A Review of Process Mining and Machine Learning Integration for Corruption Detection in Business Processes

Chaima Chaieb[1] and Kaouther Nouira [2]

Abstract— **This study investigates the integration of Process Mining (PM) techniques with Machine Learning (ML) algorithms to detect corrupt activities in business processes. PM has gained significant attention for its ability to analyze event logs and uncover inefficiencies, deviations, non-compliance, and regulatory breaches in real processes. However, its application in detecting corruption, fraud, or other unethical practices in organizational processes remains underexplored. Through a structured analysis of existing research, we examine how PM and ML have been applied in related areas such as fraud detection, and evaluate their relevance to addressing corruption-specific challenges. This paper advocates for the use of PM methods combined with ML techniques to improve corruption detection systems, outlining the key challenges and gaps in current approaches. By synthesizing insights from the literature and evaluating use-case applicability, this work provides a foundation for future research into corruption-aware process analytics.**

I. INTRODUCTION

Corruption constitutes a universal impediment that undermines economic development, erodes trust in institutions, and contributes to the misallocation of resources [8]. Detecting corruption remains a complex challenge, due to its hidden and often systematic nature. In this respect, traditional detection methods audit such as manual audits tends to be biased, costly and time-consuming and often fail to uncover complex behaviors that signal corrupt practices [9].

Nonetheless, PM which provides a data-driven analysis of processes by leveraging event logs, has shown promise in identifying inefficiencies and deviations from standard process [10]. For instance, by analyzing the sequence and timing of transactions, PM can uncover instances of favoritism in procurement processes [11], fraudulent payment approvals [12], or unusual approval patterns that might indicate bribery. Unlike traditional audits, which may focus on specific transactions or cases, PM provides a continuous, real-time view of organizational processes, enabling the identification of systemic issues that may point to widespread corruption [13].

However, PM relies on structured and complete event logs, often missing informal or concealed activities where corruption thrives. Additionally, it struggles to distinguish between errors and deliberate misconduct, especially in complex processes [15].

Furthermore, PM can be combined with ML techniques to enhance its detection capabilities. ML algorithms can analyze the data produced by PM to identify hidden patterns, classify suspicious activities, and predict future risks [14]. For example, ML can help flag transactions or contracts that deviate from established norms, classify processes as "high-risk," or even predict areas of potential corruption based on historical patterns [24]. The combination of ML along with PM presents an added advantage for more sophisticated pattern recognition, anomaly detection, and predictive insights.

Overall, combining the strengths of PM and ML may present a significant opportunity for detecting corruption in processes. PM provides a structured approach to analyzing workflows, uncovering inefficiencies, and identifying deviations, while ML enhances this capability by detecting hidden patterns and adapting to evolving corrupt practices.

The paper is structured as follows: Section 1 introduces the importance of addressing corruption and provides an overview of the study's objectives. Section 2 reviews the relevant background and related work, focusing on PM and its application in corruption detection. It explores how PM techniques can be used to uncover irregularities in business processes. Section 3 investigates the role of ML in enhancing PM, particularly in the detection of fraudulent activities . Finally, Section 4 concludes the paper by summarizing.

II. BACKGROUND AND RELATED WORK

According to [7], PM is an emerging discipline providing comprehensive sets of tools to provide fact-based insights and to support process improvements. This new discipline builds on process model-driven approaches and data mining. In other words, PM is a family of techniques used to analyze event data in order to understand and improve processes. PM is constructed on logs that include information case id, a unique identifier for a particular process instance; an activity, a description of the event that is occurring; a timestamp; and sometimes other information such as resources, costs, and so on.

There are three main types of PM: discovery, conformance, and enhancement [1]. Discovery is the most common type,

*This work was not supported by any organization.

[1]Chaima Chaieb is with the Institut Supérieur de Gestion, Université de Tunis, Tunisia.chaiebchaima@gmail.com

[2]Kaouther Nouira is with the Institut Supérieur de Gestion, Université de Tunis, Tunisia.kaouther.nouira@gmail.com

where the process model is derived from the event log data. This is typically used when there is no formal description of the process available, or when the actual process differs from the documented one. Conformance, on the other hand, is used to compare the actual process with a predefined model to identify deviations. This is useful in ensuring that the process is compliant with regulations and standards. Enhancement involves modifying or extending the existing process model based on the information derived from the event log data [6].

PM involves analyzing event logs from business processes to discover patterns, inefficiencies, and compliance issues. Traditional PM algorithms, such as Alpha Miner and Heuristic Miner, rely on predefined rules and structured data to visualize and analyze processes [3] [4]. However, these methods often struggle with the complexity of real-world data.

PM can play a critical role in detecting anomalies that could indicate fraudulent activities. These anomalies can reveal hidden fraud, or non-compliance within a business process. Below are some examples of how PM can be utilized in fraud and corruption detection:

- In a study by [28], the Heuristics Miner algorithm was used for fraud detection in procurement processes. The paper emphasized the algorithm's ability to analyze event logs and detect anomalies in business processes. By identifying deviations from standard procurement workflows, the system achieved an identification accuracy of 88%.
- The authors in [29] explored integrating process mining into financial audits while aligning with current standards. Their study confirmed PM's feasibility in enhancing audit practices by replacing manual procedures, thereby improving evidence robustness and audit reliability.
- In [27], process mining was applied to data from a Dutch financial institute for fraud detection. Compared to traditional methods, PM offered deeper insights into process flows and irregularities. Using tools like ProM, auditors visualized deviations and uncovered fraudulent behavior during forensic audits.
- PM techniques analyze event logs to identify deviations from expected workflows, which can indicate potential corruption or fraud [34].

A. Machine Learning in Process Mining

The growing volume of data in business information systems necessitates modern technologies to manage, analyze, and utilize it effectively for informed decision-making and operational control [16]. Traditional PM has been widely used to discover, monitor, and optimize processes directly from event logs, without requiring predefined models [17]. However, the majority of the proposed methods have demonstrated limitations ; such as detecting nested loops, managing duplicate and concealed works, and coping with concurrent processes [18] [2].

As previously discussed, PM focuses on identifying deviations and inefficiencies rather than intentional misconduct, making it difficult to distinguish between errors and fraudulent behavior [9]. Corruption involving collusion, off-record transactions, or deliberate data manipulation often falls outside the scope of traditional PM techniques [15].

This introduces the idea of integrating PM with ML algorithms. The integration of PM and ML algorithms presents a promising approach to detecting corruption across various sectors, particularly in auditing and financial transactions [35]. By leveraging these technologies, organizations can uncover anomalies and fraudulent activities more effectively than traditional methods. The following sections outline key aspects of this combined approach.

Recent studies have explored the use of ML to improve event log analysis and process discovery, but there has been limited research on combining PM with ML specifically for the detection of corruption-related activities.

Government procurement fraud detection In a public sector context, PM was applied to the procurement process of a government agency. The analysis revealed several anomalies, such as repeated sole-source contracts, delays in the tendering process, and approvals of excessive payments. A ML classifier trained on historical procurement data was used to flag potentially corrupt contracts. By analyzing deviations from the expected process model and applying predictive algorithms, the system identified several high-risk procurement contracts that were subsequently reviewed by auditors. [5]

Internal control evaluation in auditing In a study by [25], a model integrating PM and ML was applied to internal control evaluation in auditing. The focus was on identifying control weaknesses and anomalies within organizational processes. By using PM to map out the actual flow of activities and ML to detect deviations from normal behavior, the system highlighted high-risk areas that could indicate potential issues, including corruption. This integration allowed auditors to direct investigations toward these flagged areas, improving the efficiency of internal controls and enhancing the detection of fraudulent activities or unethical behavior.

Anomaly detection in Business Processes In a study by [30], PM was integrated with fuzzy association rule learning to detect anomalies, including fraud, in business processes. By utilizing recorded event logs and standard operating procedures, the system was able to identify deviations from normal behavior. The incorporation enhanced the accuracy of detection, particularly in spotting fraudulent activities. The use of fuzzy association rules allowed for more flexible

pattern recognition, improving the detection of complex and subtle fraud patterns, ultimately achieving high accuracy in anomaly detection within business operations.

Identity fraud detection in digital onboarding A recent study by [26] proposed the usage of a PM approach to detect identity fraud in digital onboarding using a real fintech event log. This proposed approach is capable of modelling the behavior of users as they go through a digital onboarding process, while also providing insight into the process itself. Through mixing PM techniques and the ML classifiers, they resulted a promising 80% accuracy rate in classifying users as fraudulent or legitimate.

Real-Time Workflow Optimization In a study by [19], the integration of artificial intelligence (AI) with PM was explored to enable the dynamic optimization of business workflows. The research proposed a novel model leveraging AI's predictive and adaptive capabilities alongside PM's strengths in discovering, monitoring, and improving processes from event logs. This integration aimed to provide real-time insights, allowing organizations to continuously optimize workflows, adapt to changing environments, and enhance operational efficiency.

Enhancing Clinical Operations with Process Mining and ML A study by [36] combined process mining and machine learning to improve hospital care. Using ProM and EMR logs, it identified workflow bottlenecks and checked compliance with clinical procedures. By tracking KPIs like treatment time and resource use, the approach enabled data-driven improvements. Despite healthcare complexity, adaptable ML models effectively managed patient variability, demonstrating the value of this integration for operational efficiency and decision support.

Based on the reviewed researches, we conclude that the integration of ML in PM can improves fraud detection and process optimization by detecting deviations from expected workflows. Several studies reported measurable improvements when integrating ML into PM workflows. For instance, [26] achieved an 80% accuracy in classifying fraudulent users in digital on boarding. [5] identified high-risk government contracts that were later confirmed by auditors, indicating increased detection precision. Other works reported time savings (e.g., [19] enabled real-time workflow optimization) and improved KPI tracking such as treatment duration, throughput, and resource utilization in healthcare ([36]). Despite these gains, a standard set of evaluation benchmarks remains lacking, highlighting the need for unified metrics to assess system effectiveness, scalability, and cost-benefit impact. Combining PM's process insights with ML's predictive power enables real-time monitoring and adaptive fraud prevention. As digital transformation expedites, we assume that these techniques will play a key role in ensuring compliance and integrity across sectors.

III. PM and ML for Fraud and Corruption Detection

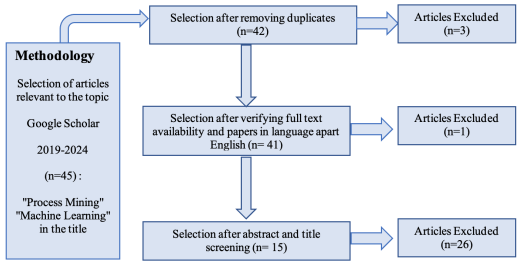
To explore the integration of PM and ML in fraud and corruption detection, we conducted a structured literature review using the following approach:

- **Search Strategy**: Google Scholar served as the primary search engine due to its wide indexing of academic and gray literature.
- **Timeframe**: Articles published between 2019 and 2024 were included to focus on recent developments.
- **Keywords**: The search used combinations of the following terms: "Machine Learning", "Process Mining", "fraud detection", and "corruption".
- **Inclusion Criteria**
  - Studies that explicitly discussed the integration of PM and ML, or their application to fraud detection.
  - Articles written in English.
  - Studies with accessible full texts
- **Exclusion Criteria**
  - Duplicate records.
  - Articles that focused solely on PM or ML without exploring their integration.
  - Studies lacking relevance to fraud, corruption, or anomaly detection in business processes.

Following the screening and selection process, the initial search yielded 45 articles. The selection proceeded as follows:

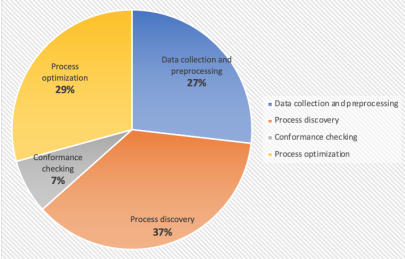
- *Step 1 (Duplicate Removal)*: duplicates were removed, resulting in 42 unique articles.
- *Step 2 (Full-Text Verification)*: 1 article was excluded due to lack of full text or insufficient methodological detail (n = 41).
- *Step 3(Abstract and Title Screening)*: 26 articles were excluded for not meeting inclusion criteria (e.g., discussing PM or ML independently, or unrelated domains like healthcare or cybersecurity).
- *Final Selection*: 15 articles were retained for in-depth analysis.

Fig. 1. Selection methodology



According to the literature review, the integration of ML in PM has demonstrated its effectiveness in four main areas. These findings are summarized in Figure 2, which presents a statistical breakdown of relevant publications, highlighting the growing adoption of ML-enhanced PM techniques in

Fig. 2. Result of selection methodology



fraud detection and process improvement.

Based on the reviewed research and provided pie chart the integration of ML in PM focuses on four main areas:

1) **Data Collection and Preprocessing** (27%)
   ML automate and enhance data collection process by extracting and cleaning event logs for better insights. ML algorithms show its capability in filtering noise, detecting missing event logs, and identifying patterns, and inconsistencies [14]. For instance, Random Forest and Support Vector Machines (SVM) can be used to classify and clean datasets by identifying data points that deviate from the norm.
2) **Process Discovery** (37%)
   ML techniques improve the discovery of process models by identifying hidden patterns and deviations within event logs that may not be obvious through PM traditional methods. ML algorithms show its capability in uncovering complex process behaviors and revealing inefficiencies or fraudulent activities [20] [23]. For example, Isolation Forest is effective in detecting outliers in complex datasets, which are often indicative of fraudulent activities or process deviations.
3) **Conformance Checking** (7%)
   ML enhance the comparison between observed processes and predefined models. In fraud detection, Anomaly Detection algorithms (like Autoencoders) can highlight discrepancies between expected and actual process behavior. Such ML algorithms show its capability in detecting deviations from expected process, helping to flag irregularities or non-compliance that may indicate fraudulent actions or errors [22].
4) **Process Optimization** (29%)
   ML is applied to enhance overall process efficiency, reduce bottlenecks, and detect fraud. ML algorithms like Random Forest and SVM not only predict where inefficiencies may lie, but also reveal areas where fraudulent actions could occur by analyzing historical data and identifying patterns of manipulation. Such ML algorithms show its capability in optimizing approval workflows, reducing opportunities for manipulation or unauthorized interventions [21].

The largest focus is on Process Discovery (**37%**), highlighting its critical role in unveiling the underlying structure of business processes—an essential step for identifying potential anomalies or inefficiencies that may be indicative of corruption. Process Optimization (**29%**) follows closely, underscoring the importance of refining process performance, which aligns with the broader objective of improving transparency and accountability in business operations. Data Collection and Preprocessing (**27%**) is also significantly represented, reflecting its foundational importance; high-quality, well-prepared data is a prerequisite for the effective application of ML techniques in PM. In contrast, Conformance Checking (**7%**) is notably underrepresented, despite its vital role in comparing actual behavior with predefined models to detect deviations often a strong indicator of non-compliant or corrupt practices. This imbalance suggests an opportunity for further research that leverages conformance checking to strengthen fraud detection capabilities.

Keeping up with this line of thinking, Figure 3 presents a quantitative analysis of ML approaches employed in fraud detection. This repartition reveals a predominance of **Supervised learning** (56%), common algorithms include SVM and Random Forest, well-suited for classification based on labeled historical data. **Unsupervised learning** (33%) techniques like Isolation Forest, k-Means, and DBSCAN help identify novel fraud patterns without prior labeling. The low occurrence of **Semi-supervised learning** (11%) might indicate that the usage of the semi-supervised paradigm is limited due to the lack of partially labeled datasets in practice.

Fig. 3. Distribution of machine learning approaches

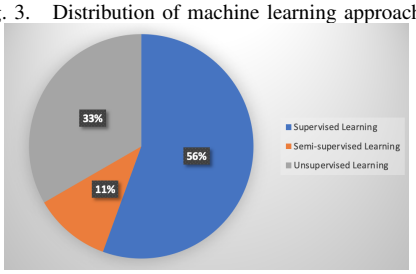


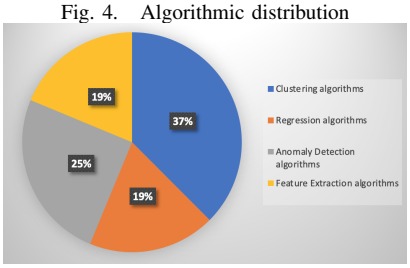
Figure 4 offers a more detailed breakdown of algorithms' types. First, **clustering algorithms** with (37%) are the most frequently used, which aligns with their effectiveness in grouping similar transactions and uncovering hidden patterns such as collusive networks—that may not be apparent through rule-based analysis. In second place, **Anomaly detection algorithms** with (25%) are widely used because of their ability to identify statistical anomalies that may be suspicious cases. **Regression algorithms and Feature extraction algorithms** make up 19% of implementations each, which is indicative of their roles in dimensionality reduction for predictive risk modeling. Regression techniques contribute to predictive risk modeling, while feature extraction methods support dimensionality reduction, enhancing model interpretability and performance.

It's properly to say that Supervised methods such as Support Vector Machines (SVM) and Random Forests are

particularly effective for classifying fraud when labeled data is available. In contrast, unsupervised techniques—including Isolation Forest, k-Means, and DBSCAN—excel at detecting unknown or emerging patterns in unlabeled datasets. Together, these approaches form a hybrid framework, where unsupervised methods initially identify potentially suspicious behavior, which is then verified and classified by supervised models.

Overall, the algorithmic distribution shown in Figure 4 emphasizes the field's reliance on pattern recognition and predictive accuracy as key components in the detection and prevention of financial fraud.

Fig. 4. Algorithmic distribution



A. Discussion

This study examined how combining Process Mining (PM) and Machine Learning (ML) can improve fraud and corruption detection. By integrating PM's event log analysis with ML's predictive capabilities, the approach enables more accurate risk assessments, increased transparency, and early identification of suspicious behavior.

PM uncovers inefficiencies, deviations, and non-compliance through conformance checking but is limited in predicting future fraud or detecting subtle patterns. ML addresses these gaps by identifying hidden behaviors and forecasting anomalies, though it requires large, well-structured datasets.

The synergy between PM and ML offers a powerful framework for fraud detection, providing:

- **Enhanced Detection**; detect hidden patterns of fraudulent activities that are not immediately visible through manual or rule-based analysis.
- **Proactive risk management**; predict anomalies before they escalate.
- **Improved compliance**; improve overall governance and compliance frameworks by identifying weaknesses or deviations from prescribed processes in real-time.

Fraudulent activities often manifest in several forms, including deviations from standard process, unauthorized modifications, or unusual transaction patterns [31]. Detecting fraud within business processes requires an advanced analytical approach that combines PM for conformance checking and ML for anomaly detection [32]. Key indicators of potential fraud identified in this study include [33];

- **Unusual sequences of activities** where events occur in an unexpected order, indicating potential manipulation or circumvention of standard procedures.
- **Abnormal attribute values** (Abnormal data points) such as unusually high transaction amounts, unauthorized access attempts, or inconsistencies in recorded data.
- **Temporal anomalies** where unexpected delays or rapid completions of tasks that may indicate artificial alterations in process execution.
- **Deviations from expected processes**; differences between actual process and the prescribed process (potential fraudulent behavior).

In conclusion, combining PM and ML enables automated, proactive, and more effective fraud detection—strengthening organizational governance and resilience against corruption.

IV. Conclusion

Integrating machine learning (ML) algorithms with process mining (PM) significantly strengthens the ability to detect corruption, fraud, and inefficiencies by introducing automation, predictive insights, and advanced anomaly detection throughout the PM lifecycle. While PM offers a robust foundation for understanding and visualizing business workflows, ML enhances this by enabling the detection of abnormal patterns, forecasting potential risks, and uncovering hidden trends indicative of corrupt practices. Together, they support more informed decision-making and enhance organizational performance.

The core motivation of this research is to explore the potential of combining PM and ML for corruption detection in business processes. This study provides a comprehensive overview of the current state of the field, highlighting both the opportunities and the challenges associated with this integration. Specifically, it examines how these technologies can complement one another, identifies technical and practical barriers to their combined application, and establishes a foundation for future research and real-world implementation.

The incorporation of ML into PM tools enhances corruption detection through several key capabilities:

- Automatically identifying anomalies and irregularities in process data.
- Predicting high-risk activities or transactions
- Uncovering hidden patterns of collusion, fraud, or bribery.
- Enabling real-time monitoring and alerts for suspicious activities
- Analyzing textual data for signs of fraudulent behavior.

Together, ML and PM provide a powerful combination for early detection, proactive prevention, and continuous monitoring of corruption, improving the overall integrity and transparency of business processes.

While significant progress has been made, the findings also reveal opportunities for future research, including:

- Designing more robust fraud detection frameworks that integrate multi-source data.
- Enhancing risk assessment tools with explainable AI components.
- Refining ML algorithms to adapt to evolving fraud patterns and emerging threats.
- Expanding the use of semi-supervised learning and text mining to address data scarcity and unstructured information.
- Investigating how ML and PM can be used not only for detection but to assess and enhance the resilience of business processes that is, their ability to prevent from corruption risks.

Ultimately, the article encourages further research into underexplored areas, paving the way for the development of advanced techniques and tools that leverage ML to optimize organizational processes and combat fraud and corruption effectively.

REFERENCES

[1] W. M. P. Van der Aalst, *PM: Data Science in Action*. Springer, 2016.

[2] C. A. and A. Khebizi, "A Road-map for Mining Business Process Models via Artificial Intelligence Techniques," *International Journal of Informatics and Applied Mathematics*, vol. 5, no. 1, pp. 27–51, 2022.

[3] P. Weber, B. Bordbar, and P. Tino, "A Framework for the Analysis of PM Algorithms," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 2, pp. 303–317, 2012.

[4] P. Ceravolo, S. Barbon, E. Damiani, and W. Van der Aalst, "Tuning ML to Address PM Requirements," *IEEE Access*, 2024.

[5] M. E. K. Niessen, J. M. Paciello, and J. I. P. Fernandez, "Anomaly Detection in Public Procurements Using the Open Contracting Data Standard," in *2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG)*, pp. 127–134, IEEE, 2020.

[6] S. Srivastava, "PM Techniques for Detecting Fraud in Banks: A Study," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 12, pp. 3358–3375, 2021.

[7] W. M. Van der Aalst, "PM: Discovering and Improving Spaghetti and Lasagna Processes," in *2011 IEEE Symposium on Computational Intelligence and Data Mining (CIDM)*, pp. 1–7, IEEE, 2011.

[8] A. Nikolaienko, O. Nikolaienko, H. Avanesov, S. Koshmal, and O. Lukashuk, "Corruption as a Threat to National Security: Analysis of Anti-Corruption Mechanisms and Their Effectiveness," *Economic Affairs*, vol. 69, pp. 23–31, 2024.

[9] N. S. Thomas, "The Applications of Data Mining Techniques in Detecting Occupational Fraud: A Qualitative Review of Forensic Accounting Practices," Doctoral dissertation, Dublin Business School, 2024.

[10] A. Mamudu, W. Bandara, S. J. Leemans, and M. T. Wynn, "A PM impacts framework," *Business Process Management Journal*, vol. 29, no. 3, pp. 690–709, 2023.

[11] L. J. Erasmus, "PM to eliminate corruption in the public sector," *Southern African Journal of Accountability & Auditing Research*, vol. 26, 2024.

[12] L. Reinkemeyer, *PM in Action: Principles, Use Cases and Outlook*, 2020.

[13] M. Imran, S. Hamid, and M. A. Ismail, "Advancing Process Audits with PM: A systematic review of trends, challenges, and opportunities," *IEEE Access*, 2023.

[14] G. Theodoropoulou, "Enhancement of PM with ML for identification of patterns in human behaviour," Doctoral dissertation, Université de Limoges; University of West Attica, 2024.

[15] N. Martin, D. A. Fischer, G. D. Kerpedzhiev, K. Goel, S. J. Leemans, M. Röglinger, and M. T. Wynn, "Opportunities and challenges for PM in organizations: results of a Delphi study," *Business & Information Systems Engineering*, vol. 63, pp. 511–527, 2021.

[16] A. Baiyere, H. Salmela, and T. Tapanainen, "Digital transformation and the new logics of business process management," *European Journal of Information Systems*, vol. 29, no. 3, pp. 238–259, 2020.

[17] M. Ghasemi and D. Amyot, "From event logs to goals: a systematic literature review of goal-oriented PM," *Requirements Engineering*, vol. 25, no. 1, pp. 67–93, 2020.

[18] F. Z. Trabelsi, A. Khtira, and B. El Asri, "Employing Data and PM Techniques for Redundancy Detection and Analytics in Business Processes," *Ingénierie des Systèmes d'Information*, vol. 28, no. 5, 2023.

[19] A. Doshi, "AI and PM for Real-Time Data Insights: A Model for Dynamic Business Workflow Optimization," *Journal of Artificial Intelligence Research and Applications*, vol. 3, no. 2, pp. 677–709, 2023.

[20] Y. Zhong, "Process Mining and Machine Learning for Intrusion Detection," Doctoral dissertation, The University of Liverpool (United Kingdom), 2023.

[21] A. Doshi, "Applying Machine Learning Models for Adaptive Business Process Mining and Workflow Optimization," *Journal of Artificial Intelligence Research*, vol. 1, no. 2, pp. 188–221, 2021.

[22] T. N. Gongada, A. Agnihotri, K. Santosh, V. Ponnuswamy, S. Narendran, T. Sharma, and Y. A. Baker El-Ebiary, "Leveraging Machine Learning for Enhanced Cyber Attack Detection and Defence in Big Data Management and Process Mining," *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 2, 2024.

[23] L. Vercosa, V. Silva, J. Cruz, C. Bastos-Filho, and B. L. Bezerra, "Investigation of lawsuit process duration using machine learning and process mining," *Discover Analytics*, vol. 2, no. 1, p. 9, 2024.

[24] O. A. Bello and K. Olufemi, "Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities," *Computer Science & IT Research Journal*, vol. 5, no. 6, pp. 1505–1520, 2024.

[25] H. K. Duan, M. A. Vasarhelyi, and M. Codesso, "Integrating process mining and machine learning for advanced internal control evaluation in auditing," *Journal of Information Systems*, pp. 1–21, 2025.

[26] M. C. D. Silva, G. M. Tavares, M. C. Gritti, P. Ceravolo, and S. Barbon Junior, "Using process mining to reduce fraud in digital onboarding," *FinTech*, vol. 2, no. 1, pp. 120–137, 2023.

[27] R. B. Bahaweres, J. Trawally, I. Hermadi, and A. I. Suroso, "Forensic audit using process mining to detect fraud," in *Journal of Physics: Conference Series*, vol. 1779, no. 1, p. 012013, IOP Publishing, 2021.

[28] D. Rahmawati, M. A. Yaqin, and R. Sarno, "Fraud detection on event logs of goods and services procurement business process using Heuristics Miner algorithm," in *2016 International Conference on Information & Communication Technology and Systems (ICTS)*, pp. 249–254, IEEE, 2016.

[29] M. Werner, M. Wiese, and A. Maas, "Embedding process mining into financial statement audits," *International Journal of Accounting Information Systems*, vol. 41, p. 100514, 2021.

[30] R. Sarno, F. Sinaga, and K. R. Sungkono, "Anomaly detection in business processes using process mining and fuzzy association rule learning," *Journal of Big Data*, vol. 7, no. 1, p. 5, 2020.

[31] T. Chiu, Y. Wang, and M. A. Vasarhelyi, "The automation of financial statement fraud detection: a framework using process mining," *Journal of Forensic and Investigative Accounting*, vol. 12, no. 1, pp. 86–108, 2020.

[32] Z. Tariq, D. Charles, S. McClean, I. McChesney, and P. Taylor, "Anomaly detection for service-oriented business processes using conformance analysis," *Algorithms*, vol. 15, no. 8, p. 257, 2022.

[33] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: a review of anomaly detection techniques and recent advances," *Expert Systems with Applications*, vol. 193, p. 116429, 2022.

[34] P. Chatsuriyawong, S. Toomsawasdi, P. Palangsantikul, and W. Premchaiswadi, "Analyze Credit Card Usage Behavior and Fraud Prevention by Process Mining," *2022 20th International Conference on ICT and Knowledge Engineering (ICT&KE)*, pp. 1–6, Nov. 2022.

[35] J. F. Rodríguez-Quintero, A. Sánchez-Díaz, L. Iriarte-Navarro, A. Maté, M. Marco-Such, and J. Trujillo, "Fraud audit based on visual analysis: A process mining approach," *Applied Sciences*, vol. 11, no. 11, pp. 4751, 2021.

[36] R. A. H. M., N. E. El-Attar, D. S. Abdelminaam, and M. Abdelfatah, "Analysis the patients' careflows using process mining," *Plos one*, vol. 18, no. 2, p. e0281836, 2023.