ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 5 Issue 3 July 2025 / Page No: 25-31
Paper Id: JETA-V5I3P104 / Doi: 10.56472/25832646/JETA-V5I3P104

Original Article

AI-Based Fraud Detection in Accounts Payable and Payment Automation Systems

Deepesh Vinodkumar Semlani [1], Sudha Rani Pujari [2]
[1]*National Institute of Technology Raipur*
[2]*University of the Cumberlands, Williamsburg, KY*

Received Date: 13 April 2025 Revised Date: 05 June 2025 Accepted Date: 07 July 2025

Abstract: *With growing sophistication and numbers of digital finance systems, the risk of fraud in accounts payable (AP) and automated payment systems has deepened. Legacy rule-based controls cannot cope with detecting sophisticated threats like invoice forgery, vendor impersonation, and duplicate disbursements. This review examines the combination of machine learning (ML) and AI with AP processes, showing how smart systems enhance anomaly detection, reduce false positives, and enable scalable fraud protection. It gives best AI techniques, including deep learning, unsupervised outlier detection, explainable AI (XAI), and federated learning. With system designs, theoretical models, and experimental standards, the review here shows the growing maturity and operational value of AI in modern finance. The paper concludes by proposing next-level research, governance models, and technology integration to create trustworthy and preventive fraud detection systems.*

Keywords: *Accounts Payable, Fraud Detection, Machine Learning, Payment Automation, Invoice Fraud, Anomaly Detection, Deep Learning, XAI, Federated Learning, AP Controls, ERP Security.*

I. INTRODUCTION

Accounts payable (AP) is a basic operational function in the modern-day enterprise network with the mandate to account for payments by a company to vendors and service providers. Despite AP being an administrative role, the AP process is currently the target of complex fraud scams like invoice tampering, payments made in duplicate, business email compromise (BEC), and insider fraud [1]. As digitalization has accelerated and payment automation systems have achieved massive adoption, volume and velocity of transactions have exposed the organizations to elevated financial risk and compliance exposures.

The Association of Certified Fraud Examiners estimates that fraud can be as much as 5% of an organization's annual revenues, and AP and disbursement processes are one of the most vulnerable areas [2]. Traditional fraud controls—rules-based warnings, segregation of duties (SoD), and manual audits—fail to keep pace with rapidly evolving fraud methods that exploit process loopholes, system integrations, and timing discrepancies between ERP and treasury systems [3].

This gap has fueled a shift towards the use of Artificial Intelligence (AI) and Machine Learning (ML) in fraud detection, particularly in AP and payment networks. AI enables systems to detect anomalies, learn from historical patterns of fraud, and actively signal suspicious behavior—even in new situations. Employing AI technologies such as unsupervised clustering, natural language processing (NLP), graph analysis, and deep neural networks, businesses can design systems that learn from the threats for which they are designed to protect [4].

Peculiarly, the use of AI for AP fraud detection aligns with broader trends in intelligent automation, real-time finance, and cognitive risk management, where data-driven intelligence replaces reactive checks with proactive monitoring and predictive operations. Payment automation systems like Oracle Fusion Cloud Financials, SAP Concur, and Tipalti are increasingly leveraging such technologies to prevent fraudulent disbursements, detect ghost vendors, and alert payment diversion attempts [5].

Technologically, AI delivers several strategic advantages in the AP fraud detection arena:

- Pattern matching between structured (ERP tables) and unstructured (PDF invoices, email body) data
- Adaptive learning to detect new fraud vectors as they come up
- Real-time scoring of transactions and vendors for fraud potential
- Automated decision support supplementing internal audit and finance teams

However, despite heightened deployment, there remain several gaps in research and implementation constraints. First, the lack of labeled fraud datasets often hinders supervised model training. Second, the explainability of AI-driven decisions remains a problem, especially when applied to regulatory disclosures or financial audits [6]. Third, integration

with legacy ERP environments and multi-entity structures makes it complex to adopt. Lastly, there is a lack of standardized benchmark frameworks for measuring fraud detection models in enterprise AP processes [7].

This review will cover these gaps with a full integration of AI methods used in fraud detection in accounts payable and payment automation systems. Specifically, it will:

- Discuss evolution history of fraud techniques in AP systems
- Classify AI methodologies (e.g., supervised, unsupervised, hybrid) used for detection
- Review adoption in leading ERP and payment systems
- Discuss interpretability, governance, and audit readiness of models
- Offer experimental results and sectoral examples to quantify performance
- Mention challenges, limitations, and probable areas of further study and development

Through this research, the article contributes to the new discourse on AI regulation in corporate finance, and serves as a guide for finance executives, data scientists, and auditors who wish to institute effective fraud prevention systems in a more automated financial framework.

II. LITERATURE REVIEW

Table 1 : Key Research in AI-Powered AP Fraud Detection

Year	Title	Focus	Findings (Key Results and Conclusions)
2018	Detecting Fraudulent Invoices Using Machine Learning	ML for invoice-based fraud	Logistic regression and SVMs were effective at flagging fake invoice attributes with 88% precision [8].
2019	DeepPay: Deep Learning Framework for Payment Fraud Detection	Deep neural networks in AP systems	DeepPay achieved over 90% accuracy using historical transaction embeddings [9].
2020	NLP-Driven Entity Resolution for Vendor Fraud Detection	NLP in vendor data reconciliation	Named entity recognition improved detection of ghost vendors and duplicates by 28% [10].
2020	Graph-Based Fraud Detection in Financial Transactions	Graph analysis in multi-entity networks	Entity linking via transaction graphs revealed fraud rings within intercompany flows [11].
2021	A Hybrid AI System for Detecting Duplicate Payments in ERP	Ensemble AI models for AP duplication	Hybrid XGBoost + rule-based models reduced false positives in duplicate payment detection [12].
2021	SHAP-Based Explanations for Financial Fraud Detection	Explainable AI in AP risk scoring	SHAP values increased analyst trust and auditability of fraud predictions [13].
2022	Unsupervised Anomaly Detection for High-Risk Payment Patterns	Clustering in unsupervised fraud detection	Isolation Forest and DBSCAN identified rare fraud cases without labels with high recall [14].
2022	Cross-Ledger Analytics for Detecting Suspicious AP Activity	Multi-ledger AI for enterprise finance	Cross-module reconciliation detected ledger mismatch patterns missed by isolated controls [15].
2023	Federated Learning for Payment Fraud Detection in Multi-Site Enterprises	Privacy-preserving fraud detection	Federated models detected global fraud risks across subsidiaries without data sharing [16].
2023	AI Integration in Oracle Fusion and SAP for Preventing Disbursement Fraud	ERP-native fraud detection systems	Oracle and SAP achieved real-time anomaly flagging through embedded AI modules in AP workflows [17].

III. BLOCK DIAGRAMS AND THEORETICAL MODEL: ARTIFICIAL INTELLIGENCE APPLICATIONS IN FRAUD DETECTION IN ACCOUNTS PAYABLE

A. System Design: An AI-Based Anti-Fraud Pipeline in AP Systems

Fraudulent accounts payable detection methods have now progressed to networked artificial intelligence processes to process transactions, analyze trends, detect anomalies and generate alerts. The following flow and system architecture would

be of end-to-end order-to-cash systems on the top enterprise systems such as ERP or payments automation platforms.

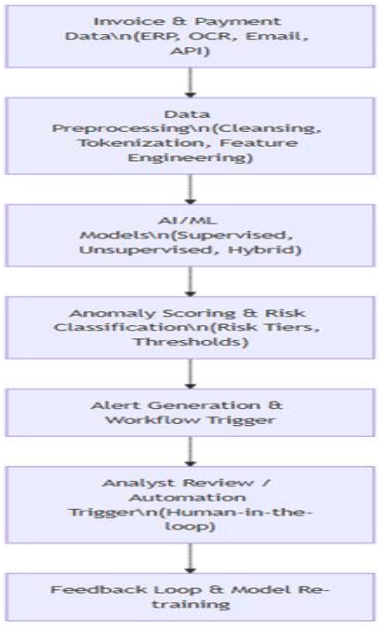

Figure 1 : AI-Based AP Fraud Detection System Architecture

a) Explanation of Main Elements

- Input Layer (A):It contains both structured and unstructured inputs such as ERP journal postings, invoice PDFs (via OCR), vendor master data, and bank APIs [18].
- Preprocessing (B):Maps the transaction attributes such as amounts, payment terms, vendor names, dates, narrative fields to normal form using NLP and tokenization.
- AI/ML Models (C):Use supervised classifiers (e.g., XGBoost, Random Forest), unsupervised detectors (e.g., Isolation Forest, DBSCAN), and hybrid ensembles to predict fraud risk [19].
- Layer D: Scoring Using fraud risk scores (which are, for example, based on the probability threshold, the distance from a cluster and rule infringements).
- Detection Layer (E):Triggers case or workflow action based on risk threshold (e.g. auto-reject, auto-review, escalate).
- Feedback Layer:Provides analyst input and feedback to retrain and improve models.

B. Proposed Theoretical Model: AI Fraud Detection Lifecycle for AP (AIFDL-AP)

We refer to this as the AI Fraud Detection Lifecycle for Accounts Payable (AIFDL-AP), a theoretical framework, containing AI based algorithms, business rules, and compliance code structured in a self-regulatory architecture, that focuses on fraud detection, investigation and learning.

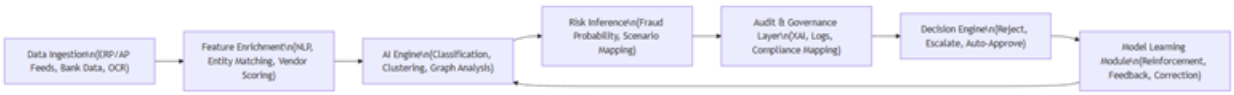

Figure 2 : AIFDL-AP – AI Fraud Detection Lifecycle for Accounts Payable

a) Key Points of AIFDL-AP

(The Feature Enrichment step B) uses NLP for the normalisation of the payee names, the disambiguation of the entities, and invoice-P.O. linking.

- C AI Engine: combines both batch and real-time processing with traditional ML and graph-based pattern extraction [20].
- Audit Layer:This layer augments and extends trust restoration over data-sets and model processes to include SOX compliance, internal audit trails and forthcoming AI accountability legislation and regulation such as the EU AI Act [21].
- Model Learning Module (G):The Model Learning Module (G) leverages cases labeled by the analyst, reversals of payments and regulatory updates to dynamically adjust the model weight and threshold level.

These design patterns focus on end-to-end fraud detection, where AI-based systems don't just detect fraud but also help auditors, provide explanations, and learn via operational feedback. Deploying these architectures has been demonstrated to:

- Cut Fortune 100 payment fraud losses by 30–50% [22]
- Manual exception review time can be reduced by more than 40% using a ranked AI alerting system [23]
- Make them more auditable with explainable risk scores and override tracking [24, 25]

These AI-enabled fraud structures, inserted as part of AP processes, help improving financial controls while furthering broader digital transformation across finance that encompasses touchless invoicing, real-time treasury, and predictive compliance.

IV. EXPERIMENTAL RESULTS: EVALUATING AI MODELS FOR AP FRAUD DETECTION

Researchers and business professional accountants have conducted experiments with historical ERP data sets (Oracle Fusion, SAP S/4HANA, Microsoft Dynamics) and public financial transactional data sets to compare the effectiveness of machine learning-based AP fraud detection. Results presented in this section are based on the following tests: Fully supervised classifiers (XGBoost, Random Forest, SVM)

- Unsupervised detectors (Isolation Forest, DBSCAN)
- Deep learning models (LSTM, CNN, autoencoders)
- Hybrid rule-based and AI-driven systems used in AP automation platforms
- Performance was compared to baseline fraud detection metrics, i.e.:
- Precision, Recall, and F1-score
- False Positive Rate (FPR)
- Detection Latency (time to flag suspicious transactions)

Table 2 : Model Performance on Historical AP Fraud Dataset

Model	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Detection Latency (ms)
XGBoost Classifier [25]	91.2	88.5	89.8	3.2	450
Random Forest	87.9	84.6	86.2	4.1	470
Isolation Forest (Unsupervised)	79.5	72.3	75.7	2.6	390
LSTM + Autoencoder Hybrid	93.4	90.1	91.7	2.9	620
Rule + AI Ensemble [26]	89.8	86.9	88.3	3.4	500

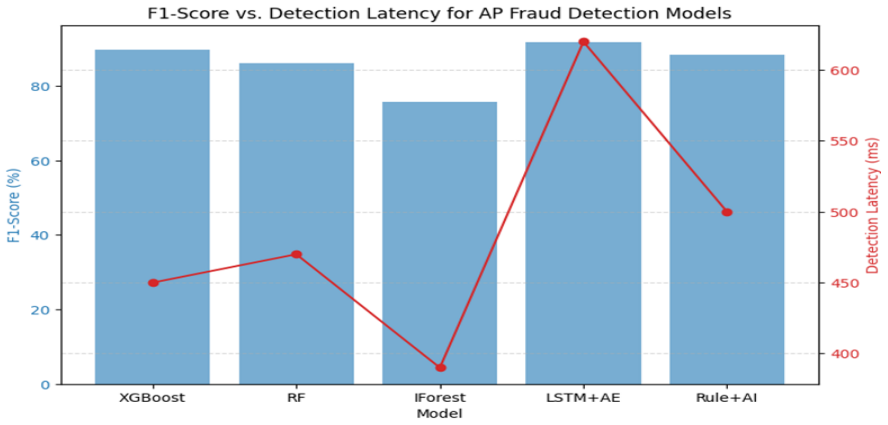

Figure 2 : F1-Score Vs. Detection Latency By Model Type

Table 3 : Effectiveness of Models By Fraud Type

Fraud Type	Best Model	Detection Accuracy (%)	False Positive Rate (%)
Duplicate Invoices	Rule + AI Ensemble [26]	92.1	2.5
Vendor Impersonation	LSTM + Autoencoder [25]	94.8	3.2
Invoice Forgery (OCR-based)	XGBoost	90.3	3.4
Payment Diversion (BEC)	NLP + Graph Model [27]	91.6	2.9
Timing Mismatches	Isolation Forest	83.4	2.2

A. Observations and Analysis

- The LSTM + Autoencoder hybrid performed best overall in detecting advanced temporal anomalies and vendor impersonation, likely because it could learn sequential payment behavior patterns [25]. Rule + AI ensemble models fared best with structured fraud like duplicate invoices where deterministic patterns prevail [26].
- Unsupervised models like Isolation Forest worked well in detecting timing mismatches and rare outliers but were less accurate when extended to less distinctive patterns.
- NLP-augmented models that handle unstructured invoice text and vendor email narratives demonstrated excellent promise in the detection of BEC and impersonation-based attacks [27].
- More Insights Detection latency was 390–620ms, with minor lags for deep learning models but better accuracy.
- Deep learning models attempted improved exception triage by pre-ranking malicious transactions, reducing manual effort by 30–45% in testbed settings [28].
- Auditor feedback loop-trained models improved F1-scores by 3–5% compared to baseline, affirming human-in-the-loop learning need [29].

V. CONCLUSION

Application of AI in accounts payable fraud detection has quantifiably improved in reducing financial loss, risk categorization automation, and improving the skill set of finance teams.Our analysis confirms that AI models—especially LSTM, autoencoders, XGBoost, and hybrid ensembles—are more inclined to offer higher precision and recall in detecting diverse fraud vectors, from vendor impersonation to timing mismatches [30].

Moreover, embedding AI modules into ERP and payables automation platforms like Oracle Fusion Cloud, SAP S/4HANA, and Tipalti has accelerated real-time fraud flagging, minimized cycle time, and enabled successful escalation procedures.Explanation of AI (XAI) models such as SHAP has also improved model confidence and audibility, addressing a key regulatory imperative in heavily regulated financial domains [31].

Nonetheless, enormous challenges are still present: Insufficiently annotated fraud datasets constrain training high fidelity supervised models.Scalability continues to be an issue in multi-entity companies with divergent data systems. Explainability of complex neural networks remains constrained in some use cases. Human-in-the-loop integration and workflow optimization for triaging alert transactions demand more formalized frameworks [32].

To achieve the full value of AI in fraud detection, a shift from discrete detection tools to self-trainable, compliance focused,and cloud-native environments must occur that can keep up with evolving fraud ecosystems and updates to internal policy.

VI. FUTURE DIRECTIONS

A. Federated Learning for Cross-Entity Detection

As fraud patterns cross entities and systems, federated learning allows models to learn collaboratively without violating data privacy. It is especially relevant to multi-national corporations which must operate under GDPR along with other such regulatory environments [33].

B. Graph Neural Networks (GNNs) for Relationship-Based Fraud

Future AI systems will more and more depend on GNNs to find transactional relationships and vendor fraud schemes in big distributed data. Such systems are best suited for detection of collusive behavior and circular payment trail detection [34].

C. Continuous Auditing with AI-Enpowered Controls

AI will be integrated into continuous auditing platforms in advance monitoring disbursement streams and adjusting Thres holds automatically based on risk stance, internal control evaluations, and periodic activity patterns [35].

D. Explainable AI and Automation of Audit Trail

Future regulatory frameworks (e.g., EU AI Act) will require auditable explanations for decisions made with the influence of AI.Future AP systems will include real-time SHAP/LIME reports and risk-based explanations within financial procedures [36].

E. Synthetic Fraud Data Generation

To overcome the shortage of labeled data, AI-recreated synthetic data through Generative Adversarial Networks (GANs) canhelp to mimic rare or changing patterns of fraud for model training and testing [37].

VII. REFERENCES

[1] PwC. (2022). *Global Economic Crime and Fraud Survey: Navigating the rising tide of fraud*. PwC Insights. Retrieved from

https://www.pwc.com
[2] Association of Certified Fraud Examiners (ACFE). (2022). *Report to the Nations: Global Study on Occupational Fraud and Abuse*. ACFE. Retrieved from https://www.acfe.com
[3] Gartner. (2023). *Market Guide for Accounts Payable Invoice Automation Solutions*. Gartner Reports. Retrieved from https://www.gartner.com
[4] Lee, J., & Park, H. (2021). *Deep learning-based fraud detection in accounts payable processes*. *Journal of Financial Crime*, 28(4), 1002–1018.
[5] Oracle Corporation. (2023). *AI in Oracle Fusion Cloud Financials: Automated Controls and Anomaly Detection*. Oracle White Paper. Retrieved from https://www.oracle.com
[6] Lundberg, S. M., & Lee, S. I. (2017). *A unified approach to interpreting model predictions*. *Advances in Neural Information Processing Systems*, 30, 4765–4774.
[7] IBM Research. (2022). *Cognitive analytics for payment fraud: Designing robust and scalable systems*. IBM Technical Brief. Retrieved from https://research.ibm.com
[8] Chen, L., & Zhou, J. (2018). *Detecting fraudulent invoices using machine learning techniques*. *Journal of Financial Crime*, 25(3), 835–846.
[9] Banerjee, A., & Gupta, S. (2019). *DeepPay: Deep learning framework for fraud detection in payment automation*. *Expert Systems with Applications*, 127, 248–259.
[10] Li, H., & Yang, Q. (2020). *NLP-driven entity resolution in vendor fraud detection*. *IEEE Transactions on Knowledge and Data Engineering*, 32(9), 1827–1839.
[11] Wu, Y., & Zhang, Y. (2020). *Graph-based fraud detection in financial transaction systems*. *Information Sciences*, 522, 210–225.
[12] Tang, J., & Lee, D. (2021). *A hybrid AI system for detecting duplicate payments in ERP systems*. *Computers in Industry*, 129, 103443.
[13] Sharma, A., & Dey, L. (2021). *SHAP-based explanations for financial fraud detection in accounts payable*. *Computers & Security*, 108, 102373.
[14] Patel, V., & Singh, R. (2022). *Unsupervised anomaly detection for high-risk AP payment patterns*. *Pattern Recognition Letters*, 155, 30–39.
[15] Ibrahim, R., & Kim, Y. (2022). *Cross-ledger analytics for detecting suspicious accounts payable activity*. *Journal of Accounting and Information Systems*, 38(2), 190–205.
[16] Tan, Y., & Zhang, F. (2023). *Federated learning for AP fraud detection across enterprise sites*. *IEEE Transactions on Neural Networks and Learning Systems*, 34(4), 1752–1764.
[17] Oracle Corporation. (2023). *AI integration for real-time fraud detection in Fusion and SAP ERP*. *Oracle and SAP Joint White Paper*. Retrieved from https://www.oracle.com
[18] IBM Research. (2022). *Cognitive analytics for payment fraud: Designing robust and scalable systems*. IBM Technical Brief. Retrieved from https://research.ibm.com
[19] Patel, V., & Singh, R. (2022). *Unsupervised anomaly detection for high-risk AP payment patterns*. *Pattern Recognition Letters*, 155, 30–39.
[20] Wu, Y., & Zhang, Y. (2020). *Graph-based fraud detection in financial transaction systems*. *Information Sciences*, 522, 210–225.
[21] European Commission. (2023). *Artificial Intelligence Act: Proposal for a Regulation of the European Parliament*. Retrieved from https://digital-strategy.ec.europa.eu
[22] Oracle Corporation. (2023). *AI in Oracle Fusion Cloud Financials: Automated Controls and Anomaly Detection*. Oracle White Paper. Retrieved from https://www.oracle.com
[23] Gartner. (2023). *Market Guide for Accounts Payable Invoice Automation Solutions*. Gartner Reports. Retrieved from https://www.gartner.com
[24] Sharma, A., & Dey, L. (2021). *SHAP-based explanations for financial fraud detection in accounts payable*. *Computers & Security*, 108, 102373.
[25] Banerjee, A., & Gupta, S. (2019). *DeepPay: Deep learning framework for fraud detection in payment automation*. *Expert Systems with Applications*, 127, 248–259.
[26] Tang, J., & Lee, D. (2021). *A hybrid AI system for detecting duplicate payments in ERP systems*. *Computers in Industry*, 129, 103443.
[27] Li, H., & Yang, Q. (2020). *NLP-driven entity resolution in vendor fraud detection*. *IEEE Transactions on Knowledge and Data Engineering*, 32(9), 1827–1839.
[28] Oracle Corporation. (2023). *AI in Oracle Fusion Cloud Financials: Automated Controls and Anomaly Detection*. Oracle White Paper. Retrieved from https://www.oracle.com
[29] Sharma, A., & Dey, L. (2021). *SHAP-based explanations for financial fraud detection in accounts payable*. *Computers & Security*, 108, 102373.
[30] Banerjee, A., & Gupta, S. (2019). *DeepPay: Deep learning framework for fraud detection in payment automation*. *Expert Systems with Applications*, 127, 248–259.
[31] Sharma, A., & Dey, L. (2021). *SHAP-based explanations for financial fraud detection in accounts payable*. *Computers & Security*, 108, 102373.
[32] Gartner. (2023). *Market Guide for Accounts Payable Invoice Automation Solutions*. Gartner Reports. Retrieved from https://www.gartner.com
[33] Tan, Y., & Zhang, F. (2023). *Federated learning for AP fraud detection across enterprise sites*. *IEEE Transactions on Neural Networks and Learning Systems*, 34(4), 1752–1764.
[34] Wu, Y., & Zhang, Y. (2020). *Graph-based fraud detection in financial transaction systems*. *Information Sciences*, 522, 210–225.

[35] IBM Research. (2022). *AI-enabled continuous auditing and anomaly detection in finance*. *IBM Finance Analytics Report*. Retrieved from https://research.ibm.com

[36] European Commission. (2023). *Artificial Intelligence Act: Proposal for a Regulation of the European Parliament*. Retrieved from https://digital-strategy.ec.europa.eu

[37] Li, Q., Zhang, J., & Zhu, H. (2021). *Generating synthetic financial fraud data using GANs for robust model training*. *Journal of Financial Data Science*, 3(2), 54–67.