamy, S. (2020). Artificial Intelligence in Banking sector: Evidence from Bahrain. *International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy*. IEEE. https://doi.org/10.1109/ICDABI51230.2020.9325600.

Adewale, A.A.,Ismal, R. (2020). Digital Transformation in Islamic Banking. *IFSB Working Paper Series*. https://www.ifsb.org/wp-content/uploads/2023/10/WP-19_En.pdf.

Al-Ghazali (1965). Ihya 'Ulumuddin. (2nd ed.) [Translation]. https://archive.org/details/ihya-ulumuddin-terjemahan-jilid-3_202302/ihya%20ulumuddin%20terjemahan%20jilid%201/.

Al-Haddad, H.A. (2009). *Al-Da'wah Al-Tammah Wa Al-Tadzkirah Al-'ammah (A. Y. Al-Muhdhor, Trans.).* Pustaka Basma & Cahaya Ilmu Publisher.

Al-Haddad, H.A. (2012). Risalah Al-Muawanah Wa Al-Muzoharoh Wa Al-Muazarah, Limaqam Al-Imam Al-Haddad.

Almustafa, E., Assaf, A., & Allahham, M. (2023). Implementation of artificial intelligence for financial process innovation of commercial banks. *Revista de Gestao Social e Ambiental*, 17(9). https://doi.org/10.24857/rgsa.v17n9-004.

Alrfai, M. M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., & Almaiah, M. A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. *Cogent Social Sciences*, 9(2). https://doi.org/10.1080/23311886.2023.2243719.

Aysan, A. F., Belatik, A., Unal, I. M., & Ettaai, R. (2022). Fintech Strategies of Islamic Banks: A Global Empirical Analysis. *FinTech*, 1(2), 206–215. https://doi.org/10.3390/fintech1020016.

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial Intelligence and Fraud Detection. *Supply Chain Management* 11, 223–247. Springer Nature. https://doi.org/10.1007/978-3-030-75729-8_8.

Bebchuk, L. A., & Kastiel, K. (2019). The perils of small-minority controllers. Georgetown Law Journal, 107(6), 1453-1514. https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/07/The-Perils-of-Small-Minority-Controllers.pdf.

Bhattacharya, C., & Sinha, M. (2022). Role of Artificial Intelligence in Banking for Leveraging Customer Experience. *Australasian Accounting, Business and Finance Journal*, 16(5), 89–105. https://doi.org/10.14453/aabfj.v16i5.07.

Bolarinwa, O. A. (2015). Principles and methods of validity and reliability testing of questionnaires used in social and health science researches. *Nigerian Postgraduate Medical Journal,* 22(4), 195-201. https://doi.org/10.4103/1117-1936.173959.

Boldea, B.I., Boldea, C.R. (2021). Facial Recognition Technology Used In The Payment System, Academy of Economic Studies of Moldova. DOI 10.5281/zenodo.6255729.

Bose, S., Dey, S. K., & Bhattacharjee, S. (2023). *Big data, data analytics and artificial intelligence in accounting:*

An overview. Handbook of Big Data Research Methods (32–51). Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781800888555.00007.

Boulieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2023). Fraud detection with natural language processing. *Machine Learning*. https://doi.org/10.1007/s10994-023-06354-5.

BSI. (2022). GCG (Good Corporate Governance) Report 2022. https://www.bankbsi.co.id/company-information/tata-kelola/dokumen/laporan_gcg.

BTPN. (2022). GCG (Good Corporate Governance) Report 2022.

Cahyadi, W., Mukhlisin, M., & Pramono, S. (2020). The Effect of Top Management Support on the Quality of Accounting Information Systems. *Scientific Journal of Management, Economics, & Accounting (MEA)*, 4(1), 1-10. DOI: 10.31289/jab.v6i1.2995.

Cressey, D. R. (1953). Other people's money; a study of the social psychology of Embezzlement. Free Press, 24. https://doi.org/10.1086/221475.

Dessain, J., Bentaleb, N., Vinas, F. (2023). Cost Of Explainibility in AI : An Example with Credit Scoring Models. *Explainable Artificial Intelligence,* 498 -516.

Dhone, M.B., Nitya, E. (2023). Big Data Analytic For Fraud Detection In Financial Transaction. *Journal of Data Acquistion and Processing* 38 (3). https://sjcjycl.cn/DOI: 10.5281/zenodo.7922883.

Donepudi, P.K. (2017). Machine Learning and Artificial Intelligence in Banking, *Engineering International*, 5(2). DOI:10.18034/ei.v5i2.490.

Eneh, O.M, Okeke, F.C. & Amahalu, N.N. (2023). Artificial Intelligence and Fraud Detection of Deposit Money Banks in Awka-South Anambra State, Nigeria. Global *Journal of Artificial Intelligence and Technology Development*, 1(2), 8-20. https://www.openjournals.ijaar.org/index.php/gjaitd/article/view/148/154.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11.

Fagella, D., Azulay, D., Bharadwaj, R. (2023). AI in Banking : Executive Cheat Sheet, *Emerj Artificial Intelligence Reasearch,* 1-9. https://emerj.com/ai-in-banking-executive-cheat-sheet/.

Fares, O. H., Butt, I., & Lee, S. H. M. (2023). Utilization of artificial intelligence in the banking sector: a systematic literature review. *Journal of Financial Services Marketing*, 28(4), 835–852. https://doi.org/10.1057/s41264-022-00176-7

Fitriani, S. D & Sunantri, S. (2022). Etika bisnis Islam menurut Imam Al-Ghazali dan Yusuf Al-Qaradhawi. *CBJIS : Cross-Border Journal of Islamic Studies,* 4(1), 50–68. https://doi.org/10.37567/cbjis.v4i1.1269

Hall, J.A. (2011). Accounting Information System (7th ed.). Cengage Learning. https://archive.org/details/accountinginform0000hall_x5u5.

Handinisari, H., Muhlisin, S., & Yono, Y. (2022). Pengaruh Keamanan, Kemudahan dan Kepercayaan Nasabah Bank Syariah Indonesia Terhadap Minat Bertransaksi Menggunakan Layanan Mobile Banking. *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam*, 4(3), 818–828. https://doi.org/10.47467/elmal.v4i3.2076..

Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2023). Fraud Detection in Banking Data by Machine Learning Techniques. *IEEE Access,* 11, 3034–3043. https://doi.org/10.1109/ACCESS.2022.3232287.

Hassan, M., Aziz, L. A.-R., & Andriansyah, Y. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110–132. https://www.researchberg.com/index.php/rcba/article/view/153.

Horwath, C. (2011). Putting the Freud in Fraud: Why the Fraud Triangle Is No Longer Enough, in Horwath, Crowe. www.s-ox.com/dsp_getWebinarDetails.cfm?CID=2668.

Joni, R., & Graepel, T. (2024). Predictive Analytics and AI: Driving the Next Wave of Risk Management in Financial Services. https://

doi.org/10.13140/RG.2.2.16499.75041.

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology,* 7(4), 396-403. doi: 10.9734/bjast/2015/14975.

Kartika, T., Firdaus, A., & Najib, M. (2020). Contrasting the drivers of customer loyalty; financing and depositor customer, single and dual customer. *Journal of Islamic Marketing,* 11(4), 933–959. https://doi.org/10.1108/JIMA-04-2017-0040.

Kaur, R., Gabriljelcic, D., Klobucar, T. (2023). Artifical Intelligence for Cybersecurity: Literatur review and future research direction. *Information Fusion,* 97. https://doi.org/10.1016/j.inffus.2023.101804.

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115–122. https://doi.org/10.2308/jeta-51730.

Krosnick, J. A., & Presser, S. (2018). Question and questionnaire design. In D. Vannette & J. Krosnick (Eds.), The Palgrave handbook of survey research (39-455). Palgrave Macmillan.

LAPS-SJK. (2022). Alternative Dispute Resolution - Financial Services Sector, Annual & Financial Report 2022. https://lapssjk.id/laporan-2022.

Mejia, N. (2019). How To Use AI to Digitize Loan Processing - A Brief Overview. https://emerj.com/ai-sector-overviews/digitize-loan-processing/.

Memis, H., Geylan, Z. (2021). Creating an AI -based personal assistant: Case Study Of Isbank Maxi. *Journal of Digital Banking* 5(4) 1-8. https://www.scribd.com/document/818191592/Creating-an-AI-based-personal-assistant.

Mohamed, H. (2021). Managing Islamic Financial Risks And New Technological Risks. In Artificial Intelligence and Islamic Finance (pp.61-76). https://doi.org/10.4324/9781003171638-5.

Muamalat. (2022). GCG (Good Corporate Governance) Report 2022. https://www.bankmuamalat.co.id/index.php/hubungan-investor/laporan-gcg.

OJKa. (2022). Indonesia Sharia Financial Development Report 2022. OJKb. (2021). Indonesia Syariah Banking Development Roadmap 2020-2025.

Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity: Navigating the fintech landscape. *International Journal of Science and Research Archive*, 11(1), 1959–1967. https://doi.org/10.30574/ijsra.2024.11.1.0258.

Ozili, P. K. (2020). Advances and issues in fraud research: A commentary. *Journal of Financial Crime*, 27(1), 92-103. DOI: 10.1108/JFC-01-2019-0012.

Panakaje, N., Madhura, K. (2023). Bank For Tomorrow: Role of an Artificial Intelligence (AI) in Banking Sector. *Emergence and Research in Interdisciplinary Management and Information Technology* 61-80. https://www.researchgate.net/publication/371938063_Bank_for_Tomorrow_Role_of_an_Artificial_Intelligence_AI_in_Banking_Sector.

Phua, C., Lee, V.C., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Applied Soft Computing, 10*(4), 990-1006. https://doi.org/10.48550/arXiv.1009.6119.

POJK 11, 2022. POJK NO.11/POJK.03/2022 Regarding the Implementation of Information Technology by Commercial Banks.

POJK 39. (2019). POJK No.39/POJK.03/2019 regarding the implementation of anti-fraud strategies for commercial banks.

Rashid, A., Akmal, M., & Shah, S. M. A. R. (2024). Corporate governance and risk management in Islamic and convectional financial institutions: explaining the role of institutional quality. *Journal of Islamic Accounting and Business Research*, 15(3), 466–498. https://doi.org/10.1108/JIABR-12-2021-0317.

Republika. (2021). OJK ungkap kerugian perbankan akibat fraud capai Rp 4,62 T. https://ekonomi.republika.co.id/berita/qzxirv457/ojk-ungkap-kerugian-perbankan-akibat-fraud-capai-rp-462-t.

Roh, Y., Heo, G., & Whang, S. E. (2021). A Survey on Data Collection for Machine Learning: A Big Data-AI Integration *Perspective. IEEE Transactions on Knowledge and Data Engineering. IEEE Computer Society*. https://doi.org/10.1109/TKDE.2019.2946162.

Ross, S. A. (1973). The Economic Theory of Agency: The Principal's Problem. *The American Economic Review,* 63(2), 134–139. http://www.jstor.org/stable/1817064.

Russel, S.,Norvig, P. (2010). *Artificial Intelligence: A Modern Approach (3rd ed.)*, Prentice Hall.

Shoimah, I., Wardayati, S. M., & Sayekti, Y. (2021). Adaptasi Laporan Keuangan Pada Entitas Nonlaba Berdasarkan Isak 35 (Studi Kasus pada Universitas Ibrahimy Sukorejo Situbondo). *Jurnal Akuntansi dan Pajak*, 21(2). https://doi.org/10.29040/jap.v21i02.1388.

Solikin, I., & Darmawan, D. (2023). Impact of Artificial Intelligence in Improving the Effectiveness of Accounting Information Systems. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 14(2), 82–93. https://doi.org/10.58346/JOWUA.2023.I2.007.

Takyar, A. 2023. AI In Fraud Detection:Fortifying Business Againts Ever-Evolving Threats. https://www.leewayhertz.com/ai-in-fraud-detection/.

Tamrakar, R., Wani, N. (2021). Design and Development of Chatbot : A Review. *International Journal of Innovative Research in Technology* 9(12), 994-999.

Umamaheswari, S., Valarmathi, A., & Phil, M. (2023). Role Of Artificial Intelligence in The Banking Sector. *Journal of Survey in Fisheries Sciences,* 10(4S). http://sifisheriessciences.com/journal/index.php/journal/article/view/1722/1769

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 372-381. DOI: 10.1108/JFC-12-2017-0128.

Warren, C.S., Reeve, J.M, Duchac, J.E. (2018). Accounting (27th ed.). Cengage Learning. https://www.academia.edu/39308660/Cengage_Learning_Accounting_27th_Edition.

West, J., & Bhattacharya, M. (2021). Intelligent financial fraud detection practices: An investigation. *International Journal of Information Security and Privacy*, 15(1), 1-22. https://doi.org/10.4018/IJISP.2021010101

Widharto, P., Pandesenda, A.I., Yahya, A.N., Sukma, E.A., Shihab, M.R., Ranti, B. (2020). Digital Transformation Of Indonesia Banking Institution:Case Study Of PT. BRI Syariah. *International Conference on Information Technology System and Innovation (ICITSI).* DOI: 10.1109/ICITSI50517.2020.9264935.

Wolfe, D. T. and Dana R. Hermanson. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal* 74(12):38–42.

Yulisnawati, Y., Pramono, S. E., & Laela, S. F. (2024). Relationship of internal auditor independence, internal audit effectiveness and sharia compliance (Case study on sharia bank in East Java). *Inspirasi Ekonomi: Jurnal Ekonomi Manajemen*, 5(4), 350–362. https://doi.org/10.32938/ie.v5i4.6250.

Zheng, W., Cheng, J. Y., Wu, X., Sun, R., Wang, X., & Sun, X. (2022). Domain knowledge-based security bug reports prediction. *Knowledge-Based Systems,* 24, 108293. https://doi.org/10.1016/j.knosys.2022.108293.