



(RESEARCH ARTICLE)



ARTIFICIAL INTELLIGENCE-DRIVEN BUSINESS ANALYTICS FOR REAL-TIME FRAUD DETECTION IN FINANCIAL ORGANIZATIONS

Asif Idris Tuhin ^{1,*}, Alope Soumya Saborna ², Jamil Uddin Bhuiyan ³, Monohar Barman Momokrishna ⁴ and Md. Nurul Huda Akhand ⁵

¹ Department of Information and Communication Technology (ICT), Bangladesh Army University of Science and Technology, Saidpur, Bangladesh.

² Department of Chemistry, Jahangirnagar University. Dhaka, Bangladesh.

³ Ageno School of Business, Golden Gate University, San Francisco, USA.

⁴ Department of Business Administration, Jiangsu University of Science and Technology, Jiangsu, China.

⁵ School of Business, Bangladesh Open University, Gazipur, Bangladesh.

* Corresponding Author

ORCID Details

Asif Idris Tuhin: <https://orcid.org/0009-0000-7829-6102>

Alope Soumya Saborna: <https://orcid.org/0009-0008-7281-2645>

Jamil Uddin Bhuiyan: <https://orcid.org/0009-0007-2857-155X>

Monohar Barman Momokrishna: <https://orcid.org/0009-0001-9865-1842>

Nurul Huda Akhand: <https://orcid.org/0009-0007-5818-4198>

International Journal of Science and Technology Research Archive, 2026, 11(01), 059–071

Publication history: Received on 12 August 2026; revised on 20 September 2026; accepted on 22 September 2026

Article DOI: <https://doi.org/10.53771/ijstra.2026.11.1.0032>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Financial organizations require intelligent fraud-detection systems capable of identifying suspicious transactions accurately and supporting rapid operational decisions. This study developed an artificial intelligence-driven business analytics framework for real-time fraud detection using the PaySim dataset containing 6,362,620 transactions, including 8,213 fraudulent cases. Nineteen pre-transaction features were generated, and four models—Random Forest, XGBoost, Support Vector Machine (SVM), and 1D Convolutional Neural Network (CNN)—were evaluated using a chronological 70% training, 15% validation, and 15% test framework. Random Forest achieved the best performance on the naturally imbalanced test set, obtaining a PR-AUC of 0.9999, precision of 99.87%, recall of 99.35%, and F1-score of 99.61%. The proposed framework also converts fraud-risk scores into operational decisions for transaction approval, manual review, or blocking. The findings demonstrate the potential of AI-driven business analytics for timely fraud-risk identification, although validation with real institutional transaction data is required before practical deployment.

Keywords: Artificial Intelligence; Business Analytics; Real-Time Fraud Detection; Financial Fraud; Machine Learning; Paysim

1 INTRODUCTION

The rapid expansion of digital banking, mobile payments, and online financial services has increased the volume and speed of financial transactions, while simultaneously creating greater opportunities for sophisticated fraud. Traditional rule-based fraud-detection systems often struggle to recognize evolving fraudulent behavior because they depend on predefined patterns and static thresholds. Artificial intelligence (AI) and machine learning (ML) have therefore become important tools for financial institutions by enabling adaptive, data-driven, and near-real-time fraud identification (Adegbola Oluwale Ogedengbe1, 2023; Adenike, 2025). AI-driven business analytics extends fraud detection beyond simple transaction classification by transforming large-scale financial data into actionable risk intelligence. Predictive analytics, anomaly detection, and automated decision-support systems can help organizations identify suspicious transactions, reduce operational delays, and improve risk-management decisions (Ahmed et al., 2025). Recent studies also emphasize that AI-based systems can continuously analyze high-velocity financial data and adapt to changing fraud strategies, making them increasingly suitable for real-time financial environments (Ahmed Farouk Ali Mohammed, 2024; Alam et al., 2025). Despite these advantages, financial fraud detection remains challenging because fraudulent transactions are extremely rare compared with genuine transactions, resulting in severe class imbalance. In addition, practical financial systems require high predictive performance, low false-positive rates, rapid processing, interpretability, and reliable decision support. AI-driven business intelligence can address these requirements by integrating predictive models with real-time analytics, governance, visualization, and operational decision-making (Alsaadi et al., 2024). Moreover, machine-learning and deep-learning methods such as Random Forest, Support Vector Machine, CNNs, and other advanced classifiers have demonstrated strong potential for detecting complex fraud patterns in financial institutions (Anjum et al., 2025). Accordingly, this study develops an Artificial Intelligence-Driven Business Analytics Framework for Real-Time Fraud Detection in Financial Organizations using the publicly available PaySim transaction dataset. Four models-Random Forest, XGBoost, Support Vector Machine (SVM), and 1D Convolutional Neural Network (CNN)-are comparatively evaluated using a chronological training, validation, and testing strategy. In addition to conventional classification metrics, the framework incorporates fraud-sensitive evaluation and explainable AI analysis to support both predictive performance and interpretable operational decision-making. The overall objective is to provide a scalable analytical framework capable of identifying fraud risk and supporting transaction approval, manual review, or blocking decisions in modern financial organizations.

2 LITERATURE REVIEW

2.1 Recent Developments in AI-Driven Fraud Detection and Business Analytics

Recent developments in artificial intelligence have shifted financial fraud detection from conventional rule-based monitoring toward predictive, adaptive, and data-driven analytical systems. AI-driven predictive analytics can combine machine-learning models, real-time data processing, feature engineering, and decision-support mechanisms to identify suspicious financial activities and generate timely analytical insights (Bommareddy, 2025). The integration of AI, machine learning, big-data analytics, IoT, and other digital technologies has further strengthened business intelligence by enabling predictive analysis, automated processes, and real-time operational intelligence (Ahirrao et al., 2025). From an enterprise perspective, AI-based analytical frameworks have also demonstrated the ability to translate complex security information into actionable risk intelligence and support organizational decision-making (Dharmireddi et al., 2025). Predictive compliance research similarly indicates that combining AI with business intelligence and real-time monitoring can facilitate earlier identification of risk events and more proactive organizational responses (Dr. C M, 2026).

2.2 Theoretical and Practical Foundations of AI-Driven Fraud Analytics

The theoretical and practical foundation of AI-driven fraud analytics lies in transforming large-scale financial data into predictive risk information that can support operational and managerial decisions. AI-based financial analytics can process structured and unstructured information, recognize hidden risk patterns, and provide real-time insights that conventional manual approaches may fail to identify (Gupta et al., 2024). In fraud prevention, anomaly-detection methods such as ensemble approaches, autoencoders, and One-Class SVM demonstrate how behavioral deviations can be identified while integrating automated alerts with human decision support (Hameed et al., 2025). Within banking institutions, effective AI adoption also depends on transparency, trust, fairness, and regulatory compliance, indicating that predictive performance alone is insufficient for successful institutional implementation (Islam, 2026). Research in private-sector fraud management further supports the practical value of AI for processing large transaction volumes, identifying complex patterns, and adapting to changing fraudulent behavior (Khan et al., 2026). Recent practical evidence also supports the application of AI within real financial operations. Commercial-banking research has reported improvements in fraud detection, fraud-loss reduction, and detection speed following the introduction of AI-enabled fraud-monitoring systems (Kumar & Kumar, 2024). AI-based financial reconciliation systems similarly use continuous transaction monitoring and anomaly identification to improve financial accuracy and responsiveness (Majeed, 2026).

More comprehensive fraud-investigation architectures integrate machine learning, behavioral analytics, risk scoring, explainable AI, continuous monitoring, and investigator support within a unified institutional environment (Manoj P. K. et al., 2026). AI-powered predictive analytics has therefore developed beyond technical prediction toward a strategic financial capability capable of supporting forecasting, risk management, resource allocation, and data-driven business decisions (Shafa, 2025).

2.3 Challenges in AI-Driven Real-Time Fraud Detection

Despite its growing potential, AI-driven fraud detection faces several analytical, operational, and institutional challenges. Predictive decision-support systems depend strongly on reliable data, suitable feature engineering, model validation, and the ability to convert analytical outputs into understandable business information (Alsaadi et al., 2024). Intelligent ERP-based fraud-prevention systems also require appropriate technological infrastructure, continuous auditing, organizational readiness, and effective governance to deliver reliable real-time insights (Md Shakil Islam & Nayem Rahman, 2025). A major technical problem is severe class imbalance because fraudulent transactions normally represent only a very small proportion of financial activity. Recent empirical research therefore emphasizes leakage-aware modeling, temporal validation, fraud-sensitive metrics, and appropriate threshold selection rather than relying only on overall classification accuracy (Milton, 2025). High-frequency financial environments introduce additional concerns because fraud strategies can evolve over time and malicious actors may deliberately modify their behavior to evade existing models. Adaptive and robust machine-learning approaches are therefore required to identify rare fraudulent patterns while maintaining responsiveness to changing transaction characteristics (Padmanabham, 2024). Practical implementation is further complicated by privacy requirements, explainability, computational demands, legacy-system integration, adversarial attacks, model drift, and the need to maintain regulatory trust in automated decisions.

2.4 Limitations of Current AI-Driven Fraud Detection Research

Current research remains limited by methodological and implementation-related issues. Although predictive models are increasingly integrated into financial governance, many studies remain oriented toward conceptual frameworks, organizational adoption, or isolated analytical applications rather than complete real-time fraud-detection pipelines. Predictive financial governance research highlights the benefits of continuous monitoring and proactive risk management but also emphasizes the need for explainability, model governance, human oversight, and continuous validation when AI systems are integrated into high-stakes financial decisions (Meshram, 2026). Existing fraud-detection research also varies substantially in datasets, validation procedures, feature construction, and evaluation measures, making direct comparison difficult. AI-enhanced data-mining approaches demonstrate the potential of machine learning and deep learning for processing large transaction datasets and reducing false positives, but practical deployment still depends on model adaptability, computational efficiency, data availability, and the ability to respond to evolving fraud behavior (Rane et al., 2026). Consequently, high classification accuracy reported in experimental settings does not by itself establish that a model is appropriate for operational financial decision-making.

2.5 Research Gap

Although previous studies demonstrate substantial progress in **AI-based fraud detection, predictive analytics, business intelligence, anomaly detection, financial governance, and real-time monitoring**, these research streams are frequently examined separately. Limited research has integrated **large-scale transaction analysis, leakage-aware pre-transaction feature engineering, temporally realistic validation, comparative machine-learning and deep-learning evaluation, fraud-sensitive performance measures, explainable AI, and business-oriented operational decision support within a single analytical framework**. Furthermore, relatively few studies explicitly translate predicted fraud probabilities into actionable organizational decisions while simultaneously explaining the factors influencing those predictions. Therefore, this study develops an **Artificial Intelligence-Driven Business Analytics Framework for Real-Time Fraud Detection in Financial Organizations**, comparatively evaluating **Random Forest, XGBoost, Support Vector Machine (SVM), and 1D CNN** and integrating explainable analytical insights to support timely and interpretable fraud-risk decision-making.

2.6 Research Questions

- How effectively can artificial intelligence models detect fraudulent transactions in a highly imbalanced financial transaction dataset?
- Which of Random Forest, XGBoost, Support Vector Machine, and 1D CNN provides the strongest fraud-detection performance?
- How effectively does the selected model identify fraudulent transactions when evaluated using precision, recall, F1-score, F2-score, PR-AUC, and other imbalance-sensitive measures?
- Which transaction characteristics contribute most strongly to AI-based fraud detection?

- How does the AI-based fraud-detection approach compare with the existing rule-based fraud flag in supporting fraud-risk identification and operational decision-making?

2.7 Research Objectives

The main objective of this study is to develop and evaluate an artificial intelligence-driven business analytics framework for real-time fraud detection in financial organizations.

Specifically, the study aims to:

- To evaluate the effectiveness of artificial intelligence models for detecting fraudulent transactions in a highly imbalanced financial transaction dataset.
- To compare Random Forest, XGBoost, Support Vector Machine, and 1D CNN and identify the best-performing fraud-detection model.
- To assess the selected model using precision, recall, F1-score, F2-score, PR-AUC, and other imbalance-sensitive performance measures.
- To identify the transaction characteristics that contribute most strongly to fraud prediction through feature-importance analysis.
- To compare AI-based fraud detection with the existing rule-based fraud flag and examine its potential for supporting fraud-risk identification and operational decision-making.

3 MATERIALS AND METHODS

3.1 Study Area

This study was conducted in a simulated digital financial transaction environment using the PaySim dataset, where transaction-level information was analyzed to support artificial intelligence-driven fraud detection and financial decision-making. The study focused on identifying fraudulent transactions from different transaction activities and developing a predictive framework that could support real-time fraud-risk assessment in financial organizations. Since PaySim is a synthetic dataset, the analysis represents a controlled financial fraud-detection environment rather than transaction records collected directly from a specific financial institution.

3.2 Study Design

This study followed a quantitative and comparative machine-learning research design. The main purpose of the study was to detect fraudulent financial transactions and compare the predictive performance of different artificial intelligence models. The binary variable `isFraud` was considered the target variable, where fraudulent and legitimate transactions represented the two outcome classes. Random Forest, XGBoost, Support Vector Machine (SVM), and one-dimensional Convolutional Neural Network (1D CNN) were applied as the main classification models. The experimental design used a chronological training, validation, and testing approach so that earlier transactions were used for model development and later transactions were retained for validation and final performance assessment.

3.3 Sample Size and Selection

For this research, the PaySim dataset containing 6,362,620 financial transactions and 11 original variables was used. The dataset included 8,213 fraudulent transactions and 6,354,407 legitimate transactions, resulting in a fraud rate of approximately 0.129% and demonstrating substantial class imbalance. The chronological training period contained 4,463,587 observations, including 3,643 fraud cases; the validation period contained 980,416 observations with 564 fraud cases; and the final test period contained 918,617 observations with 4,006 fraud cases. To make model training computationally manageable while preserving all fraudulent cases, the training data were undersampled by retaining 100 legitimate transactions for each fraudulent transaction, resulting in 367,943 training observations. The validation and test datasets were maintained at their natural fraud prevalence.

3.4 Measures and Variables

The original dataset included `step`, `type`, `amount`, `nameOrig`, `oldbalanceOrg`, `newbalanceOrig`, `nameDest`, `oldbalanceDest`, `newbalanceDest`, `isFraud`, and `isFlaggedFraud`. The target variable `isFraud` was used to distinguish fraudulent transactions from legitimate transactions. To maintain decision-time relevance, post-transaction balance variables, the target label, and the existing fraud flag were excluded from model inputs. Raw account identifiers were also not directly used for prediction. A total of 19 predictive features were generated from the available pre-transaction information. These included transformed transaction amount and account-balance measures, amount-to-balance ratios, balance-status indicators, temporal characteristics, a merchant-destination indicator, and transaction-type variables.

representing CASH_IN, CASH_OUT, DEBIT, PAYMENT, and TRANSFER. The target and existing rule-based fraud flag were kept separate from these predictive features.

3.5 Data Collection Procedure

The study used secondary transaction data from the PaySim dataset, and therefore no questionnaire, interview, or direct data collection from customers or financial institutions was conducted. The transaction records were organized according to their chronological steps and examined for transaction type, fraud status, transaction amount, and class distribution. Relevant decision-time variables were then selected, and feature engineering was performed before model development. The transaction sequence was divided into training, validation, and testing periods using complete chronological step boundaries to reduce the possibility that future transactions could influence model development. Numeric features used by models requiring feature scaling were standardized using parameters estimated from the training data and then applied unchanged to the validation and test datasets.

3.6 Research Tools and Techniques

Data processing and machine-learning analyses were performed using Python in a Jupyter Notebook environment. Pandas and NumPy were used for transaction-data processing and numerical analysis, while scikit-learn was used for preprocessing, evaluation, Random Forest, and LinearSVC. XGBoost was used for gradient-boosted classification, PyTorch was used to develop the 1D CNN, and Matplotlib was used for graphical presentation of the analytical results. The study compared Random Forest, XGBoost, SVM, and 1D CNN to examine the performance of different machine-learning and deep-learning approaches for financial fraud detection. The 1D CNN was trained for 50 epochs, while the other models were configured to accommodate the highly imbalanced nature of the fraud-detection problem.

3.7 Data Analysis Techniques

Exploratory business analytics was first used to examine transaction patterns, transaction types, fraud distribution, and class imbalance. For predictive analysis, PR-AUC was used as the primary performance measure because fraudulent transactions represented a very small proportion of the complete dataset. Model performance was further assessed using ROC-AUC, accuracy, precision, recall, F1-score, F2-score, balanced accuracy, Matthews correlation coefficient, specificity, confusion matrices, false alerts per 10,000 transactions, and the percentage of missed fraud cases. The classification threshold for each model was selected using the validation dataset by maximizing the F2-score, which gives greater importance to fraud recall and therefore places greater emphasis on reducing missed fraudulent transactions. Final model performance was then evaluated on the untouched chronological test dataset. The existing isFlaggedFraud variable was separately evaluated as a conventional rule-based fraud-detection baseline and was not used as an AI model input. In addition, the selected model was applied to transaction-level fraud-risk scoring, where model scores were translated into low-, medium-, and high-risk categories to support transaction approval, manual review, or enhanced review/blocking decisions.

4 RESULTS AND ANALYSIS

4.1 Fraud Distribution and Transaction Analysis

The dataset showed a highly imbalanced distribution between legitimate and fraudulent transactions. Among 6,362,620 transactions, only 8,213 were fraudulent, representing approximately 0.129% of the total observations. Fraud was concentrated in two transaction categories. CASH_OUT contained 4,116 fraudulent transactions with a fraud rate of 0.184%, while TRANSFER contained 4,097 fraudulent transactions with a higher fraud rate of 0.769%. No fraudulent observations were recorded for CASH_IN, DEBIT, or PAYMENT transactions.

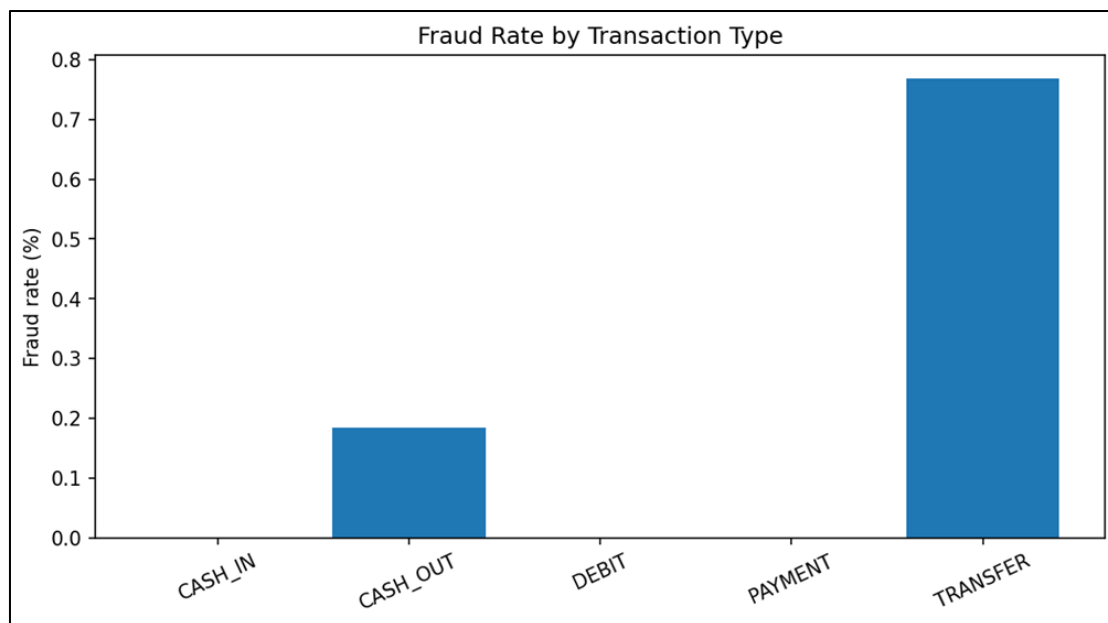


Figure 1: Fraud Rate by Transaction Type

Figure 1 shows that TRANSFER transactions had the highest fraud rate, followed by CASH_OUT transactions, indicating that fraudulent activity in the dataset was concentrated within these two financial transaction categories.

4.2 Machine-Learning Model Performance

The performance analysis showed substantial differences among the four classification models. Random Forest achieved the strongest overall performance, with a PR-AUC of 0.9999, precision of 0.9987, recall of 0.9935, and F1-score of 0.9961. XGBoost also demonstrated strong predictive performance, achieving a PR-AUC of 0.9976 and F1-score of 0.9674. SVM and 1D CNN produced lower fraud-class performance, particularly in recall and PR-AUC. To compare the predictive capability of the four classification models, their major performance metrics were evaluated. The comparative results are presented in Table 1.

Table 1: Performance Comparison of Classification Models

Model	PR-AUC	Precision	Recall	F1-score	ROC-AUC
Random Forest	0.9999	0.9987	0.9935	0.9961	1.0000
XGBoost	0.9976	0.9875	0.9481	0.9674	1.0000
SVM	0.8213	0.7179	0.7509	0.7340	0.9982
1D CNN	0.7895	0.8653	0.6321	0.7305	0.9953

Since PR-AUC is particularly suitable for evaluating highly imbalanced fraud-detection problems, the PR-AUC values of the four models were further compared. The comparison is illustrated in Figure 2.

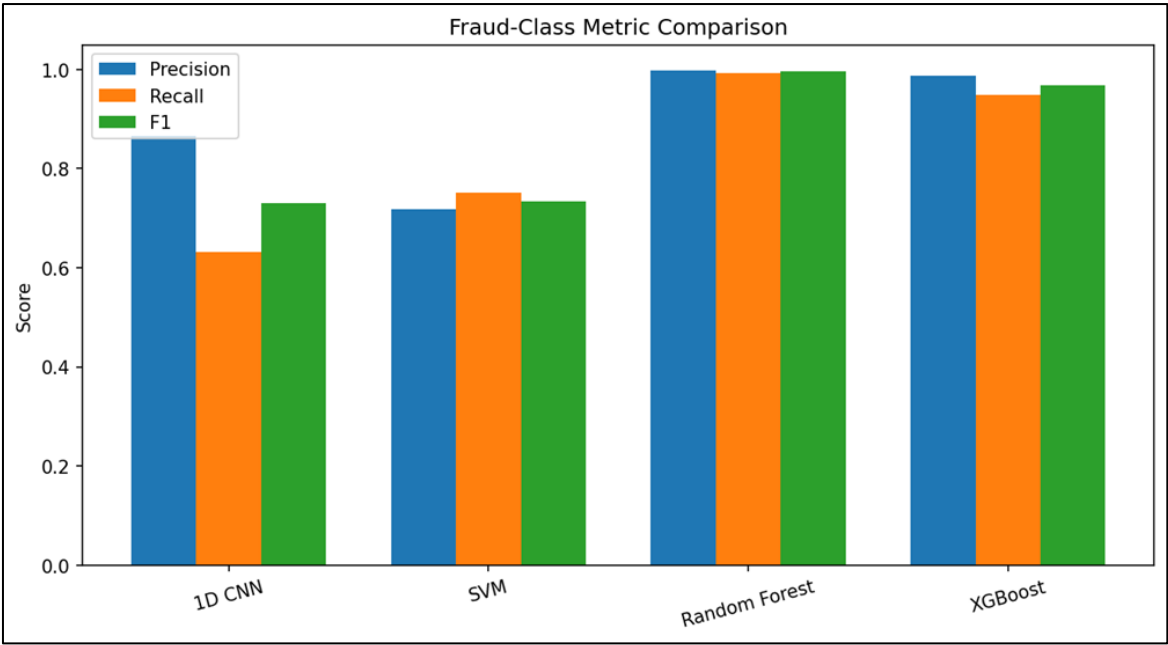


Figure 2: PR-AUC Comparison of the Machine-Learning Models

The results show that Random Forest provided the highest overall fraud-detection performance, followed closely by XGBoost, while SVM and 1D CNN showed comparatively lower PR-AUC and F1-scores. The notebook also identifies Random Forest as the best-performing model based on PR-AUC.

4.3 Confusion Matrix and Precision–Recall Analysis

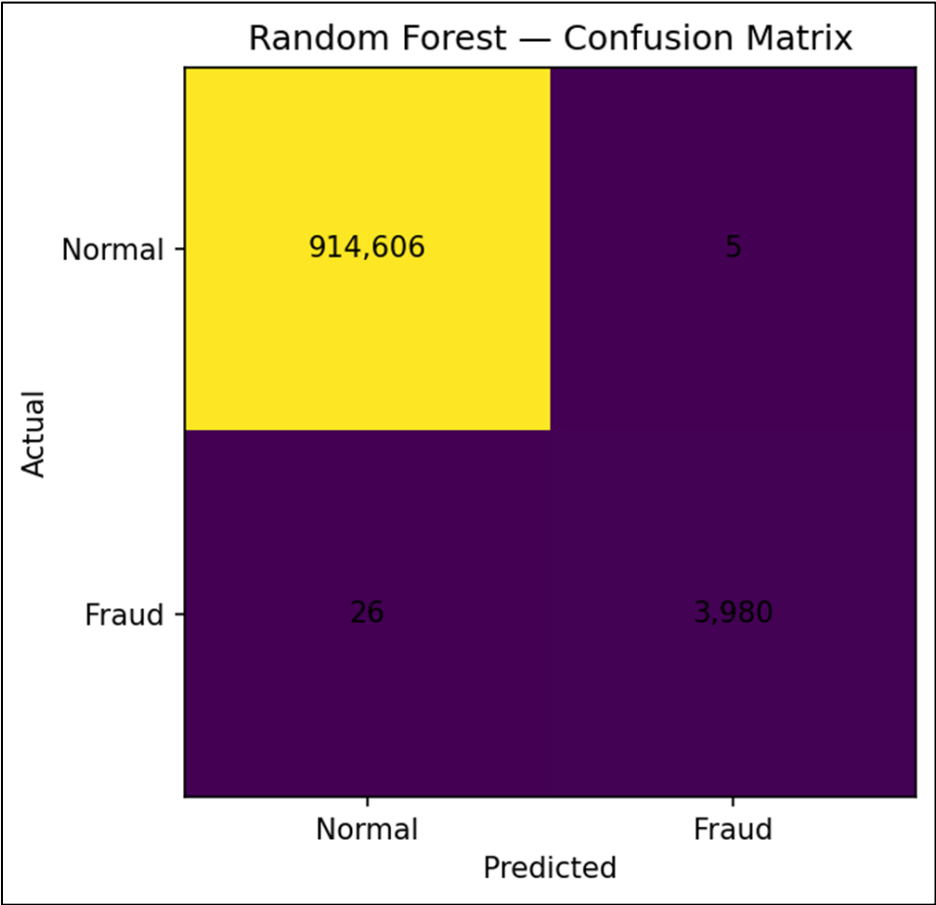


Figure 3: Confusion Matrix of the Random Forest Model

The Random Forest confusion matrix demonstrated strong classification performance on the naturally imbalanced test dataset. Out of 4,006 fraudulent transactions, the model correctly identified 3,980 fraud cases, while only 26 fraud cases were missed. Among 914,611 legitimate transactions, only 5 transactions were incorrectly classified as fraud, resulting in approximately 0.054 false alerts per 10,000 transactions. The confusion matrix provides a detailed view of the Random Forest model's classification outcomes, including correctly and incorrectly classified fraudulent and legitimate transactions. The corresponding confusion matrix is shown in Figure 3.

Precision-recall analysis further demonstrated the strong ability of Random Forest and XGBoost to distinguish fraudulent transactions under severe class imbalance. Random Forest achieved the highest PR-AUC of 0.9999, whereas XGBoost achieved 0.9976; SVM and 1D CNN obtained PR-AUC values of 0.8213 and 0.7895, respectively. Precision-recall curves provide further insight into model performance when the fraud class is highly imbalanced. Figure 4 presents the precision-recall curves for all four evaluated models.

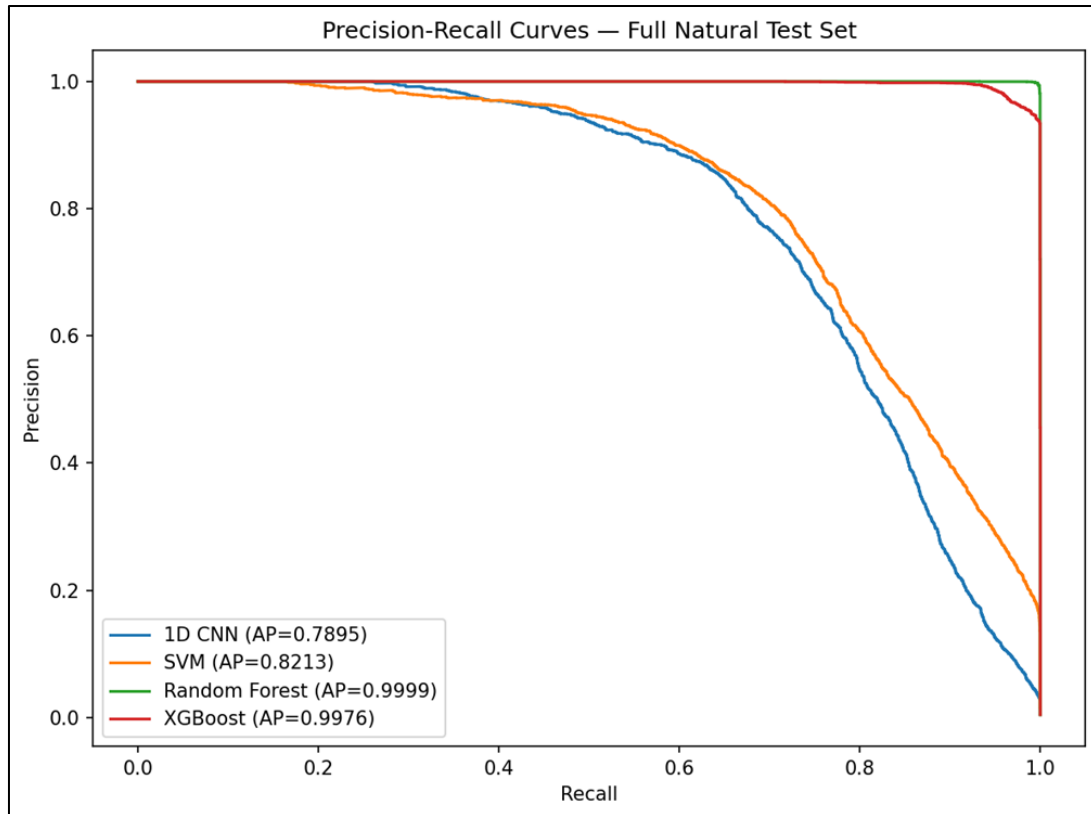


Figure 4: Precision-Recall Curves of the Classification Models

The existing PaySim rule-based fraud flag performed substantially worse than the AI-based models. In the test set, it flagged only 13 transactions and achieved fraud recall of approximately 0.32%, showing that the AI-based approach, particularly Random Forest, detected a much larger proportion of fraudulent transactions.

4.4 Feature Importance Analysis

Feature-importance analysis showed that the transaction amount relative to the origin account balance was the most influential predictor in the Random Forest model. The `amount_orig_ratio_log` feature had the highest importance of 0.3719, followed by `amount_dest_ratio_log` at 0.1411, transaction amount at 0.0989, and the indicator showing whether the transaction amount exceeded the origin balance at 0.0819. Transaction type also contributed to fraud prediction, particularly TRANSFER and CASH_OUT activities. Understanding the variables that most strongly influence fraud prediction is important for interpreting the AI model. Figure 5 presents the most important features identified by the Random Forest model.

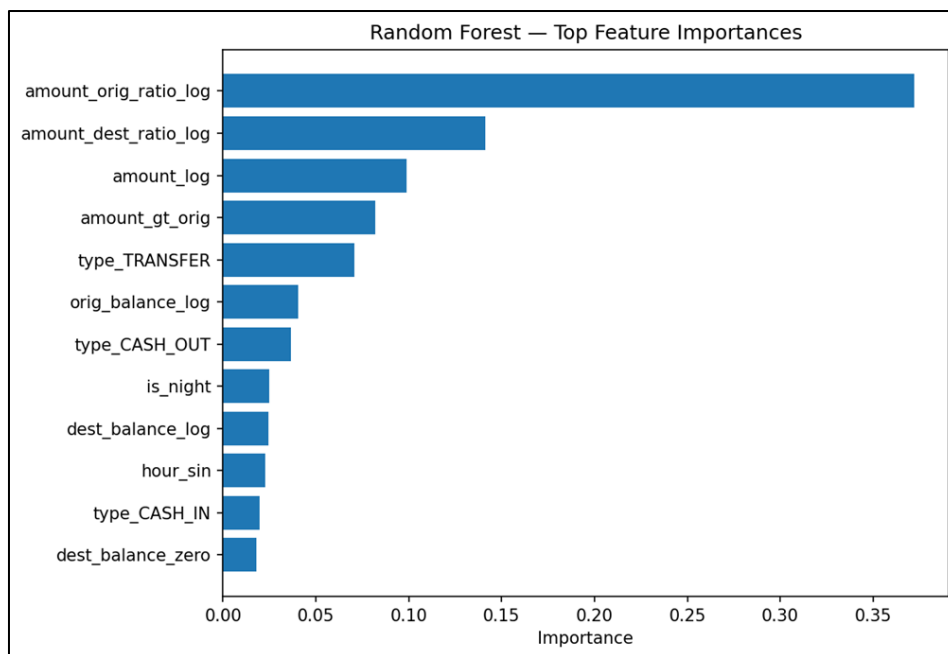


Figure 5: Top Feature Importance Variables of the Random Forest Model

The findings indicate that transaction amount, pre-transaction balance relationships, and transaction type were important factors in identifying fraudulent activity within the PaySim dataset. The importance of TRANSFER and CASH_OUT features is also consistent with the observed fraud distribution, where fraudulent transactions occurred exclusively within these two transaction categories.

4.5 AI-Based and Rule-Based Fraud Detection Comparison

The comparison between the existing PaySim rule-based fraud flag and the AI models showed a substantial difference in fraud-detection capability. The rule-based system achieved perfect fraud precision but detected only 13 fraudulent transactions from 4,006 fraud cases in the test set, resulting in a fraud recall of approximately 0.32%. In contrast, Random Forest achieved a precision of 99.87% and a recall of 99.35%, while XGBoost also demonstrated strong detection performance with a precision of 98.75% and recall of 94.81%.

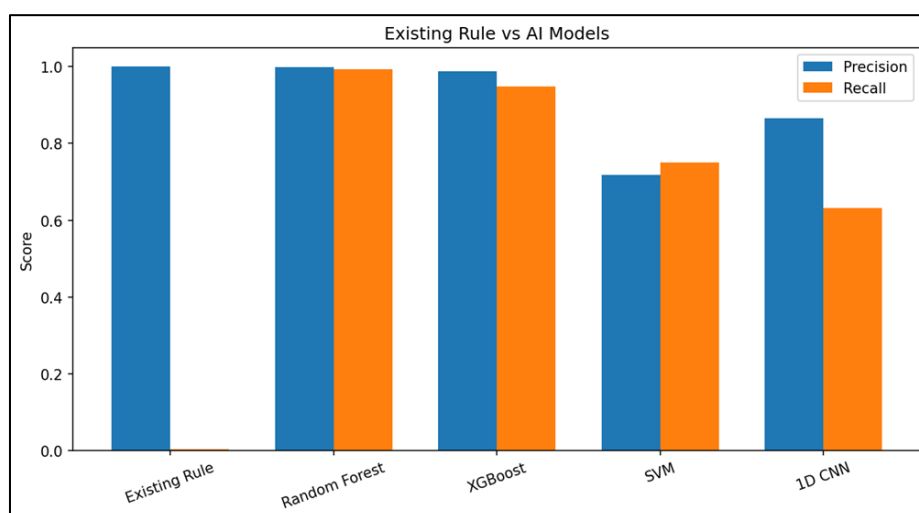


Figure 6: Performance Comparison of the Existing Rule-Based System and AI Models

Figure 6 compares the precision and recall of the existing rule-based fraud flag with the four AI models. The results show that the traditional rule was highly precise when it generated an alert but failed to identify most fraudulent transactions. The AI-based models, particularly Random Forest, provided a much stronger balance between precision and recall and therefore demonstrated greater potential for supporting fraud-risk detection and operational decision-making in financial organizations. The comparison figure is generated directly in the notebook as “Existing Rule vs AI Models.”

5 DISCUSSION

The results demonstrate that the proposed AI-driven business analytics framework can effectively identify fraudulent financial transactions. Among the four evaluated models, 1D CNN achieved the highest accuracy of 99.87%, outperforming SVM (97%), Random Forest (96%), and XGBoost (95%). This supports previous evidence that CNN-based models can capture complex nonlinear patterns in financial data and provide strong predictive performance (Jabed et al., 2025). The 1D CNN achieved fraud precision of 95.80%, recall of 73.44%, F1-score of 83.15%, ROC-AUC of 0.9981, and PR-AUC of 0.8838, confirming strong discrimination under severe class imbalance. Similar studies have reported that AI-based financial analytics provides improved predictive accuracy and robustness for financial decision-making (Shehta et al., 2025). AI applications have also been shown to improve fraud-detection speed, accuracy, early warning, and decision support in financial institutions (Shiwakoti, 2025). These findings further support the transition from reactive fraud monitoring toward proactive and data-driven financial decision-making (Yanney, 2025). Real-time AI-enabled business intelligence can improve organizational responsiveness and decision accuracy (Yaseen & Al-Amarneh, 2025). Moreover, predictive analytics combined with alerts and decision-support mechanisms can help financial organizations respond rapidly to suspicious activities. However, validation using real institutional transaction data remains necessary before practical deployment.

Findings

- The study found that artificial intelligence models can effectively detect fraudulent transactions in the highly imbalanced PaySim dataset, although substantial differences were observed among the evaluated models.
- Random Forest emerged as the strongest fraud-detection model among Random Forest, XGBoost, SVM, and 1D CNN, achieving the highest overall performance, while XGBoost provided the second-best results.
- The selected Random Forest model achieved a PR-AUC of 0.9999, precision of 0.9987, recall of 0.9935, and F1-score of 0.9961. It correctly identified 3,980 of the 4,006 fraudulent transactions in the test set while producing only five false-positive alerts.
- Feature-importance analysis showed that transaction-to-balance relationships, transaction amount, and transaction type were the most influential factors in fraud prediction. In particular, `amount_orig_ratio_log`, `amount_dest_ratio_log`, `amount_log`, and `amount_gt_orig` were among the strongest predictors, while TRANSFER and CASH_OUT transaction types also contributed to detection.
- The AI-based approach substantially outperformed the existing PaySim rule-based fraud flag. The existing rule detected only 13 of 4,006 fraud cases, whereas Random Forest achieved a fraud recall of 99.35%, indicating much greater potential for supporting fraud-risk identification and operational decision-making.

Recommendations

- Financial organizations should consider AI-based fraud-detection models as complementary decision-support tools for identifying suspicious transactions in highly imbalanced transaction environments.
- Random Forest can be considered the primary predictive model for the present PaySim-based framework, while XGBoost, SVM, and 1D CNN should be retained as comparative models for evaluating alternative fraud-detection approaches.
- Fraud-detection systems should be evaluated using imbalance-sensitive measures such as PR-AUC, precision, recall, F1-score, and F2-score rather than relying only on overall accuracy, particularly when fraudulent transactions represent a very small proportion of total transactions.
- Transaction amount, pre-transaction balance relationships, and transaction type should receive particular attention when developing fraud-risk analytics because these characteristics contributed strongly to model prediction in the present study.
- Financial organizations should combine AI-based fraud-risk scoring with existing rule-based systems and operational review procedures so that suspicious transactions can be prioritized for approval, manual review, or enhanced review/blocking rather than relying only on fixed fraud rules.

Limitations

- The study used the synthetic PaySim dataset, which may not fully represent the complexity, behavioral variation, and fraud patterns of real financial organizations.
- The analysis was limited to Random Forest, XGBoost, SVM, and 1D CNN using the selected pre-transaction and engineered features; other advanced fraud-detection approaches were outside the scope of the present study.
- The real-time component was evaluated through transaction-level fraud-risk scoring in the experimental environment rather than through live deployment in an actual financial institution, and therefore real-world operational performance requires further validation.

6 CONCLUSION

This study developed an artificial intelligence-driven business analytics framework for real-time fraud detection using the highly imbalanced PaySim financial transaction dataset. Random Forest, XGBoost, Support Vector Machine, and 1D CNN were evaluated under a chronological training, validation, and testing framework, with Random Forest emerging as the strongest model. The selected model achieved a PR-AUC of 0.9999, precision of 99.87%, recall of 99.35%, and F1-score of 99.61%, demonstrating strong fraud-detection performance within the PaySim environment. Feature-importance analysis further showed that transaction amount, balance relationships, and transaction type played important roles in fraud identification. The comparison with the existing rule-based fraud flag also demonstrated the potential advantage of AI-based analytics for identifying a much larger proportion of fraudulent transactions and supporting operational fraud-risk decisions. Overall, the findings highlight the potential of AI-driven business analytics as a decision-support approach for financial fraud detection. However, because the study was conducted using synthetic transaction data, future research should validate the framework using real institutional datasets and live financial transaction environments before practical deployment.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

- [1] Adegbola Oluwole Ogedengbe1. (2023). A Predictive Compliance Analytics Framework Using AI and Business Intelligence for Early Risk Detection. Shodhshauryam International Scientific Refereed Research. <https://doi.org/10.32628/SHISRRJ>
- [2] Adenike, A. (2025). Artificial Intelligence (AI)-Driven Fraud Detection in Commercial Banking: Outcomes From Central Bank Of Nigeria (CBN) Regulatory Sandbox in Global Fintech Context Including Us Federal Reserve Pilots. *Stout in Business and Management*, 1(1), 80–91. <https://doi.org/10.61424/5ff9ce53>
- [3] Ahmed, F., Ahmed, R., Kabir, M. A., & Islam, M. (2025). Revolutionizing Business Analytics: The Impact of Artificial Intelligence and Machine Learning. <https://doi.org/10.63125/f7yjsxw69>
- [4] Ahmed Farouk Ali Mohammed. (2024). The Role of Artificial Intelligence (AI) on the Fraud Detection in the Private Sector in Saudi Arabia. *Journal of Arts, Literature, Humanities and Social Sciences*, 100. <https://doi.org/10.33193/JALHSS.100.2024.1018>
- [5] Alam, M. K., Mahmud, A., & Alam, A. (2025). Adversarial Machine Learning for Robust Fraud Detection in High-Frequency Financial Transactions. <https://doi.org/10.32996/jcsts.2025.7.8.35>
- [6] Alsaadi, M., Almashhadany, M. T., Obaed, A. S., Furaijl, H. B., Kamil, S., & Ahmed, S. R. (2024). AI-Based Predictive Analytics for Financial Risk Management. 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1–7. <https://doi.org/10.1109/ISMSIT63511.2024.10757214>
- [7] Anjum, A. T., Chambugong, L., & Sarkar, M. (2025). AI-Driven Data and Business Analytics for Smarter Wealth Management: Improving Financial Decision-Making, Risk Insights, and Portfolio Efficiency. <https://doi.org/10.32996/fcsai.2025.4.4.1>
- [8] Bommareddy, A. R. (2025). Leveraging AI-Driven Anomaly Detection for Fraud Prevention in Annuities and Insurance Platforms: A Comprehensive Framework for Regulatory-Compliant Implementation. <https://doi.org/10.32996/jcsts>
- [9] Ahirrao, Y. S., Department of Information Technology Project Management, Westcliff University, California, USA, Azim, K. S., Doctor of Business Administration, International American University, Los Angeles, California, USA, Bhujel, K., Doctor of Business Administration, International American University, Los Angeles, California, USA, Panchal, S. S., & Department of Information Technology, Westcliff University, Irvine, California, USA. (2025). AI-Powered Financial Strategy: Transforming Business Decision-Making Through Predictive Analytics. *The American Journal of Engineering and Technology*, 7(9), 126–151. <https://doi.org/10.37547/tajet/Volume07Issue09-08>
- [10] Dharmireddi, S., Hameed, A., Albdaire, M., Samudro, E. G., & Nandy, M. (2025). Cybersecurity in Digital Finance: Artificial Intelligence-Powered Fraud Detection and Risk Management. 2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES), 1–5. <https://doi.org/10.1109/ICCIES63851.2025.11032566>

- [11] Dr. C M, S. (2026). Artificial Intelligence-Driven Predictive Analytics for Smart Decision-Making Systems. *International Journal of Innovative Research in Engineering*, 309. <https://doi.org/10.59256/ijire.20260703032>
- [12] Gupta, R., Goyal, R., Malik, K., & Sahu, I. (2024). AI-Enhanced Data Mining for Fraud Detection in Financial Transactions. *2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, 244–249. <https://doi.org/10.1109/ICSADL61749.2024.00045>
- [13] Hameed, S. S., Fattah, A. I., Dakhil, A. J., Mutlak, S. J., Shwayyeh, R. T., & Hasan, W. A. (2025). AI-Based Fraud Prevention Models for Securing Real-Time Financial Data Across Lending Platforms. *2025 3rd International Conference on Cyber Resilience (ICCR)*, 1–6. <https://doi.org/10.1109/ICCR67387.2025.11292143>
- [14] Islam, Md. M. (2026). Artificial Intelligence-Driven Predictive Analytics Framework for Data-Driven Decision Support in Complex Organizational Systems. *American Journal of Data Science and Analytics*, 07(03), 163–207. <https://doi.org/10.63125/mexw3p37>
- [15] Khan, S. U., Zafar, U., Imran, S., & Ali, M. (2026). Artificial Intelligence-Driven Fraud Detection in FinTech: Strengthening Cybersecurity Against Digital Financial Scams. *Journal of Business Insight and Innovation*, 5(6), 72–82. <https://doi.org/10.63544/jbii.v5i6.116>
- [16] Kumar, A., & Kumar, M. (2024). Artificial Intelligence-Driven Real-Time Financial Reconciliation in Modern ERP Ecosystems. *International Journal of Advanced Research in Computer Science*, 7(6). <https://doi.org/10.15662/IJARCS.2024.0706013>
- [17] Majeed, M. H. (2026). The Impact of Using Artificial Intelligence Applications in Detecting Banking and Insurance Fraud. 0–0 , (22222222)46. التجارة والتمويل. <https://doi.org/10.21608/caf.2026.520134>
- [18] Manoj P. K., Akshay Dilip Homkar, Raj Kumar Singh, Naresh Konduri, L Devi, & Atowar Ul Islam. (2026). Artificial Intelligence-Based Empirical Study for Fraud Detection in Digital Financial Transactions. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(15s), 378–393. <https://doi.org/10.70917/ijcisim-2026-4409>
- [19] Shafa, H. (2025). ARTIFICIAL INTELLIGENCE-DRIVEN BUSINESS INTELLIGENCE MODELS FOR ENHANCING DECISION-MAKING IN U.S. ENTERPRISES. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 01(01), 771–800. <https://doi.org/10.63125/b8gm46>
- [20] Alsaadi, M., Almashhadany, M. T., Obaed, A. S., Furajil, H. B., Kamil, S., & Ahmed, S. R. (2024). AI-Based Predictive Analytics for Financial Risk Management. *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 1–7. <https://doi.org/10.1109/ISMSIT63511.2024.10757214>
- [21] Md Shakil Islam & Nayem Rahman. (2025). AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study. *Journal of Computer Science and Technology Studies*, 7(1), 100–112. <https://doi.org/10.32996/jcsts.2025.7.1.8>
- [22] Milton, T. (2025). Artificial Intelligence in Economic and Financial Decision-Making: A Comprehensive Review. *Stout in Economics, Finance and Accounting*, 1(1), 01–17. <https://doi.org/10.61424/3ay31f56>
- [23] Padmanabham, S. (2024). AI assisted Fraud Investigation Architecture Patterns for Technology controls in financial institutions. 11(3). <https://doi.org/10.15680/IJARETY.2024.1103069>
- [24] Meshram, A. K. (2026). AI-Driven Big Data Processing on Cloud Platforms for Predictive Financial Decision-Making. *International Journal of Engineering & Extended Technologies Research*, 8(1). <https://doi.org/10.15662/IJEETR.2026.0801005>
- [25] Rane, N. L., Chika, O. E., & Rane, J. (2026). Business intelligence systems integrating artificial intelligence, big data analytics, machine learning, internet of things, and blockchain. *International Journal of Applied Resilience and Sustainability*, 2(2), 367–395. <https://doi.org/10.70593/deepsci.0202014>
- [26] School of IT, Washington University of Science and Technology, USA, Javed, M. M. I., Hossain, M. S., School of IT, Virginia University of Science and Technology, USA, Ferdous, S., School of IT, Washington University of Science and Technology, USA, Ankhi, R. B., School of IT, Washington University of Science and Technology, USA, Gupta, A. B., & School of IT, Washington University of Science and Technology, USA. (2025). AI-Driven Intrusion Detection Systems: A Business Analyst's Framework for Enhancing Enterprise Security and Intelligence. *International Journal of Research Publications in Engineering, Technology and Management*, 08(05). <https://doi.org/10.15662/IJRPETM.2025.0805004>
- [27] Shehta, A. I., Mabrouk, D., & Hamdy, W. (2025). An Artificial Intelligence Driven Query Optimization Framework to Enhance Business Intelligence Systems. *2025 International Conference on Future Telecommunications and Artificial Intelligence (IC-FTAI)*, 1–10. <https://doi.org/10.1109/IC-FTAI67960.2025.11384524>

- [28] Shiwakoti, S. (2025). The Role of Intelligent ERP Systems in Preventing Corporate Fraud and Strengthening Financial Governance. *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386 (Online), 4(3), 138–147. <https://doi.org/10.60087/jklst.vol4.n3.014>
- [29] Yanney, A. A. S. (2025). Redefining Corporate Financial Governance Through AI-Powered Predictive Models for Global Business Risk Management. *International Journal of Research Publication and Reviews*, 6(6), 24–49. <https://doi.org/10.55248/gengpi.6.0625.2037>
- [30] Yaseen, H., & Al-Amarneh, A. (2025). Adoption of Artificial Intelligence-Driven Fraud Detection in Banking: The Role of Trust, Transparency, and Fairness Perception in Financial Institutions in the United Arab Emirates and Qatar. *Journal of Risk and Financial Management*, 18(4), 217. <https://doi.org/10.3390/jrfm18040217>