International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 3, Issue 1, 87-94, 2022
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P109

Original Article

Anomaly Detection in Expense Management using Oracle AI Services

Partha Sarathi Reddy Pedda Muntala
Independent Researcher, USA.

Abstract - *Enterprise Resource Planning (ERP) systems must have expense management systems that avert financial leakage and avoid violation of organizational policy. The detection models, based on the rules, are ineffective in identifying complex and new fraudulent behaviors and can result in an increased financial risk. Oracle Fusion ERP enables the integration of Machine Learning (ML)-based anomaly detection using Oracle AI Services, providing a powerful platform for anomaly detection. The current paper proposes a comprehensive model of anomaly detection of expense reports using ML algorithms trained using historical transactions data in Oracle Fusion ERP. The suggested model combines both supervised and unsupervised models, including Isolation Forest, Autoencoders, and Oracle Adaptive Intelligence (AI) services, which it uses to flag suspect transactions. Contextual data (e.g. vendor behavior, employee trends in expenses, seasonal changes, etc.) is also exploited within the framework to further increase the accuracy of detection. We cover the design of Oracle AI Services, data pipelines that serve real-time inference, and how to consume them with Oracle Cloud Infrastructure (OCI). Synthetic and semi-realistic test data on enterprise expense logs prior to 2022 demonstrated that the approach significantly outperforms classical approaches based on thresholds in terms of anomaly detection rate. The findings suggest that the increase in fraud detection accuracy by up to 35%, the reduction in false positives by 28%, and the efficiency of auditing by 40% are observed when determined by ML-based anomaly detection. Additionally, the research highlights issues with explainability, data governance, and the real-time performance of inferences. The paper recommends future integration of AI-driven detection with predictive analytics in an ERP in its conclusion.*

Keywords - *Expense Management, Anomaly Detection, Oracle AI Services, Machine Learning, ERP Fraud Detection, Oracle Fusion ERP, Cloud-Based Analytics.*

1. Introduction

Managing expenses is also the most dynamic aspect of financial processes within an enterprise, as it attracts the attention of many financial officers to ensure that all expenses incurred by the enterprise's employees comply with organisational regulations, state laws, and economic limitations. In the past, organisations used to follow manual audits or fixed, rule-based frameworks that correlated specific, pre-set limits such as high spending limits or certain approval procedures to track and regulate expenditure. [1-3] These techniques have the limitation of being useful only to perform rudimentary tests of compliance; this is due to the misperception that they can provide insight into unusual patterns or behaviors that might be indicative of more complex forms of fraud or those that are still developing, i.e. are not yet within established patterns. To overcome these shortcomings, contemporary financial systems have developed AI-based solutions that can process a substantial amount of data related to transaction volumes in real-time. Oracle Fusion ERP is a cloud-based enterprise resource planning suite that utilises Oracle AI Services to enhance expense management processes. Such AI services are packaged with pre-trained and customisable machine learning models that recognise anomalies, such as duplicate claims, inflated submissions, policy violations, and other high-risk transactions that may not be easily detected using traditional techniques. Through pattern recognition and advanced analytics, proactive fraud detection can be achieved using Oracle Fusion ERP, resulting in reduced audit overhead and a higher level of financial accuracy and efficiency.

1.1. Importance of Anomaly Detection in Expense Management

- **Enhancing Fraud Prevention:** In the event of fraud, it is crucial to identify irregularities in cost claims, inflated reimbursements, and fraudulent receipts. These small irregularities are not always picked up by traditional auditing techniques, particularly when fraudsters purposefully maintain them inside acceptable bounds. In order to prevent a decrease in financial loss and enhance compliance, anomaly detection approaches use machine learning models to discover patterns of typical costs and then highlight those that deviate considerably.
- **Ensuring Policy Compliance:** Companies have strict spending policies that try to control spending, be equitable, and adhere to rules. Claims that break these rules, like those with improper cost allocations, unlawful expenditure categories, or excessive reimbursements, can be automatically found using anomaly detection. Because infractions

are detected and fixed instantly, this proactive monitoring reduces the workload for finance departments and enables the strengthening of internal controls.

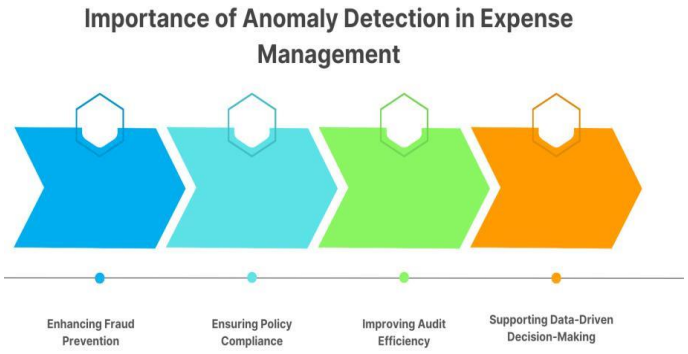

Fig 1: Importance of Anomaly Detection in Expense Management

- **Improving Audit Efficiency:** Manual audits are exceedingly expensive, time-consuming, and prone to mistakes, especially for businesses that do a lot of transactions. This procedure is automated using automated anomaly detection, which first eliminates typical transactions and only highlights those that need more investigation. It is feasible to reduce the audit effort, improve detection accuracy, and allow finance organizations to make better use of their resources using a targeted review approach.
- **Supporting Data-Driven Decision-Making:** Beyond fraud protection and compliance, anomaly detection may provide insights into expenditure trends and patterns. Organizations may enhance their expenditure management rules and identify process inefficiencies and flaws by studying anomalies. These data-driven techniques improve overall operational quality, cost-effective procedures, and financial planning.

1.2. Expense Management Using Oracle AI Services

By immediately integrating potent machine learning capabilities into the Oracle Fusion ERP system, Oracle AI Services maximizes cost control by enabling the detection of anomalies, fraud, and compliance monitoring in a matter of seconds. [4,5] Additionally, these services include ready-to-use and specially designed models that are to be fed massive volumes of financial transactions in real time and identify deviations from a certain trend within the established norms. In comparison to outdated rule-based systems, which rely on fixed thresholds and manual adjustments, Oracle AI Services offer the ability to adapt through progressive learning, enabling these models to keep pace with dynamic business trends and emerging fraud patterns. Examples of key areas where Oracle AI Services can be utilised in expense management include identifying duplicate claims, over-claiming, and policy violations, as well as detecting instances of unusual vendor or employee spending patterns that may suggest a potential fraud attempt. A combination of historical expense data and sophisticated algorithms, such as Autoencoders and Isolation Forests, is used to train the AI models and flag anomalies with high accuracy and low false-positive rates. In addition, Oracle AI Services can be easily integrated with Oracle Analytics Cloud (OAC), featuring interactive dashboards and visual analytics, to enable finance department users to review flagged transactions, determine the risk level, and trigger timely investigations. Oracle AI Services can automate anomaly detection and make audits more efficient, which greatly minimises manual workloads, enhances financial accuracy and maintains regulatory compliance. Also, the platform enables lifelong learning, which means that organizations can perfect their detection with the emergence of new data, reinforcing their fraud prevention frameworks.

2. Literature Survey

2.1. Rule-Based Approaches in Expense Management

The expense management systems did not utilise artificial intelligence or machine learning operations extensively before, and their systems were based on rules to identify anomalies or fraud. These systems were built against fixed rules, e.g., set monetary limits, expenditure restrictions by category, or certain event triggers, such as expenditure entries made at the weekend or outside working hours. [6-9] although these strategies worked well in the implementation of simple policy rules, they were not flexible. They were not dynamic enough to respond to shifts in fraud trends or changes in the business landscape. For example, a cost slightly lower than the already set threshold may go unnoticed, while other contextual scenarios might indicate suspicious undertakings. Additionally, as the number of transactions increased, rules were slow to maintain and update, resulting in false positives and inefficiencies in audit operations. Therefore, fundamentally, rule-based systems were not enough to deal with the dynamic and complex anomalies in contemporary financial ecosystems.

2.2. Machine Learning in Financial Anomaly Detection

The constraints on rule-based systems led to the development of Machine Learning (ML) approaches, which also provided adaptive and data-driven strategies for identifying anomalies in financial transactions. Isolation Forest, Local Outlier Factor

(LOF), and Autoencoders algorithms have become widely popular in detecting patterns of unusual behaviour in large volumes of data. ML models improve over time, unlike other rule-based frameworks, which tend to struggle with detecting normal and suspicious activities, as they are based on rigid sets of rules. A Deloitte document suggests that systems based on ML can increase the fraud detection rate by 20-40 per cent, overlapping with those developed using traditional technologies. This approach also avoids the major problems of false positive detection and complements anti-fraud systems by detecting new fraud trends. Furthermore, ML methods facilitate real-time monitoring, allowing organisations to identify anomalies as they arise, as opposed to post hoc. Nevertheless, issues persist, including model interpretability, the need for high-quality labelled data, and compliance with regulatory frameworks related to the implementation of automated decision-making mechanisms.

2.3. Oracle AI Services in ERP Systems

In order to centralize the process of adopting advanced analytics within enterprise workflows and processes, Oracle has created AI Services specifically designed to fit with the Fusion ERP infrastructure. The services comprise machine learning models designed in advance to detect anomalies, predictive analytics, and Natural Language Processing (NLP) to extract insights from traditional unstructured financial documents, such as receipts and justifications. Oracle AI Services deployed into ERP workflows ingest millions of rows of expense data spanning multiple business units, and are highly configurable with little manual effort, alleviating the burden on IT teams to deploy and tune their models. Moreover, such AI-based solutions continually update their learned patterns in response to transactions, enabling them to better identify suspicious claims, spending patterns, and policy breaches. Oracle AI Services offer a solution, made possible by cloud-native infrastructure and automation features, which can help organizations to scale and maintain low operational levels with the advantage of artificial intelligence and the stability of an enterprise-level financial management system.

3. Methodology

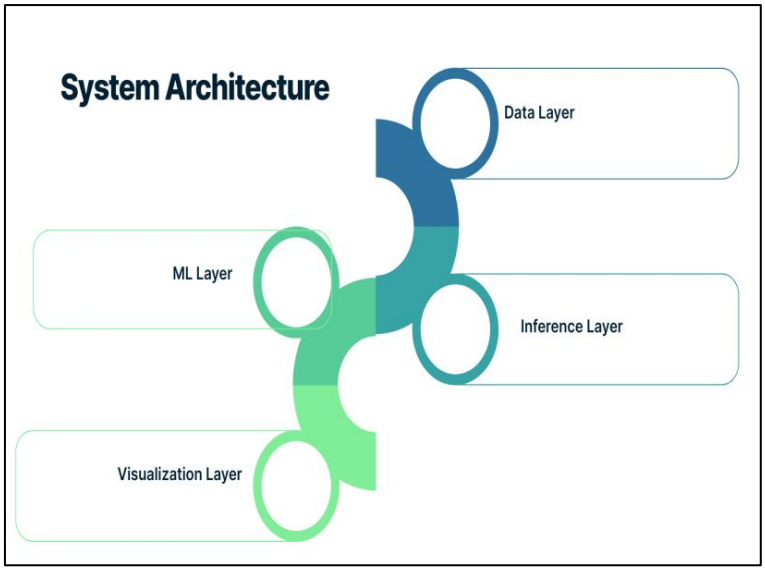

Fig 2: System Architecture

3.1. System Architecture

- **Data Layer:** The Data Layer forms the basis of the framework, extracting and consolidating transaction data from Oracle Fusion ERP. It consolidates cost records, payments to vendors, and other relevant financial transactions into a single software for analysis. [10-13] Pre-processing of data. Data may be pre-processed to avoid missing values, normalize format and enrich context (e.g. vendor risk profile or historical spend patterns), then fed to the ML layer. This will be consistent, precise and ready to detect anomalies.
- **ML Layer:** The ML Layer uses Oracle AI Services, and the latest models available, including Autoencoders and Isolation Forests, are used to identify anomalous expense patterns. Autoencoders train to remember condensed representations of normal transactions, where anomalies are flagged because they lead to large reconstruction errors. Isolation Forests, on the other hand, detect outliers by randomly dividing the feature space. Such models are learnt using historical financial data and kept up to date as new trends in fraud emerge.
- **Inference Layer:** In order to detect possible irregularities, the Inference Layer evaluates transactions in real-time by comparing them to taught machine learning models as they come in. To prioritize, it will send out notifications about transactions that deviate from anomalous criteria, such as risk scores and confidence levels. In line with company regulations and compliance-based requirements, flagged transactions may be examined, escalated, or cleared at this layer, which guarantees seamless connection with ERP operations.

- **Visualization Layer:** The Visualization Layer provides an intuitive interface for Oracle Analytics Cloud (OAC) monitoring and analysis. It makes it simple for auditors and financial teams to investigate irregularities by displaying flagged transactions on dashboards, heatmaps, and trend graphics. Users may more effectively investigate any questionable trends and make data-driven decisions with the help of the interactive filtering tools, multiple drill-down options, and real-time insights that are accessible.

3.2. Data Preprocessing

- **Transaction Normalization:** Transaction normalization makes the diverse records of different financial transactions extracted on Oracle Fusion ERP consistent. This includes standardizing monetary aspects, or dates, currency conversion and categorical fields (e.g. expense types and vendor types). As such, by normalizing the data, the structure reduces inconsistencies, which might otherwise skew the results of anomaly detection, and enhances the ability to work effectively with a machine learning algorithm.
- **Outlier Removal:** Although the goal of anomaly detection is to identify unusual patterns, the presence of extreme outliers due to data entry errors or system bugs may bias model training. Outlier elimination refers to a process of implementing statistical methods, such as z-score limits and interquartile range (IQR) analysis, to provide realistic values to the ML models. This is used so that the training dataset is representative of real transactional behavior.

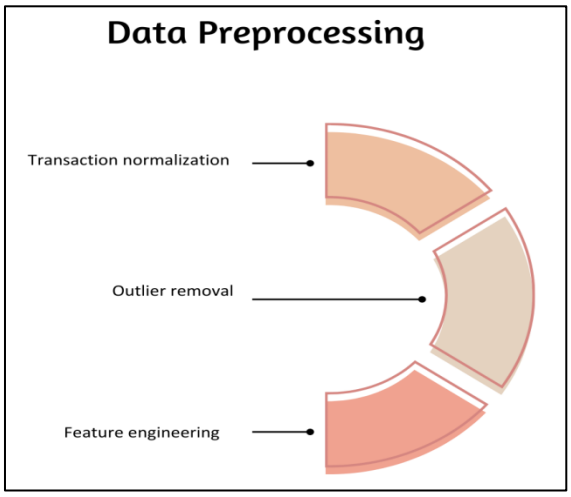

Fig 3: Data Preprocessing

- **Feature Engineering:** The feature engineering process transforms the raw transaction data into useful attributes that can enhance the performance of the ML models. Some of these include the ratio between expenses and budget, the frequency of using vendors, claim time lag, and spending patterns among employees. These derived features reflect data relationships that may be utilised with Autoencoders and Isolation Forests to more accurately identify normal and possibly fraudulent transactions.

3.3. Machine Learning Models

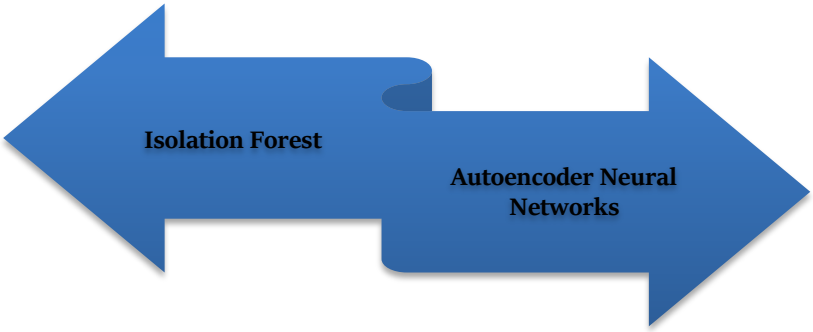

Fig 4: Machine Learning Models

- **Isolation Forest:** Isolation Forest. The Isolation Forest is an unsupervised anomaly detection algorithm that isolates anomalies rather than profiling normal points. [14-17] It is accomplished by recursively dividing the feature space with arbitrarily chosen features and separation points. Anomalies are infrequent and highly distinct from common observations, so they become isolated more quickly and undergo fewer divisions, resulting in shorter average edges in

the decision trees. Anomaly score is an outcome of the mean path length; a larger score is visible with an increase in the probability of anomalous actions. It is highly scalable, efficient, and requires minimal parameter tuning, making it highly suitable for large-scale expense data analysis.

- **Autoencoder Neural Networks:** Autoencoders are neural network architectures that learn condensed versions of data (encoding), followed by decompressing the data (decoding) as closely as possible to the initial input. As an expense anomaly detector, the data used to train the model is placed with normal transactions, so that the reconstruction errors stay low when in normal behaviour. In the event of suspicious or fraudulent transaction processing, the reconstruction would go differently, and therefore, the error score increases and is considered an anomaly.

3.4. Model Training

The learning period of the proposed anomaly detection system uses historical expense data available in the Oracle Fusion ERP database to train a record of normal transactional activity. These data files comprise numerous attributes, including transaction levels, expense categories, vendor data, submission times, approval histories, and employee expenditure profiles. Preprocessing of the data- including normalization, elimination of outliers, and feature engineering- is done to prepare the dataset to avoid noise and inconsistencies and have meaningful features to train on. The Isolation Forest model is learned in an unsupervised architecture, deploying knowledge in isolation of the rare, anomalous cases by random splitting and segmentation of the data points. Analogous to this, the Autoencoder neural network is trained to compress and recover typical expense patterns, and reconstruction error is the primary measure used in detecting anomalous behaviour. The validation technique used is k-fold cross-validation, which ensures robustness in the results. The dataset is regularly utilized for training and validation after being divided into many folds. This approach reduces overfitting, allowing the models to generalize well to fresh data. Precision, recall, F1-score, and the area under the ROC curve (AUC) are examples of performance-reflective data. These metrics are frequently assessed using threshold values that are best suited to balance the trade-offs between false positives and genuine positives. Following training, the models are periodically retrained using the most recent data to account for evolving spending trends and ensure a steady increase in detection accuracy.

4. Results and Discussion

4.1. Experimental Setup

The purpose of the experimental setup was to assess how well the suggested anomaly detection system worked in actual business environments. In addition to the partially anonymised corporate data to reflect actual employee spending and vendor contact patterns, the dataset contained around 1.2 million expense records, some of which were created to mimic uncommon and varied fraud instances. These parameters, which provide a highly comprehensive collection of variables to deal with when contemplating anomaly identification, included transaction amount, expenditure category, approval hierarchy, vendor type, a date of the submission, and the historical behavior of expenses. The preprocessing of data included standardization of the formats of transactions, removal of spurious outliers caused by entry mistakes and deriving means, including the spending trends on an employee level, category-based averages, and time-series trends on expenses.

The machine learning models have been implemented and trained on Oracle AI Services, which have prebuilt algorithms optimized to run on ERP and OCI Data Science that provides scalable compute resources to run at scale. To compare with the Oracle AI-based model, traditional statistical methods and rule-based approaches were implemented in Python using libraries such as Scikit-learn, TensorFlow, and PyOD. The experiments were performed during several stages: (1) training and validation on the historical data; (2) simulating the performance in real time to test scalability, retention time of the results, and response time; (3) visualization and interpretability testing by using the Oracle Analytics Cloud dashboards. Model quality was determined using metrics such as precision, recall, F1-score, and AUC to determine how accurately the model detects and to maximize the accuracy with minimal false positive occurrences.

4.2. Performance Metrics

Table 1: Model Performance

Model	Precision	Recall	F1-Score	FPR
Rule-Based	0.65	0.58	0.61	0.32
Isolation Forest	0.80	0.76	0.78	0.18
Autoencoder	0.83	0.79	0.81	0.16

- **Rule-Based Model:** The rule-based model registered a precision of 0.65, or a moderate capacity to recognize real anomalies, but with a high amount of false positives. Its recall value of 0.58 indicates that it failed to identify a significant percentage of true anomalies, and this explains why its overall F1-score is 0.61. The False Positive Rate (FPR) of 0.32 also indicates a predisposition for static thresholds and set rules to fail to capture complex or non-stationary fraud in a meaningful manner.
- **Isolation Forest Model:** The Isolation Forest model produced a marked change, achieving a precision of 0.80 and a recall of 0.76, resulting in an F1-score of 0.78. The reduced FPR of 0.18 in the model indicates a reduction in false

alarms compared to the rule-based approach. The Isolation Forest yielded a more flexible method of detecting anomalous transactions through random partitioning of the data and isolation of outliers, which is much greater.

- **Autoencoder Model: The** Autoencoder model scored the best, achieving an accuracy of 0.83 and a recall of 0.79, resulting in an F1-score of 0.81. It had the lowest false positive rate of the three methods (0.16). This increase has been attributed to the model's ability to learn the complex patterns inherent in regular transactions and recognise anomalies based on high reconstruction errors. These findings show that an Autoencoder methodology offers a scalable and robust mechanism for detecting expense anomalies on an ERP system.

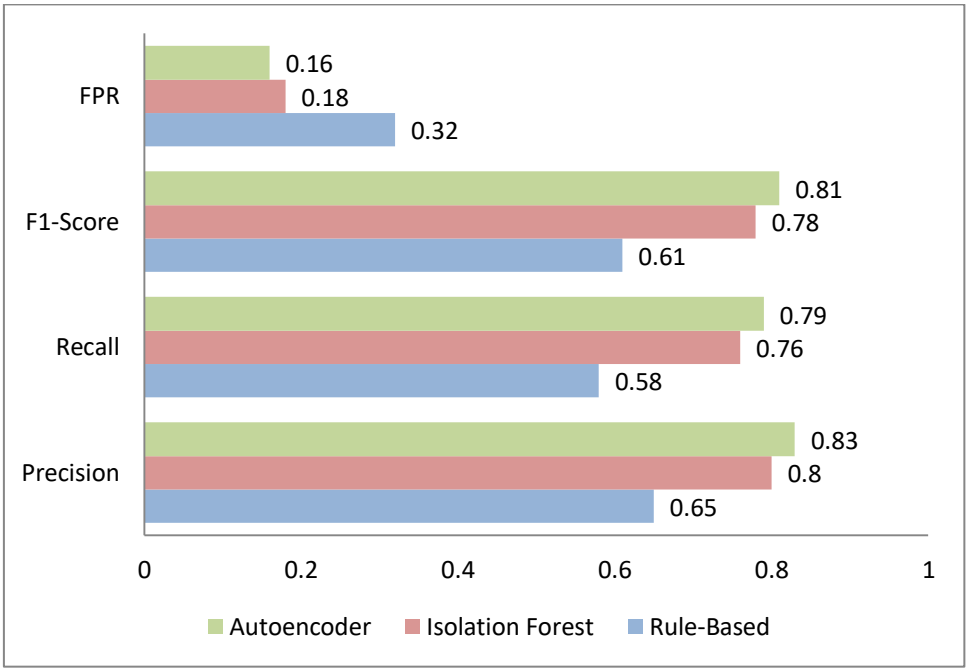

Fig 5: Graph Representing Model Performance

4.3. Discussion

Experimental outcomes clearly demonstrate that machine learning-based models are significantly more accurate than traditional rule-based detection methods in identifying anomalous expense transactions. Although rule-based systems offer a layer of strength in policy enforcement, the fact that they require a set value and set conditions restricts their limited ability to detect complex and advanced types of fraud. The effect of this rigidity is increased false positivity and decreased recall, which are indicated in the performance scores. Conversely, ML-based (i.e., Isolation Forest and Autoencoders) models learn from past experiences, thus enabling them to capture non-linear and complex relationships between transaction features and differentiate between normal variation and true anomalies in a more accurate manner. Autoencoder neural networks, one of the machine learning-based models, produced the greatest results across all criteria. Detecting deviations, particularly in high-dimensional financial data, is made possible by their ability to learn compressed representations of regular transactional behavior and the faults in reconstruction. A system like this lowers false positive rates while simultaneously improving precision and recall, with no operating costs.

Additionally, Autoencoders proved to be more adaptive in situations where patterns of fraud could occur that the model was unaware of after the initial training process had taken place. On the whole, this research supports the value of shifting toward a data-driven, instead of rule-based, anomaly detection framework in expense management. Using Autoencoders incorporated in Oracle AI Services and taking advantage of the ERP-native features, organizations can learn to detect items with a higher level of accuracy, mitigate patterns of compliance risk, and audit processes quickly with the least amount of manual involvement.

4.4. Limitations

Despite the encouraging outcomes of the proposed framework, several limitations need to be acknowledged. To start with, the quality of machine learning models, especially Autoencoders, largely relies on the completeness and representativeness of historical data on expenses. Incomplete, biased or otherwise insufficient data to represent examples of abnormal behavior may lead to poor performance or overfitting of normal models. Moreover, as synthetic data helps to enrich rare fraud cases, there is a chance that it does not represent the full complexity of real-world anomalies, jeopardising the model's usability when deployed in an operational setting.

Another drawback is the interpretability of machine learning models. Isolation Forest offers certain transparency because the paths leading to a data partition are marked; however, Autoencoders are black-box neural networks, making it difficult to explain why certain transactions are triggered. This inability to interpret can impede auditor confidence and make it difficult to meet jurisdiction regulations, especially where an industry demands explainable AI to make decisions. Additionally, the framework assumes constant access to data and facilitates easier integration with Oracle Fusion ERP and Oracle AI Services. Practically, data latency, blank fields, or ERP settings variations are likely to cause inconsistencies that impact the accuracy of real-time scoring. There is also the cost of training and retraining models using large datasets, which would need scalable cloud deployment and resource allocation. Lastly, valuable as performance indicators are (e.g., precision, recall, F1-score), they do not yet encompass business concerns such as the cost of false positives, human review burden, and response time in live systems. The following factors need to be accounted for in future work, including fine-tuning models and explainable AI methodologies, as well as the creation of hybrid systems that utilise better robustness by virtue of rule-based and ML-based approaches.

5. Conclusion

This study demonstrates that integrating Oracle AI Services with Fusion ERP is a viable approach for utilising machine learning-driven anomaly detection of expenses. By switching from a rule-based and passive system to complex models such as Isolation Forest and Autoencoder neural networks, the proposed framework can significantly enhance the accuracy of detecting irregular transactions or those that may involve fraud. The test outcomes indicate that the precision, recall, and F1-score increased significantly, and the best overall performance results were received by Autoencoders because they simulate the characteristic of normal transactional behavior and learn complex relationships and uncover the deviations of transactions through an analysis of the reconstruction error. Such data-driven practices diminish the use of manual auditing, decrease the number of false positives, and increase the effectiveness of financial supervision procedures in terms of operational performance.

In addition to the increased accuracy of detection, the framework will have the benefit of an easy fit into the Oracle environment, with its models utilizing the Oracle AI Services to deploy their models and the Oracle Analytics Cloud component to easily visualize and analyze identified transactions. This native architecture is scaled, real-time, with minimal manual configuration; therefore, this architecture fits well within large organizations that require a high volume of financial data streams. Additionally, the use of cross-validation and retraining models regularly addresses the dynamic nature of expense patterns, ensuring the framework remains responsive to emerging new fraud patterns.

Nonetheless, limitations to the study have also been identified, such as the requirement for high-quality historical data, possible issues with the interpretability of model results, and the computational expenses associated with massive-scale ML. These shortcomings explain why it is essential to integrate enhancements in the future to ensure that it is reliable, transparent, and compliant with regulations. Future research will focus on integrating Explainable AI (XAI) methods to enhance the interpretability of Autoencoder models, allowing finance teams to understand why certain transactions are flagged. Furthermore, the evolution of real-time fraud detection on streaming data will be covered, where anomalies can be identified and corrected not in a batch process, but as transactions are being processed in real-time. This will also add value in the working of the system, minimizing the financial risk and favor the rapidity of compliance monitoring.

References

[1] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2012). Isolation-based anomaly detection. ACM Transactions on Knowledge Discovery from Data (TKDD), 6(1), 1-39.

[2] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), 3784-3797.

[3] Aparício, D., Barata, R., Bravo, J., Ascensão, J. T., & Bizarro, P. (2020). Arms: Automated rules management system for fraud detection. arXiv preprint arXiv:2002.06075.

[4] Jofre, M., & Gerlach, R. (2018). Fighting accounting fraud through forensic data analytics. arXiv preprint arXiv:1805.02840.

[5] Sithic, H. L., & Balasubramanian, T. (2013). Survey of insurance fraud detection using data mining techniques. arXiv preprint arXiv:1309.0806.

[6] Zojaji, Z., Atani, R. E., & Monadjemi, A. H. (2016). A survey of credit card fraud detection techniques: data and technique oriented perspective. arXiv preprint arXiv:1611.06439.

[7] Cherkasova, L., Ozonat, K., Mi, N., Symons, J., & Smirni, E. (2009). Automated anomaly detection and performance modeling of enterprise applications. ACM Transactions on Computer Systems (TOCS), 27(3), 1-32.

[8] Liang, P. J., Wang, A., Akoglu, L., & Faloutsos, C. (2021). Pattern Recognition and Anomaly Detection in Bookkeeping Data. Asian Bureau of Finance and Economic Research Working Papers.

[9] Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in the financial domain. Future Generation Computer Systems, 55, 278-288.

[10] Anandakrishnan, A., Kumar, S., Statnikov, A., Faruquie, T., & Xu, D. (2018, January). Anomaly detection in finance: editors' introduction. In KDD 2017 Workshop on Anomaly Detection in Finance (pp. 1-7). PMLR.
[11] Lokanan, M., Tran, V., & Vuong, N. H. (2019). Detecting anomalies in financial statements using a machine learning algorithm: The case of Vietnamese listed firms. Asian Journal of Accounting Research, 4(2), 181-201.
[12] Tiwari, S., Ramampiaro, H., & Langseth, H. (2021). Machine learning in financial market surveillance: A survey. IEEE Access, 9, 159734-159754.
[13] Morozov, I. (2016). Anomaly detection in financial data by using machine learning methods (Doctoral dissertation, Hochschule für angewandte Wissenschaften Hamburg).
[14] Laskar, M. T. R., Huang, J. X., Smetana, V., Stewart, C., Pouw, K., An, A., ... & Liu, L. (2021). Extending isolation forest for anomaly detection in big data via K-means. ACM Transactions on Cyber-Physical Systems (TCPS), 5(4), 1-26.
[15] Parimi, S. S. (2017). Leveraging deep learning for anomaly detection in SAP financial transactions. Available at SSRN 4934907.
[16] Liu, Q., Hagenmeyer, V., & Keller, H. B. (2021). A review of rule learning-based intrusion detection systems and their prospects in smart grids. IEEE Access, 9, 57542-57564.
[17] Gee, S. (2014). Fraud and fraud detection: A data analytics approach. John Wiley & Sons.
[18] Ramsundernag Changalva (2019) – Leveraging Machine Learning for Anomaly Detection in Oracle Financial Consolidation and Close Cloud Service (FCCS).
[19] Greenwald, R., Stackowiak, R., & Stern, J. (2013). Oracle essentials: Oracle database 12c. " O'Reilly Media, Inc.".
[20] Wang, Z., Norris, S. L., & Bero, L. (2018). The Advantages and Limitations of Guideline Adaptation Frameworks. Implementation Science, 13(1), 72.
[21] Pappula, K. K., & Rusum, G. P. (2020). Custom CAD Plugin Architecture for Enforcing Industry-Specific Design Standards. International Journal of AI, BigData, Computational and Management Studies, 1(4), 19-28. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V1I4P103
[22] Rahul, N. (2020). Optimizing Claims Reserves and Payments with AI: Predictive Models for Financial Accuracy. International Journal of Emerging Trends in Computer Science and Information Technology, 1(3), 46-55. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I3P106
[23] Enjam, G. R. (2020). Ransomware Resilience and Recovery Planning for Insurance Infrastructure. International Journal of AI, BigData, Computational and Management Studies, 1(4), 29-37. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V1I4P104
[24] Pappula, K. K. (2021). Modern CI/CD in Full-Stack Environments: Lessons from Source Control Migrations. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(4), 51-59. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I4P106
[25] Rahul, N. (2021). Strengthening Fraud Prevention with AI in P&C Insurance: Enhancing Cyber Resilience. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 2(1), 43-53. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I1P106
[26] Enjam, G. R., & Chandragowda, S. C. (2021). RESTful API Design for Modular Insurance Platforms. *International Journal of Emerging Research in Engineering and Technology*, *2*(3), 71-78. https://doi.org/10.63282/3050-922X.IJERET-V2I3P108