Improving Information System Audit Security through Artificial Intelligence (AI) Technology Integration

Fajrillah[1], Shamir Hasyim Syarif[2], Nirmadarningsih Hiya[3]
[1,2]Manajemen, Fakultas Ilmu Sosial dan Humaniora, Universitas IBBI, Medan, Sumatera Utara, Indonesia
[3]Manajemen, Fakultas Ekonomi, Universitas Pembinaan Masyarakat Indonesia, Medan, Sumatera Utara, Indonesia
[1]fajrillahhasballah@gmail.com, [2]shamir.hasyim@gmail.com, [3]nirmadarningsih.hiya@gmail.com

Article Info

Article history:

Received May 26, 2025
Revised May 28, 2025
Accepted May 31, 2025

Keywords:

Information Systems Auditing
Artificial Intelligence
Cybersecurity
Data Analytics
Explainable AI
Data Governance

ABSTRACT

In today's digital age, information systems are the backbone of various organizations' operations, yet they are vulnerable to increasingly complex cybersecurity threats. Information system auditing plays a crucial role in ensuring system security and reliability, but conventional audit methods are beginning to face various limitations, particularly in handling large volumes of data and detecting threats quickly. This study aims to analyze the role, benefits, and challenges of integrating artificial intelligence (AI) technology into the information system audit process. Using a literature review method, this research found that AI can enhance audit effectiveness through data analysis automation, real-time fraud detection, and optimizing auditors' roles in strategic analysis. However, the implementation of AI still faces issues such as data quality, algorithm transparency, potential bias, auditor readiness, and the need for strong regulation and governance. This study recommends the need for synergy between technology, policy, infrastructure, and human resource competencies to ensure the effective and responsible implementation of AI in information system auditing in modern business environments.

Corresponding Author:

Fajrillah
Universitas IBBI
Email: fajrillahhasballah@gmail.com

1. INTRODUCTION

In today's digital era, information systems have become a vital part of the operations of various organizations, both in the business, government, and public service sectors. The increasing dependence on this information system is also in line with the increasing risk of increasingly complex cybersecurity threats. Various types of attacks such as malware, phishing, and data manipulation now appear with more sophisticated, structured patterns, and are difficult to detect manually. This condition requires organizations to have a more responsive and adaptive information system control and auditing mechanism to various potential threats.

Information system auditing plays an important role in ensuring the security, reliability, and compliance of systems with various operational standards and regulations. However, in the field, traditional auditing methods often face challenges, ranging from very large data volumes, speed of threat detection, to the accuracy of analysis of anomalous patterns that appear in the system [1]. This situation has led to the idea of integrating artificial intelligence (AI) technology into the information system audit process as a more effective solution.

AI technology offers the ability to quickly analyze large-scale data, identify unusual patterns, and provide early warning of potential threats. In addition, AI can also be used to automate routine audit processes, perform risk predictions, and compile recommendations for mitigation steps based on previous incident patterns [2]. With these advantages, AI integration is believed to be able to increase the effectiveness, efficiency, and accuracy of information system auditing in the modern business environment.

Based on this background, this article aims to examine the role and potential of AI integration in the information system audit process, starting from the benefits, applications, to the challenges of its implementation. This study was compiled through a descriptive research method with a literature study approach (library research), where data was obtained from various secondary sources such as scientific journals, books, industry reports, and other relevant publications. All data was then analyzed systematically to produce a comprehensive understanding of the topic discussed.

Based on the background that has been described, this study starts from several main problems that need to be studied further. First, what is the role of information system auditing in maintaining the security and reliability of system operations in the digital era that is increasingly vulnerable to cyber threats. Second, what are the challenges faced in the process of auditing information systems with conventional methods, especially in dealing with large data volumes and increasingly complex threats. Third, how the application of artificial intelligence (AI) technology can be integrated into the information system audit process to address various existing obstacles. Finally, this study also wants to find out what are the benefits and potential obstacles that may arise in the implementation of AI technology in information system auditing, both from technical and operational aspects in the modern business environment.

This study aims to comprehensively examine the role and urgency of information system auditing in dealing with cybersecurity threats in the digital era. In addition, this study aims to analyze various obstacles faced in the process of auditing information systems based on traditional methods, as well as to offer alternative solutions based on artificial intelligence technology. Furthermore, this study aims to identify the concept, application, and mechanism of AI integration in the process of auditing information systems, as well as explain the benefits that can be obtained and potential challenges that may be faced in its implementation. It is hoped that the results of this study can be a reference for practitioners, academics, and policy makers in improving the security and effectiveness of information system auditing in modern organizational environments.

2. METHOD

This study uses a descriptive method with a literature study approach (library research). This method was chosen because it is in accordance with the objectives of the study, namely to describe, explain, and examine the phenomenon of integration of artificial intelligence (AI) technology in the information system audit process without conducting direct experiments in the field or hypothesis testing.

The data sources in this study come from various secondary literatures relevant to the topics discussed. Data were collected from indexed scientific journals, reference books, industry research reports, conference proceedings articles, and technical guides that discuss information system auditing and the use of AI technology in the field of data security and information systems. All sources used were selected based on the criteria of validity, recency, and relevance to the focus of the research study.

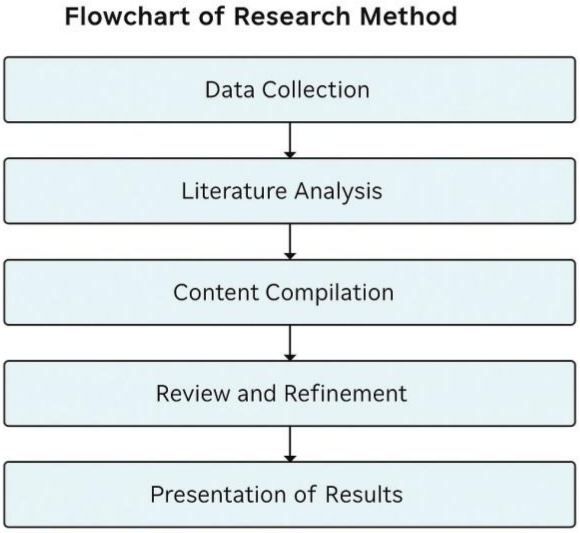
The methodological steps taken in this research include:

1. Data Collection
   Data was collected by searching and collecting various scientific publications, articles, reports, and other literature that discuss information system auditing and the application of AI technology in this field.
2. Literature Analysis
   The collected data is critically analyzed to identify concepts, important findings, technology trends, and problems faced in the audit process of conventional and AI-based information systems.
3. Content Preparation
   The results of the analysis are presented in the form of a systematic narrative description, including an explanation of the objectives, benefits, and potential for AI integration in improving the security and effectiveness of the information system audit process.
4. Review and Refinement
   Article content is reviewed to ensure accuracy, consistency, and completeness of information before being presented to readers.
5. Presentation of Results
   Articles are written in a scientific format with a regular structure, starting from the introduction, research methods, discussion, to the conclusion.

The data analysis technique used in this study is a critical and systematic analysis of literature content, namely by reviewing the contents of various references collected to find patterns, relationships, and key concepts related to the research topic. Through this approach, it is hoped that a comprehensive understanding can be obtained regarding the contribution of AI to the security and effectiveness of information system auditing in the digital era.

Table 1. Research Method Stages

No	Stage	Description
1	Data Collection	Collecting secondary literature from academic journals, books, research reports, and related articles.
2	Literature Analysis	Critically analyzing the content of the literature to identify key concepts, trends, and issues.
3	Content Preparation	Compiling the analysis results into a systematic and structured descriptive narrative.
4	Review and Refinement	Reviewing the article content to ensure accuracy, consistency, and completeness of the data.
5	Results Presentation	Preparing a complete scientific article from introduction to conclusion.



Fugure 1. Flowchat of Research Method

3. RESULTS AND DISCUSSION

3.1. Benefits of AI Integration in Information System Auditing

The integration of artificial intelligence technology into the information system auditing process provides a number of significant benefits. First, AI enables the automation of large amounts of data analysis quickly and comprehensively, replacing traditional audit sampling methods. This technology is capable of processing all transactions and data activities in the system, thereby minimizing the risk of missing anomalies or undetected fraud [3]. A study by Vinayakumar et al. [4] shows that deep learning-based AI can detect attack patterns that were previously unrecognized by manual methods.

AI supports real-time fraud and risk detection through the application of machine learning, natural language processing (NLP), and anomaly detection. This technology allows audit systems to provide early warning of potential threats before damage escalates [5]. AI improves operational efficiency and auditor productivity. Routine audit processes can be automated, allowing auditors to focus more on strategic analysis and decision-making based on AI analysis results [6].

Table 2. Benefits of AI Integration in Information Systems Auditing

No	Benefit	Description
1	Automation of Big Data Analysis	Processing all transactions, not just samples.
2	Real-Time Fraud and Anomaly Detection	Early warnings through AI-based machine learning.
3	Improved Auditor Efficiency and Productivity	AI takes over routine audit tasks, allowing auditors to focus on strategic analysis.

3.2. Challenges of AI Implementation in System Audit

Although it offers many advantages, the implementation of AI in information system auditing faces various challenges. First, related to data quality and integrity. AI relies heavily on clean, complete, and relevant data. Bad data can lead to biased or misinterpreted analysis results [7].

Transparency and explainability challenges. Many AI algorithms, especially deep learning, are black box in nature, making it difficult to explain how the AI arrived at a decision. This can hamper the acceptability of audit results [8]. ethical issues and algorithmic bias. AI can introduce unintentional discrimination, especially in the areas of finance or automated selection [9]. Lack of auditor competence in AI technology. Training and capacity building of auditors are needed to understand how AI works and interpret results [10]. The regulatory and governance aspects of AI are still developing. Regulations are needed to address privacy, data security, and accountability for AI audit results [11].

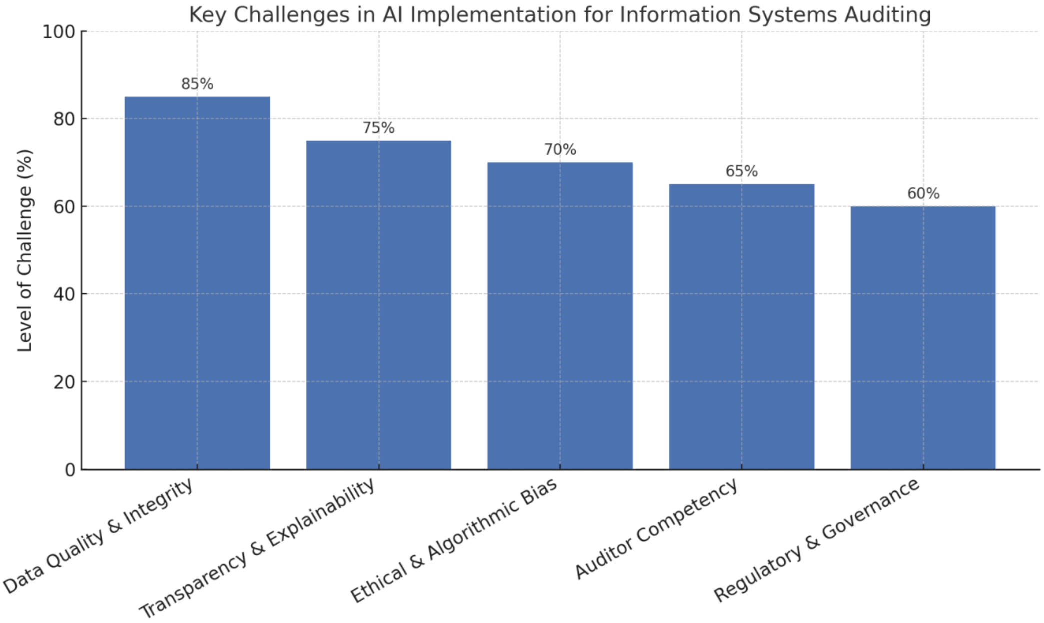


Figure 2. Key Challenges of AI Implementation in System Audit
(visual bar chart per challenge category: data quality, transparency, ethics, competence, regulation)

3.3. Supporting Factors for Successful AI Implementation

The success of AI implementation in auditing is not only determined by technology, but also by non-technical factors. First, the existence of adequate policies and governance related to the use of AI in system audits [12]. Second, investment in technology infrastructure and a strong data culture in the organizational environment are important foundations [13].

Third, collaboration between auditors and AI experts needs to be built. Continuous training is a prerequisite for aligning understanding between AI systems and auditors [14]. Fourth, the adoption of Explainable AI (XAI) is a solution to the challenges of transparency and accountability of AI-based audit results [15].

3.4. Implications for IT Auditing Practices

The adoption of AI in information systems auditing brings strategic implications for the world of the audit profession. Auditors in the future will not only dig up data and create reports, but also become strategic advisors for management [16]. In addition, the curriculum for professional auditor education and training needs to integrate AI, data analytics, and technology ethics materials [17]. Organizations also need to develop technology oversight policies (‘human-in-the-loop’) and a strict data and AI governance framework [18].

The integration of AI in information system auditing has great potential in improving the security, efficiency, and accuracy of the audit process. AI is able to detect anomalies and risks in real-time, and support auditors to focus on strategic analysis. However, challenges of data quality, transparency, bias, auditor competence, and regulatory frameworks are still issues that need to be managed comprehensively. The success of implementing AI in system auditing depends heavily on the synergy between intelligent technology, good governance, and human resource capacity.

4. CONCLUSION

In the digital era full of cybersecurity risks, information system auditing plays a vital role in maintaining the integrity and reliability of organizational operations. However, traditional audit methods are starting to face limitations, especially in handling large volumes of data and detecting increasingly complex threats. The integration of artificial intelligence (AI) technology is here as a solution that offers speed, accuracy, and real-time anomaly detection capabilities.

The results of this study show that AI can improve audit effectiveness and efficiency through big data analysis automation, early fraud detection, and support auditors to focus more on strategic analysis. However, its implementation still faces a number of challenges, such as data quality issues, algorithm transparency, potential bias, auditor competency readiness, and AI regulation and governance that are not yet fully mature.

The success of AI implementation in information system audit is not only determined by the sophistication of technology, but also by the readiness of the organization in terms of infrastructure, policies, data culture, cross-skill collaboration, and adoption of Explainable AI (XAI) principles. With the right approach, AI integration has great potential to become a new standard in modern audit practices, while strengthening cybersecurity systems in an increasingly dynamic business environment.

REFERENCES

[1] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, dan S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[2] G. Nguyen *et al.*, "Machine Learning and Deep Learning Frameworks and Libraries for large-scale Data Mining: A Survey," *Artif. Intell. Rev.*, vol. 52, no. 1, pp. 77–124, 2019, doi: 10.1007/s10462-018-09679-z.

[3] MindBridge, "Artificial intelligence in auditing: Increasing trust through automation," *Financial Times*, 2021. [Online]. Available: https://www.ft.com/content/bd9c415f-cab5-4ae1-8bf2-a17c57f9b5db

[4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[5] G. Nguyen et al., "Machine learning and deep learning frameworks and libraries for large-scale data mining: A survey," *Artificial Intelligence Review*, vol. 52, no. 1, pp. 77–124, 2019, doi: 10.1007/s10462-018-09679-z.

[6] DiVA Portal, "Integration of Artificial Intelligence in Auditing: The Effect on Auditor Performance," *Uppsala University*, 2020. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1446778/FULLTEXT01.pdf

[7] J. Kim and S. Park, "The effects of data quality on AI audit performance," *Journal of Information Systems*, vol. 34, no. 3, pp. 85–107, 2020.

[8] Wikipedia, "Automated decision-making," 2023. [Online]. Available: https://en.wikipedia.org/wiki/Automated_decision-making

[9] M. Brundage et al., "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," *arXiv preprint arXiv:1802.07228*, 2018.

[10] K. Kokina and T. Pachamanova, "Artificial intelligence in accounting: Opportunities and challenges," *Journal of Emerging Technologies in Accounting*, vol. 17, no. 1, pp. 91–100, 2020.

[11] R. Binns, "Fairness in machine learning: Lessons from political philosophy," *Proceedings of the 2020 ACM Conference on Fairness, Accountability, and Transparency (FAT)*, pp. 149–159, 2020.

[12] H. Yu et al., "Building ethical AI governance," *Nature Machine Intelligence*, vol. 1, no. 6, pp. 261–263, 2019.

[13] S. Ransbotham et al., "Expanding AI's impact with organizational learning," *MIT Sloan Management Review*, vol. 61, no. 1, pp. 1–10, 2019.

[14] Deloitte, "AI and audit: Navigating ethical risks and governance," *Deloitte Insights*, 2021.

[15] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, 2018.

[16] PwC, "AI in audit: Changing the role of the auditor," *PricewaterhouseCoopers*, 2020.

[17] K. Alles, "Educating auditors in artificial intelligence: A call for action," *International Journal of Accounting Information Systems*, vol. 36, 2020.

[18] European Commission, "Ethics guidelines for trustworthy AI," *European Union Publications*, 2019.