Indonesia Accounting Research Journal, 13 (4) (2026), pp. 296-306

Published by: Institute of Accounting Research and Novation (IARN)

Indonesia Accounting Research Journal

Journal homepage: https://journals.iarn.or.id/index.php/IARJ/index

Automated Z-Score method for fraud detection in rural credit banks

Nano Suyatna

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

Article Info

Article history:

Received March 12, 2026
Revised May 10, 2026
Accepted Jun 17, 2026

Keywords:

Agile Software Development;
Accounting Information System;
Early Warnings;
Real-time Monitoring;
Z-Score and Interquartile Range.

ABSTRACT

This research proposes a new transaction monitoring framework using AIS, integrating Z-Score and Interquartile Range methods into a real-time system for fraud detection and early warning in Rural Credit Banks. The previous studies on fraud detection have been mainly oriented towards analytical models and machine learning approaches. Very little attention has been paid to integrating lightweight statistical anomaly detection approaches in operational Accounting Information Systems. Unlike traditional AIS-based monitoring systems that rely on periodic audits and manual supervision, the proposed framework enables continuous statistical anomaly detection in a real-time AIS environment based on computationally efficient methods. The main contribution of this work is not the development of new statistical techniques, but the operational integration of statistical anomaly detection methods into an AIS-based monitoring environment. The framework was conceptually designed using an Agile Software Development approach to classify transactions as normal or suspicious based on Z-Score and IQR calculations. A preliminary empirical validation was conducted on a synthetic banking transaction dataset with 852 transactions. The framework also achieved detection accuracy of 98.00%, precision of 92.38%, recall of 100%, and F1-score of 96.04%. The findings indicate that the incorporation of statistical anomaly detection methodologies within AIS environments can improve internal control, boost the efficiency of transaction monitoring, and support the prevention of fraud in Rural Credit Banks and similar financial entities.

Corresponding Author:

Nano Suyatna,
Department of Computerized Accounting, Faculty of Computer,
Ma'soem University,
Cipacing Highway No. 22 Jatinangor District. Jatinangor, Sumedang, West Java, Zip Code 45363, Indonesia
Email: nanosuyatna@masoemuniversity.ac

1. INTRODUCTION

With the arrival of information technology, banking activities across the world have been revolutionized by the usage of integrated banking systems and Accounting Information Systems (AIS). Such systems increase the efficiency of transaction processing, financial data management, and operational decision-making (Devineni et al., 2023). But the growing complexity and volume of digital transactions have also raised fraud risk in both developed and developing countries. Poor internal controls and ineffective transaction monitoring create opportunities for transaction manipulation, unauthorized fund transfers, and irregular financial reporting, which increases the likelihood of undetected fraud and reduces public trust in financial institutions (Al-Ababneh et al., 2025; Singh,

2024). The theory of Fraud Triangle Approach argues that the chance for fraudulent activity within organizations is created through ineffective monitoring mechanisms.

Financial institutions all over the world have used several methods of fraud detection such as rule based systems, statistical anomaly detection, data mining and machine learning techniques. Machine learning techniques such as neural network, decision tree and support vector machine are powerful in prediction and can manage enormous transaction database. However, these methods require enormous computer resources, big labeled datasets and complex model training processes. On the other hand, statistical anomaly detection methods such as Z-Score and Interquartile Range (IQR) are more transparent, computationally efficient, scalable, and easier to integrate into operational financial systems, especially for small-scale financial institutions lacking technological infrastructure(Olateju et al., 2024). However, statistical procedures are less flexible to highly dynamic fraud patterns in comparison to sophisticated machine learning techniques. This indicates that the choice of fraud detection techniques should include organizational competence, operational needs and the scalability of the system.

The difficulties are especially problematic for Rural Credit Banks (BPR) in Indonesia and other microfinance institutions in developing countries, because they often operate with minimal financial resources, poor technology infrastructure and limited human resource capability. Some BPRs have recently had to close down or have encountered financial difficulties because of weak internal controls, risk management incompetence and inadequate oversight of transactions. From the standpoint of Agency Theory, the asymmetry of information between management and stakeholders may result in opportunistic conduct and opacity in financial reporting. Such conditions imply that traditional AIS-based monitoring systems are still predominantly reactive as transaction supervision is still largely dependent on periodic audits, manual inspection and post-transaction review processes as opposed to continuous real-time monitoring mechanisms.

Much of the existing literature has focused on fraud detection models and prediction methods. However, most of the existing research has been dedicated to developing algorithms and assessing prediction performance, with little attention paid to the operational implementation of anomaly detection mechanisms into AIS systems. Many financial organizations still have AIS installations that are mostly transaction recording and reporting systems without the capability of real-time statistical monitoring. Previous studies tend to focus on complex machine learning architectures and large-scale banking datasets, with less attention given to simple, scalable and computationally efficient techniques that can be used in smaller financial institutions. The research gap, therefore, is not the lack of use of statistical approaches in fraud detection research, but the lack of integrated AIS-based monitoring frameworks that can facilitate continuous, real-time and scalable anomaly detection in operational financial systems.

This gap leads to the presentation of a conceptual AIS-based transaction monitoring framework in this work, which integrates Z-Score and Interquartile Range (IQR) approaches in a real-time fraud monitoring and early warning setting. The main contribution of this study is not the development of new statistical methods or a standalone prototype application, but the conceptual integration of the three elements of Accounting Information Systems, statistical anomaly detection mechanisms and automated monitoring processes into a unified fraud monitoring architecture.The proposed framework is designed to facilitate the continuous monitoring of transactions, detection of suspicious transaction patterns and enhancement of internal control mechanism in the Rural Credit Banks and similar financial institutions.

The author of the study bases the research questions on the literature of fraud detection in accounting information systems, statistical anomaly detection, and the fraud detection systems:

RQ1. In what ways does the accounting information system in rural credit banks enable the detection of fraud and the monitoring of transactions?

RQ2. In what ways is it possible to apply Z-Score, Interquartile Range methods, and other statistical anomaly detection techniques to the fraud detection and monitoring systems?

RQ3. In what ways does fraud detection and monitoring integrate Z-Score and Interquartile range to the fraud detection and monitoring systems?

RQ4. In what ways does the rural credit banks integrated accounting systems and fraud monitoring systems provide the rural credit banks with internal controls and fraud detection?

In the banking sector, fraud could be in the form of tampered transactions, illegal money transfers, or falsified banking records. Fraud is a crime. It causes financial loss and diminishes the confidence of the public, which underlines the importance of strong fraud detection and prevention systems and counter measures (Rojan, 2024). Technological advancement has led to the Automation of the Accounting Information Systems (AIS). With the Automation of the AIS, recording, processing and storage of financial transactions has supported and improved management decision processes. Furthermore, the Advancement of technology has allowed the Automation of the AIS to aid continuous transaction monitoring and transactions evaluations, thereby helping organizations in the early detection of unusual or anomalous financial transactions and/or activities (Devineni et al., 2023; Rojan, 2024). The Improvement of the Automation of the AIS improves operational control and clarity in Rural Credit Banks by the Improvement of a well organized Process of transactional record management. Furthermore, Automation of the AIS can serve as a tool or means of enhancing Managing the processes of Fraud Detection and/or Prevention.

Detecting fraud is an analytical process and technique of identifying data that is significantly different from what is considered normal. In the context of financial transactions, anomalies may suggest an operational mistake or, in the worst case, fraud (Karshiyev, 2025). The Z-Score method is one of the most commonly used methods. It shows how far a transaction value is from the mean of the dataset in terms of standard deviation. In other words, transactions that have a very high or very low Z-Score, deviate from the norm, and in that sense, may become an anomaly. The other well-known method is the Interquartile Range (IQR). It shows the spread of data using the difference between the first (Q_1) and third (Q_3) quartiles as the range of the data. Any transaction that falls out of the IQR limits is considered an outlier. Z-Score and IQR methods help one another. When used together, they enhance fraud anomaly analysis. It is due to the reason that they have different ways of looking at the distribution of data (Ma'muriyah et al., 2025). The more unusual financial transaction, the more data distribution fraud is in the system.

The development of Information Technology (IT) encourages institutions to develop automated systems for real time tracking of financial dealings. These systems streamline analysis of enormous amounts of transaction data and recognize unusual behavior more efficiently than manual tracking (Hu, 2025; Udeh et al., 2024). The addition of analytical tools to Accounting Information Systems augments the efficacy of their monitoring capabilities. These tools assist the systems in the analysis of transaction data, identification of outlier transactions, and construction of detection systems that may even signal fraudulent behavior before it occurs. Thus, the addition of statistical anomaly detection systems such as Z-Score and IQR will allow transaction monitoring systems to automatically identify unusual transactions, and allow financial institutions to approach data analysis in a more comprehensive manner (Herreros-Martínez et al., 2025).

Systems for monitoring activities using technology are able to analyze data from numerous monetary transactions and are able to analyze this data for the instance of fraudulent activities on an ongoing basis. Techniques that are automated allow organizations to identify actions that are suspicious much more rapidly than a human auditor would be able to do. Previous research, for instance, Antwi et al. (2024), have posited that strengthening the internal control structures and improving the monitoring capabilities of a control system can be achieved when accounting information systems are integrated with some form of analytical approach. The system, upon automatically identifying an anomalous transaction, has the capability to create notifications to be sent to management and auditors so that they can conduct additional inquiries. Applying monitoring systems that can detect fraud in advance can be beneficial to Rural Credit Banks and decrease the possibility of financial loss from fraud.

2. RESEARCH METHOD

The purpose of this research is to develop a Transaction Monitoring Framework on an Accounting Information System (AIS) to detect the Fraud in Rural Credit Banks (BPR) utilizing the Research and Development (R&D) technique in the conceptual design phase (Hansen et al., 2022).

The R & D method is useful because it can provide a mental picture of the system that can be used, tried, and improved in further study (Aulia & Putra, 2025; Peña & Castro, 2024). The project is mainly focused on designing the system architecture, framework for identifying anomalies, and monitoring systems for early detection of fraud in AIS environments (Abbasi et al., 2012; Waldner et al., 2017). Apart from conceptual modeling, the research also adopts a simulated banking transaction dataset for simulation based evaluation, thereby offering some initial empirical support for the suggested technique. We need to know what Rural Credit Banks are looking for in their transaction monitoring systems in order to start the study. This includes the presentation of financial transaction data, what management and internal auditors want from these systems and the role of AIS in transaction surveillance. AIS facilitates in tracking, capturing and storing financial transactions (Romney, M. B., Steinbart, 2020). It also assists in internal control, and in monitoring of a firm. The results of this step form the basis of the conceptual monitoring framework (Devineni et al., 2023). The second phase is to design the overall structure of the monitoring system. The design incorporates modules for transaction processing, problem detection, and monitoring approaches, and management and internal auditor systems that issue reports or warnings of problems. With this stage we will build a tracking model that can examine financial transactions in a planned way to discover strange tendencies that could indicate fraud. In the field of information systems, conceptual system modeling is often used to explain how the different parts of the system work together before being put into operation (Laudon,K C., & Laudon, 2020). A third stage is to model and mimic, conceptually, statistical anomaly detection approaches such as the Z-Score and Interquartile Range (IQR) methodologies. In this study, the proposed methodology was tested on a simulated financial transaction dataset of 852 transactions. The collection comprised regular transaction patterns, high-value transaction situations, duplicate transactions, and purposely aberrant transactions that could point to fraud. Simulation dataset was generated to simulate the usual banking transactions taking place at the Rural Credit Banks. This encompasses payments, withdrawals, transfers and transaction spikes. The suggested AIS based monitoring system was used to handle these transaction scenarios in order to evaluate the capability of the system in detecting the abnormal transactions under the varied operational situations.

Standard deviation and the Z-Score technique were used to calculate the number of transactions that deviated from the dataset mean. Transactions with $|Z| > 3$ (absolute value of Z-Score larger than 3) were studied. These transactions were not normal, hence in normally distributed datasets, values more than three standard deviations from the mean are considered statistically extreme deviations (George et al., 2024). This level was set to minimize the rate of false alarms while being sensitive to unusual transaction patterns.

The Outlier agreements were identified based on the Interquartile Range (IQR) method using the quartile distribution boundaries (George et al., 2024). The lower and upper bounds were obtained using the standard IQR method: Lower Bound = Question 1 – (1.5 * IQR) and Lower Bound = Q1 - (1.5 * IQR). Transactions outside these constraints were regarded with suspicion. For detecting statistical anomalies, the IQR threshold of 1.5 was chosen as it is commonly used in research to identify extreme outliers and is able to capture the skewed distribution of financial transactions (Ma'muriyah et al., 2025). Our methodology can detect both statistically different transactions and trends that do not follow the distribution by using Z-Score and IQR together.

The numerical performance metrics, such as accuracy, precision, recall and F1-score, were used to evaluate the performance of the anomaly identification. The F1-score, accuracy, precision, and recall to find odd transactions of the proposed model were 96.04%, 99.00%, 92.38%, and 100% correspondingly. The results suggest that the integration of Z-Score and IQR in the AIS-based monitoring framework was effective in identifying aberrant transaction trends and issuing timely fraud alerts in the simulated banking environment.

The second to last part is the study of the suggested tracking system and the simulation results. This review studies the synergy between AIS transaction processing and statistical anomaly detection and the extent to which the framework may be applied to real time transaction tracking and alerts on fishy transactions. Antwi et al. (2024). contend that the incorporation of analytical approaches into tracking systems can lead to enhancement of internal controls and ease in identification of fraud. The analysis of the simulations and the proposed architecture seems to make it plausible to incorporate statistical anomaly detection methods in AIS based transaction monitoring systems for Rural Credit Banks.

3. RESULTS AND DISCUSSIONS

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily (Bayraksan & Love, 2015)(Jiang & Guan, 2016). The discussion can be made in several sub-chapters.

3. 1. Results

3.1.1 Transaction monitoring results based on simulation

The work has been simulated with a banking transaction dataset of 852 transactions that includes both typical and aberrant transaction patterns to give a preliminary empirical validation. The simulated dataset was run through the proposed AIS based transaction monitoring system integrating Z-Score and Interquartile Range (IQR) methodologies.

The confusion matrix of the proposed model is presented as follows:

Table 1 The confusion matrix of the proposed model

Actual Condition	Predicted Normal	Predicted Anomaly
Normal Transaction	629 (TN)	17 (FP)
Anomalous Transaction	0 (FN)	206 (TP)

The simulation results suggest that the proposed framework successfully identified:

Table 2. Simulation-Based Transaction Monitoring Results

Classification Category	Description	Total Transactions
True Positive (TP)	Anomalous transactions correctly detected	206
True Negative (TN)	Normal transactions correctly classified	629
False Positive (FP)	Normal transactions incorrectly classified as anomalies	17
False Negative (FN)	Anomalous transactions not detected	0

Based on the examination of confusion matrix, the proposed framework achieved:

Table 3. Performance Metric Description Outcome

Performance Metric	Description	Result
Accuracy	Overall correctness of anomaly detection classification	98.00%
Precision	Percentage of detected anomalies that were truly anomalous	92.38%
Recall	Percentage of anomalous transactions successfully detected	100%
F1-Score	Harmonic mean of precision and recall	96.04%

The performance metrics indicate that the proposed AIS-based anomaly detection framework has successfully detected suspicious transaction patterns in the simulated banking environment.
Performance Metrics of Proposed AIS Based Fraud Detection Framework

Figure 1. Results of simulation based evaluation using 852 banking transactions.

3.1.2 Evaluation of Scenarios

To assess the capabilities of the proposed framework under various transaction settings, three transaction scenarios were simulated:

Table 4. Evaluation of scenarios

Scenario	Description	Detection Result
Normal Transactions	Transactions within normal statistical distribution	Correctly classified as normal
High-Value Transactions	Transactions significantly above average values	Detected as anomalous using Z-Score
Extreme Outlier Transactions	Transactions outside quartile boundaries	Detected as anomalous using IQR

The scenario-based evaluation showed that the suggested framework was able to detect both of statistically deviated transactions and extreme outlier transactions. The Z-Score approach efficiently recognized the transactions with substantial deviations from the mean of the dataset, while the IQR method successfully identified the transactions outside the usual quartile distribution range.

3.1.3 Results of the Monitoring Architecture Based on AIS

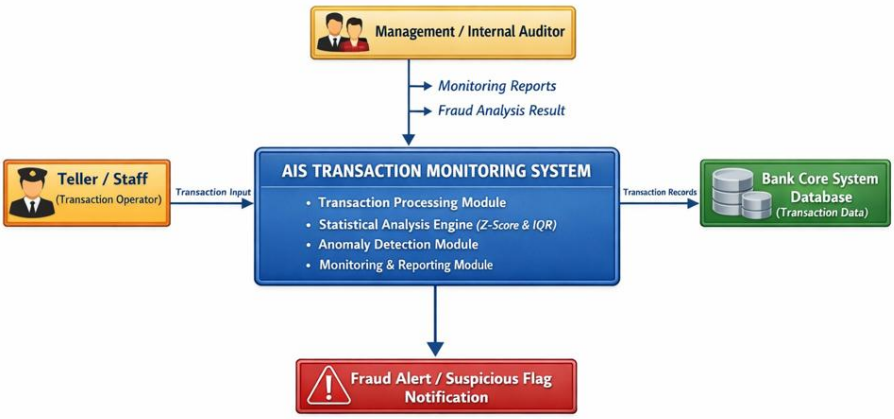

Figure 2. AIS-Based transaction monitoring system

The conceptual architecture of the AIS-based transaction monitoring system is illustrated in Figure 1. The design incorporates transaction processing modules, anomaly detection engines, monitoring mechanisms and fraud alert systems inside a single AIS environment. The architecture presented enables constant monitoring of transactions and automatic issuance of alerts on fraud to management and internal auditors.

3.1.4 Results of Early Warning and Fraud Alert

The simulation findings further showed that transactions identified as abnormal immediately triggered fraud alerts and risk notifications within the monitoring system. The early warning mechanism enables the reporting of questionable transactions in real time via the monitoring dashboard, hence aiding speedier management reaction and fraud investigation processes.
Based on the transaction simulation results:

Table 5. Detected Anomalies

Anomaly Detection Category	Description	Total Transactions
WARNING ML	Transactions detected as anomalous by the ML-based detection mechanism	162
WARNING IQR & ML	Transactions detected simultaneously by both IQR and ML mechanisms	44
WARNING IQR	Transactions detected as anomalous by the IQR method	17
Total Detected Anomalies	Total anomalous transactions identified by the framework	223

Therefore:

$$\text{Detected Anomalies} = 162 + 44 + 17 = 223$$

Since all anomalous transactions in the dataset were successfully identified, then:

$$\text{Total Actual Anomalies} = 223$$

The Detection Rate calculation is:

$$\text{Detection Rate (\%)} = \frac{\text{Detected Anomalies}}{\text{Total Actual Anomalies}} \times 100 \quad \text{..... (1)}$$

$= 223/223 \times 100$
$= 1 \times 100$
$= 100\%$

Table 6 Detected Anomalies

Metric	**Value**
Detected Anomalies	223
Total Actual Anomalies	223
Detection Rate	100%

The suggested AIS-based anomaly detection system could detect all the anomalous transactions present in the simulated dataset of banking transactions. It can be observed that the integrated Z-Score and IQR monitoring algorithms successfully discovered all the 223 actual anomalous transactions, resulting in a detection rate of 100% . This result demonstrates that the proposed framework has shown high ability of discovering suspicious transaction patterns without missing anomalous cases in the simulation process.

3.2 Discussion

The simulation results indicate that the use of statistical anomaly detection methods with an AIS-based transaction monitoring framework can improve the fraud monitoring capability of small-scale financial institutions like Rural Credit Banks(Tiwari, 2025). In contrast to prior work that focused primarily on conceptual system design or the construction of analytical models, this work presents initial empirical evidence through simulation-based evaluation and quantitative performance analysis(Al-Ababneh et al., 2025). The suggested framework is able to identify anomalous transaction pattern in the simulated banking dataset with 98.00% accuracy, 92.38% precision, 100% recall and 96.04% F1-score.

The 100 % recall result is of special interest as it implies that no aberrant transactions were missed in the review process. In fraud detection systems, unnoticed anomalies may lead to financial losses, inefficient internal control mechanisms and diminished institutional credibility. The high values of accuracy and precision also show that the framework was able to distinguish between routine

and suspicious transactions with relatively low rates of false detection. These results imply that very simple statistical methods can nevertheless give high anomaly detection capacity in structured financial transaction contexts(Gkegkas et al., 2025).

This study also presents an analytical comparison between statistical anomaly detection methods and machine learning methods. Machine learning techniques such as neural networks, random forest and support vector machines are well known for their powerful predictive ability and flexibility to complicated fraud patterns(Tieu & Tran, 2026). However, these methods often demand huge labeled datasets, significant computer resources, extensive training processes, and specialist technical knowledge. On the other hand, the Z-Score and IQR approaches employed in this work are simpler, more clear, computationally efficient and easier to be integrated in operational Accounting Information Systems. Hence, statistical methods may be more suitable for small-scale financial organizations with limited technology infrastructure and constrained human resources.

The scenario-based evaluation also highlights the complimentary capacity of Z-Score and IQR approaches. The Z-Score technique was successful in identifying transactions with considerable deviations from the average of the dataset, particularly for large-value transactions. Meanwhile the IQR technique was more effective to identify extreme outlier transactions outside the quartile distribution bounds. Therefore, the combination of both methodologies enhanced the coverage of anomaly identification by fusing deviation-based and distribution-based anomaly analysis. This combination reduced the likelihood of detecting suspicious transactions in the simulated monitoring environment.

From the standpoint of Fraud Triangle Theory, the suggested monitoring system decreases the potential of fraud by boosting transaction supervision and raising the possibility of detecting abnormalities in operational banking activities(Tieu & Tran, 2026)(Kramer, 2015)(Julian et al., 2022)(Rizani & Respati, 2018)(Saleh et al., 2021). Automated monitoring techniques may lower the opportunity factor of fraud, as suspicious transactions may be recognized more immediately using continuous monitoring processes(Jarugula, 2025)(Jones & Free, 2026) . Besides, the implementation of anomaly detection methods in AIS systems is also in favor of Agency Theory since the real-time monitoring of transactions can lessen the information asymmetry between management and stakeholders by enhancing transparency of transactions and efficacy of internal controls(Alfawareh et al., 2025).

The suggested paradigm is especially crucial for practical implications for Rural Credit Banks (BPR) and comparable small-scale financial institutions. Unlike sophisticated machine learning algorithms that are expensive to deploy due to the need for costly infrastructure, specialized expertise, and high implementation costs, the Z-Score and IQR methods utilized in this framework are reasonably inexpensive and easy to implement in existing AIS setups. This issue is especially critical for BPRs that generally operate with inadequate technological infrastructure, limited financial resources, and limited IT professionals. Financial firms can do real-time transaction monitoring with light statistical methods without having to spend heavily in AI infrastructure or advanced analytical systems. The suggested architecture thus provides a viable and scalable strategy for fraud monitoring that is appropriate for smaller financial institutions.

The framework also exhibits concrete advantages in terms of simplicity of implementation and operational integration. The Z-Score and IQR approaches are based on fairly simple statistical computations, therefore the monitoring mechanism can be embedded into existing AIS platforms without requiring large modifications to banks operational systems. This simplicity may aid in deployment, maintenance expenses of the system, and training of internal auditors and management professionals(Dongre et al., 2025). Thus, the framework can help in quicker deployment of automated fraud monitoring methods in Rural Credit Banks and comparable institutions.

Theoretically, this work adds to the progression of Accounting Information Systems (AIS) from traditional transaction processing and reporting systems to intelligent and proactive monitoring systems. Typically, traditional AIS are meant to assist transaction recording, financial reporting, and post-audit control activities. However, the integration of statistical anomaly detection mechanisms

and automated early warning systems into AIS environments shows the potential transformation of AIS into continuous real-time monitoring platforms able to support predictive fraud detection and dynamic internal control functions. Therefore, this paper broadens the theoretical function of AIS from administrative and reporting tasks to emphasizing the integration of analytical monitoring activities into operational financial systems.

Compared with earlier work that has mostly been concerned with algorithm design or prediction performance of models, this work complements that by a conceptual integration of statistical anomaly detection mechanisms into practical AIS-based monitoring systems. Therefore, the contribution of this study is not in the development of new statistical methods, but in demonstrating how simple statistical approaches such as Z-Score and IQR can be operatively integrated into real-time transaction monitoring architectures to support fraud prevention and internal control mechanisms in small-scale financial institutions.

4. CONCLUSION

This research proposes a conceptual transaction monitoring framework based on AIS which combines Z-Score and Interquartile Range (IQR) methods in a real-time fraud monitoring and early warning system for Rural Credit Banks (BPR). The main contribution of this study is the integration of Accounting Information Systems, statistical anomaly detection and automated monitoring in a unified fraud monitoring framework. The study shows how simple and computationally efficient statistical methods, when combined, can support continuous transaction monitoring and fraud detection in AIS environments, rather than developing new statistical methods. The study also proposes a conceptual framework and a prototype model based on simulation for an AIS-based fraud monitoring system. The simulation results show that the proposed framework obtained 98.00% accuracy, 92.38% precision, 100% recall and 96.04% F1-score in detecting anomalous transactions. These results indicate that the combination of Z-Score and IQR methods in AIS-based monitoring systems can be useful in detecting suspicious transaction patterns and facilitating early warning systems for fraud detection. Theoretically, this research advances the development of Accounting Information Systems from conventional transaction recording systems to intelligent and proactive monitoring systems that facilitate real-time anomaly detection. In practice, the proposed framework provides a low-cost, transparent and scalable monitoring solution for small financial institutions that have limited technological resources. However, this study is limited to a conceptual design and simulation-based evaluation using simulated transaction datasets and has not been tested in real banking environments. Therefore, future work should be addressed on the implementation of the framework using real transaction datasets and the integration of machine learning or artificial intelligence techniques for improving the fraud detection capability, scalability and real-time monitoring performance in large-scale and big-data transaction environments.

REFERENCES

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). Metafraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly: Management Information Systems*, *36*(4), 1293-1327.A12. https://doi.org/10.2307/41703508

Al-Ababneh, H. A., Onyshko, O., Panchenko, A., Shashyna, M., & Barinov, O. (2025). USING ARTIFICIAL INTELLIGENCE FOR DIGITAL FINANCIAL TRANSACTION MONITORING. *Journal of Theoretical and Applied Information Technology*, *103*(24), 10358–10372. https://www.scopus.com/inward/record.uri?eid=2-s2.0-105028105281&partnerID=40&md5=53556c9f2c3c692fb5bdd70e327f62a8

Alfawareh, F. S., Al-Kofahi, M., Erman Che Johari, E., & Chai-Aun, O. (2025). Digital payments, ownership structure, and bank performance: insights from Jordan. *International Journal of Bank Marketing*, *43*(2), 262–291. https://doi.org/10.1108/IJBM-01-2024-0062

Antwi, B. O., Adelakun, B. O., & Eziefule, A. O. (2024). Transforming Financial Reporting With AI: Enhancing Accuracy and Timeliness. *International Journal of Advanced Economics*, *6*(6), 205–223. https://doi.org/10.51594/ijae.v6i6.1229

Aulia, M. R., & Putra, Y. H. (2025). Prototype a Decision Support Framework for Fraud Detection in Accounting Information Systems. *Proceeding of International Conference on Business Economics Social Sciences and*

Humanities, *8*, 139–144. https://doi.org/10.34010/icobest.v8i.687

Devineni, S. K., Kathiriya, S., & Shende, A. (2023). Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity. *Journal of Artificial Intelligence & Cloud Computing*, 1–9. https://doi.org/10.47363/jaicc/2023(2)184

Dongre, P. K., Patel, V., Bhoi, U., & Maltare, N. N. (2025). An outlier detection framework for Air Quality Index prediction using linear and ensemble models. *Decision Analytics Journal*, *14*. https://doi.org/10.1016/j.dajour.2025.100546

George, E. P., Idemudia, C., & Ige, A. B. (2024). Predictive Analytics for Financial Compliance: Machine Learning Concepts for Fraudulent Transaction Identification. *Open Access Research Journal of Multidisciplinary Studies*, *8*(1), 15–25. https://doi.org/10.53022/oarjms.2024.8.1.0041

Gkegkas, M., Kydros, D., & Pazarskis, M. (2025). Using Data Analytics in Financial Statement Fraud Detection and Prevention: A Systematic Review of Methods, Challenges, and Future Directions. *Journal of Risk and Financial Management*, *18*(11). https://doi.org/10.3390/jrfm18110598

Hansen, C. A., Arlitt, R., Eifler, T., & Deininger, M. (2022). Design by Prototyping: Increasing Agility in Mechatronic Product Design Through Prototyping Sprints. *Proceedings of the Design Society*, *2*, 201–210. https://doi.org/10.1017/pds.2022.22

Herreros-Martínez, A., Magdalena-Benedicto, R., Vila-Francés, J., Serrano-López, A. J., Pérez-Díaz, S., & Martínez-Herráiz, J. J. (2025). Applied Machine Learning to Anomaly Detection in Enterprise Purchase Processes: A Hybrid Approach Using Clustering and Isolation Forest. *Information (Switzerland)*, *16*(3). https://doi.org/10.3390/info16030177

Hu, N. (2025). Influence and Applications of AI in Accounting and Audit Practice. *Advances in Economics Management and Political Sciences*, *219*(1), 28–38. https://doi.org/10.54254/2754-1169/2025.gl27242

Jarugula, S. (2025). AI-Driven Real-Time Transaction Monitoring and Automated Threat Response : Revolutionizing Payment Security. *International Journal on Science and Technology (IJSAT)*, *16*(1), 1–14.

Jones, S., & Free, C. (2026). What accountants need to know about artificial intelligence and machine learning: a review and call for future research. *Journal of Accounting Literature*, *48*(5), 133–158. https://doi.org/10.1108/JAL-12-2025-0693

Julian, L., Johari, R. J., Said, J., & Wondabio, L. S. (2022). FRAUD RISK JUDGMENT MEASUREMENT SCALE DEVELOPMENT. *Journal of Governance and Regulation*, *11*(1 Special Issue), 303–311. https://doi.org/10.22495/jgrv11i1siart10

Karshiyev, Z. (2025). Adaptive Hybrid Ensemble Framework for Real-Time Anomaly Detection in Large-Scale Data Streams. *Techscience Uz - Topical Issues of Technical Sciences*, *3*(12), 74–93. https://doi.org/10.47390/ts-v3i12y2025n09

Kramer, B. (2015). Trust, but verify: Fraud in small businesses. *Journal of Small Business and Enterprise Development*, *22*(1), 4–20. https://doi.org/10.1108/JSBED-08-2012-0097

Laudon,K C., & Laudon, J. P. (2020). *Managing the Digital Firm. Pearson*.

Ma'muriyah, N., Richard, & Haeruddin, H. (2025). Implementation Mean Imputation and Outlier Detection for Loan Prediction Using the Random Forest Algorithm. *Jitk (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *10*(4), 937–944. https://doi.org/10.33480/jitk.v10i4.6437

Olateju, O. O., Okon, S. U., Igwenagu, U. T. I., Salami, A. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud. *Asian Journal of Research in Computer Science*, *17*(6), 264–292. https://doi.org/10.9734/ajrcos/2024/v17i6472

Peña, I. P. A., & Castro, J. C. O. (2024). Implementation and Evaluation of an Anti-Fraud Prototype Based on Generative Artificial Intelligence for the Ecuadorian Financial Sector. *Revista De Gestão Social E Ambiental*, *18*(9), e08601. https://doi.org/10.24857/rgsa.v18n9-162

Rizani, F., & Respati, N. W. (2018). Factors influencing the presentation of fraudulent financial reporting in Indonesia. *Journal of Advanced Research in Law and Economics*, *9*(1), 254–264. https://doi.org/10.14505//jarle.v9.1(31).31

Rojan, Z. (2024). Financial Fraud Detection Based on Machine and Deep Learning: A Review. *Indonesian Journal of Computer Science*, *13*(3). https://doi.org/10.33022/ijcs.v13i3.4059

Romney, M. B., Steinbart, P. J. (2020). *Accounting Information Systems* (14th ed.). Pearson Prentice Hall.

Saleh, M. M. A., Aladwan, M., Alsinglawi, O., & Saleh, H. M. I. (2021). Predicting fraudulent financial statements using fraud detection models. *Academy of Strategic Management Journal*, *20*(SpecialIssue3), 1–17. https://www.scopus.com/pages/publications/85107744655?origin=resultslist

Singh, S. (2024). Artificial Intelligence and Machine Learning in Financial Services: Risk Management and Fraud Detection. *Jes*, *20*(6s), 1418–1424. https://doi.org/10.52783/jes.2929

Tieu, T. T. H., & Tran, N. H. (2026). Integrating the fraud triangle with machine learning for financial misstatement detection: Evidence from an emerging market. *Cogent Business and Management*, *13*(1). https://doi.org/10.1080/23311975.2026.2614367

Tiwari, S. (2025). Enhancing Financial Crime Detection Through Data Science-Driven Transaction Monitoring: A Comprehensive Framework for Modern Financial Institutions. *International Journal of Computing and Engineering*, *7*(13), 53–63. https://doi.org/10.47941/ijce.3001

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The Role of Big Data in Detecting and Preventing Financial Fraud in Digital Transactions. *World Journal of Advanced Research and Reviews*, *22*(2), 1746–1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

Waldner, F., Hansen, M. C., Potapov, P. V, Löw, F., Newby, T., Ferreira, S., & Defourny, P. (2017). National-scale cropland mapping based on spectral-temporal features and outdated land cover information. *PLoS ONE*, *12*(8). https://doi.org/10.1371/journal.pone.0181911