International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 5, Issue 4, 105-116, 2024
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V5I4P111

Original Article

Automated Risk Scoring in Oracle Fusion ERP Using Machine Learning

Partha Sarathi Reddy Pedda Muntala[1], Sandeep Kumar Jangam[2]
[1,2]Independend Researcher, USA.

Abstract *- Enterprise Resource Planning (ERP) systems, such as Oracle Fusion ERP, serve as the backbone of financial and operational processes for many organizations. These systems manage vast amounts of data, making them ripe for risk assessment initiatives. However, traditional rule-based risk evaluation mechanisms within ERP systems can be static, slow to adapt, and limited in scope. This paper presents an automated, intelligent risk scoring framework using machine learning (ML) techniques integrated within Oracle Fusion ERP. The framework aims to assess risks associated with transactions, suppliers, and employees across financial and procurement modules. We developed and evaluated several ML models using historical ERP datasets and tested their performance using key metrics like precision, recall, and F1-score. Feature engineering focused on contextual ERP attributes like transaction frequency, supplier ratings, fraud indicators, and user behavior anomalies. The results demonstrate the potential of AI to transform risk management by enabling dynamic, real-time risk scoring within ERP systems. This approach improves decision-making, reduces financial fraud, and ensures better compliance with regulatory frameworks. The paper concludes with an analysis of implementation challenges, integration strategies, and the future scope of AI-driven risk scoring in enterprise environments.*

Keywords *- Oracle Fusion ERP, Machine Learning, Risk Scoring, Procurement, Financial Risk, Fraud Detection, AI in ERP, Compliance.*

1. Introduction

The ERP systems have emerged as a pillar of contemporary organizational activity, and they connect such essential business processes as finance, procurement, human resources, and supply chain management, combining them into an integrated digital environment. Oracle Fusion ERP is one of the most advanced solutions in the field, a next-generation ERP system with cloud-based functionality that supports cross-functional processes and provides real-time data visibility. [1-4] These ERP systems produce huge amounts of operational and transactional enterprise data as organizations continue to enhance their operations by increasing their level of digitization. Although the primary aim of installing ERP systems is to simplify operations and ensure consistent data, these tools are now capable of providing solid data-driven guidance on new risks, ineffective operations, and failure to ensure regulatory compliance, among other issues. The shift in how enterprises can utilise ERP data, from traditional process automation to intelligent, risk-aware platforms, represents a paradigm shift. Specifically, the volume and diversity of data that can be recorded within an Oracle Fusion ERP, including aspects such as invoice approvals, engagements with suppliers, or employee access patterns, provide a distinct advantage for utilising advanced analytics and machine learning tools to make informed decisions and prevent risks. With an increasing burden of regulation and exposure to financial fraud or operational failure, the need to hard-code intelligence into ERP systems is becoming more than performance-driven; it is also governance- and resilience-driven.

1.1. Importance of Automated Risk Scoring

- **Growing Complexity of ERP Environments:** The new generation of ERP systems, such as Oracle Fusion ERP, covers multiple departments and geographies, handling thousands of transactions per day. As more finance, procurement, human resources, and compliance processes become integrated, the manual-review-based or rule-based static approach to identifying risk is simply cost-ineffective and prone to error. The amount, speed, and diversity of data that ERP systems produce make it almost impossible to capture each anomaly, each fraud, or each policy violation promptly using traditional audit procedures.
- **Limitations of Traditional Rule-Based Systems:** Traditional ERP risk detection involves the use of predetermined thresholds or business rules. Although these methods are effective in prompting simple or ordinary control procedures, such as eliminating transactions that exceed a particular amount and requiring sanctioning of certain vendors, they are not flexible. They are unable to identify the development of subtle and emerging fraud activities. Additionally, they tend to yield high false positives or false negatives, which can overwhelm compliance teams or pass risks undetected.
- **Advantages of Machine Learning in Risk Scoring:** Machine Learning (ML)-based automated risk scoring offers a data-driven and dynamically adaptable alternative. It enables ERP systems to assess and evaluate risks with

consideration for potential variations in historical behaviour, patterns, and contemporary deviations. ML algorithms can suggest the likelihood of occurrence based on prior reports of fraud or compliance violations to detect such patterns in new data, and improve over time. This enables organizations to shift their focus from risk detection to risk prevention.

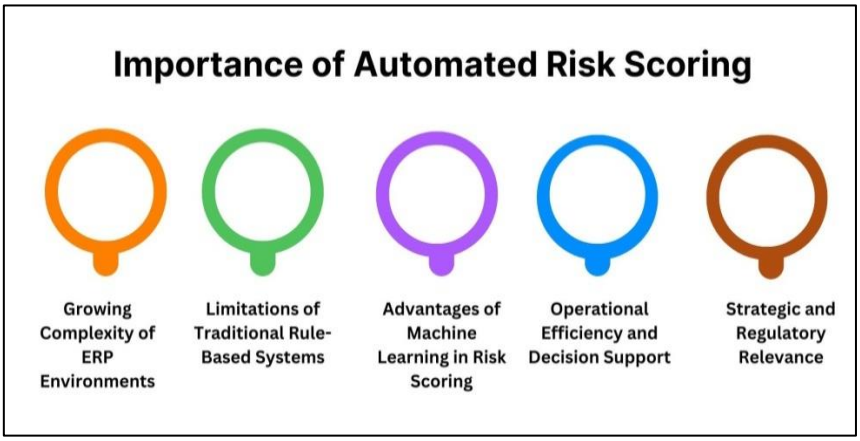

Fig 1: Importance of Automated Risk Scoring

- **Operational Efficiency and Decision Support:** Ensuring accurate risk scoring is more likely to improve accuracy than other detectors, thus ensuring a high level of productivity in the operational mechanism. It enables focused investigation and resource deployment, as it prioritises high-risk transactions, suppliers, or users. Moreover, by generating these scores straight into ERP processes, real-time decision support can be immediately available, including alerts, duplicate signatures, or transaction blocks on risk transactions, so that smart governance becomes part of normal business practice.
- **Strategic and Regulatory Relevance:** Compliant with regulations in risk scoring, the ease of automating and explaining the risk scoring process also ensures compliance in an environment where data privacy regulations and audit transparency are increasingly becoming stricter. Organizations can keep regulatory compliance, such as SOX, GDPR, internal audit requirements, etc. -- by keeping traceable and defendable risk decisions. That is why automated risk scoring is a strategic enabler of both operational integrity and enterprise resilience.

1.2. Oracle Fusion ERP Using Machine Learning

Oracle Fusion ERP is a global enterprise platform developed on cloud-native technologies, supporting various business processes, including finance, procurement management, human capital management, and supply chain management. [5,6] With organizations producing more and more operational and transactional data using these modules, it has become more imperative that some insight must be generated out of this data. The demand can be addressed with a powerful solution that enables Oracle Fusion ERP to go beyond automation and into intelligent decision-making, provided by Machine Learning (ML). When ML models are integrated into the ERP workflow, organizations can identify trends, mitigate risks, and perform difficult decision-making processes that would require a lot of time and effort to counter manually.

The possibility of improving risk management through the enterprise is one of the cornerstone advantages of integrating ML with Oracle Fusion ERP. For example, ML can be used to train on historical pull databases to detect suspicious instances in purchase orders, suppliers, or employee actions. These observations can subsequently be used to create risk scores, focus real-time audits, or activate real-time preventive controls. Moreover, the data architecture and analytics features of Oracle, especially when combined with tools such as Oracle Analytics Cloud and Oracle Integration Cloud (OIC), provide an optimal basis for training, deployment, and support of ML models in the ERP setting. Machine learning is also capable of supporting future predictions, anomaly detection, and smart automation of various ERP processes, in addition to reducing risk incidence. This involves forecasting cash flow, optimising procurement schedules, and suggesting approvals on a contextual basis. With ML integrated into its architecture, Oracle Fusion ERP helps increase operational efficiency while also driving strategic value, enabling data-driven governance and mitigating risks. The adoption of ML is still in a state of evolution, yet it is placing Oracle Fusion ERP at the focal point of an enterprise's smart operations.

2. Literature Survey

2.1. Traditional Risk Management in ERP

Risk management in classical ERP installations is usually considered to be based on a workflow, rule-driven, and essentially immovable. [7-10] Such systems work on predefined thresholds and conditions. An example is that a financial transaction likely to have a monetary limit may automatically induce a manual review or secondary endorsement. Although such mechanisms are simple and mostly effective, they are plagued by scalability issues and a failure to identify more complex

fraud types or frauds that do not overcome trivial limits. Additionally, manual review can lead to delays and is often prone to human errors, particularly in complex cases.

2.2. AI and ML Applications in ERP

The role of Artificial Intelligence (AI) and Machine Learning (ML) in ERP systems has seen a strong dynamism in recent years. Research has shown that machine learning models, including logistic regression, decision trees, support vector machines (SVMs), and neural networks, are utilised to identify anomalies, automate internal audits, and monitor compliance on ERP systems. These models offer a dynamic and data-driven approach that yields better results than traditional systems relying on rules in identifying non-obvious patterns. However, past implementations of ML in ERP have, in many cases, been focused on small domains, particularly by detecting invoice fraud or automating approval routines, rather than providing system-wide intelligence across modules.

2.3. Gaps in Existing Research

Although there are some achievements, there are still some gaps in the existing study environment. A single weakness is the lack of integrated AI structures, which can span multiple ERP modules (e.g., finance, procurement, HR). Many current applications are limited to single processes, resulting in disintegrated intelligence and cross-functional risks. Additionally, most AI models do not integrate well with modern cloud-based enterprise resource planning systems, such as Oracle Fusion ERP, which limits their ability to successfully deploy and scale in real-world enterprise systems. Another issue is the lack of emphasis on explainability and compliance with regulations. The interpretability of black-box ML models is notoriously challenging, creating problems with audits and user trust, as well as adhering to guidelines such as GDPR or SOX.

2.4. Recent Advances

Recent research has attempted to address these pressures with varying degrees of effectiveness. Some of the prominent approaches highlighted, along with the respective AI methods employed and their limitations regarding ERP systems, are summarised below. For instance, the implementation of logistic regression on SAP systems has proven its effectiveness, although it is currently confined to the finance module. Neural networks, employed in Oracle E-Business Suite, exhibit satisfactory predictive ability but are non-interpretable. The application of Support Vector Machines to custom ERP systems can be effective in specific cases; however, it is generally not scalable and does not transfer well to other enterprises.

3. Methodology

3.1. System Architecture

- **Data Layer:** The data layer is meant to transform and extract data in Oracle Fusion ERP. This encompasses transaction logs, user activity records, master data, and audits across various departments, including finance, procurement, and human resources. The data is also scrubbed, standardized, and organized into forms favorable for use downstream. [11-14] This layer helps ensure the integrity of data and gives a uniform basis of analysis and modelling.
- **Feature Engineering Layer:** After obtaining raw data, the next level, feature engineering, generates useful variables and patterns that are suitable for use by machine learning models. It entails counting transactions over time and generating a time-based trend, encoding categorical variables and determining deviations from historical trends. The objective is to present raw information material as a formatted and educational list of features that would represent not only present-day behavior but also past context.

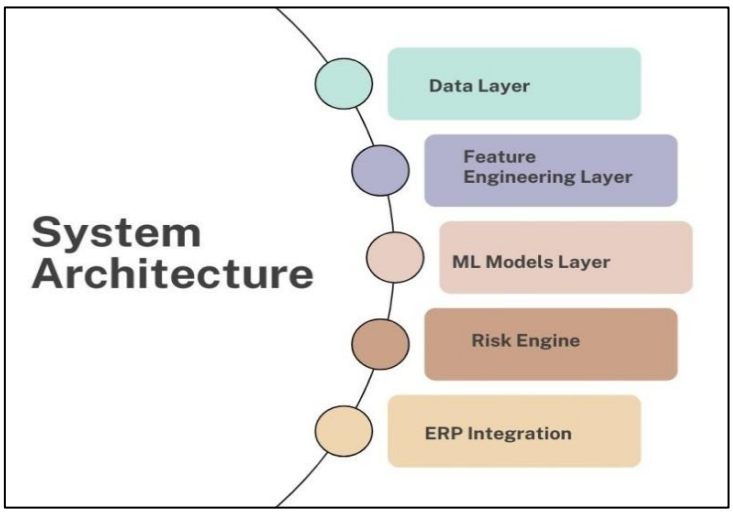

Fig 2: System Architecture

- **ML Models Layer:** This layer utilises various machine learning models on the engineered features. Based on the application case, either logistic regression, decision trees, or neural network models will be used to create anomalies, predict fraud, or score risk. Historically labelled data are used to train each model and validate the model using the training data to support accuracy and generalisation. The performance of the models is regularly checked to monitor changes in business processes and data patterns.
- **Risk Engine:** The risk engine integrates the predictions of ML models to create a score for the risks associated with various entities, including transactions, vendors, and employees. It uses business logic, thresholds and weightings to categorize risks as being low, medium and high. Those risk scores then instruct the system to generate an alert, initiate a workflow, or flag a transaction for manual review. The engine is the most crucial component in making AI outputs actionable intelligence.
- **ERP Integration:** Lastly, the ERP integration layer returns the risk scores and insight to Oracle Fusion ERP workflows. This provides an opportunity to take real-time actions, such as halting suspect transactions, placing a vendor under review, or implementing exception handling measures. The feedback loop will make the insights generated by the AI visible and a part of the day-to-day activities of the ERP system, making it more responsive and controllable as a whole.

3.2. Data Sources

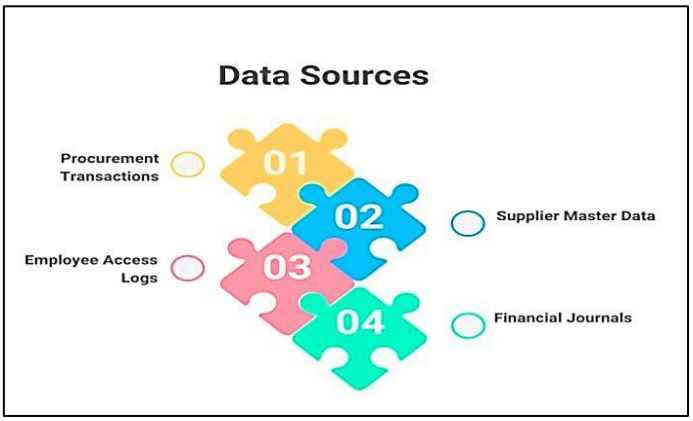

Fig 3: Data Sources

- **Procurement Transactions:** The data available in procurement transactions includes purchase requisitions, purchase orders, goods receipts, and payments to suppliers. This information tracks the entire procurement cycle and plays a crucial role in identifying abnormalities within the procurement process, such as duplicate orders, inflated pricing, or unauthorised purchases. By examining trends in quantities, frequencies, and vendor patterns, this data can be used to base procurement risk assessments and detect fraud.
- **Supplier Master Data:** Supplier master data contains reference and static information about each vendor, including its business name, contact details, bank accounts, tax identification numbers, and contractual terms. This information can help confirm the authenticity of suppliers and is necessary to identify risks, such as duplicate or fake suppliers, blacklisted vendors, or suppliers without compliance documents. Any deviances or regular alterations in such data may be an indication of fraud or even self-collusion.
- **Employee Access Logs:** The employee access logs track the actions users take in the ERP system, including their login times, activities performed, modules accessed, and modifications made to records. This information becomes fundamental in detection of unauthorized access, policy or insider threats. Using the access patterns concerning the transaction behavior, the system can make discoveries on the abnormal user activities which are not normal in job designed activities or times.
- **Financial Journals:** Accounting entries are recorded in finance journals when handling various transactions, including general ledger postings, adjustments, and accruals. These entries reveal the financial consequences of business transactions. They are an essential part of identifying irregularities in the accounting system, which may include bizarre journal entries, backdated entries, or failure to properly map accounts. Financial journals also help ensure the integrity of procurement and expense data by providing a cross-reference of recorded transactions.

3.3. Feature Engineering

When applying machine learning to a situation such as ERP-based risk detection, feature engineering is a major intervening variable in producing successful machine learning models. Features applied in this system were chosen based on extensive knowledge in procurement, finance, and IT controls. These characteristics are meant to garner the trend in behavior, trends in operations and anomalies that may point towards possible risks or anomalies. The system is also better able to identify small abnormalities that traditional rule-based systems would otherwise overlook, as it can transform mundane raw

transactions and audit data into valuable attributes. The most important of them is txn_amount_avg, which determines the average amount of transactions made by a supplier or employee in the last six months.

This aspect helps define the normalcy of transactions by prompting the system to raise red flags whenever there is an anomaly, such as large purchases or spikes in payments. There is another key attribute, supplier_rating, which indicates the supplier's performance score in areas such as timeliness of delivery, accuracy of invoices, and dispute cases. This is an excellent option in predictive modelling because suppliers with lower ratings may have a greater operational or financial risk. The number of accesses by an employee to the ERP system within 30 days is calculated using the employee_login_freq feature. An abrupt increase or decrease in the number of logins, especially by individuals with privileges on financials or procurement, may indicate an imminent internal threat or corruption. Finally, the txn_flagged_ratio is used to calculate the ratio of the number of transactions that have been flagged in the past due to review or anomaly on an entity level. A significantly high ratio may also be a sign of a non-compliance trend or frequent problems worthy of further investigation and analysis. Such characteristics, as well as others, constitute the input to the elements of machine learning. They need to be chosen in the first place and developed on an ongoing basis, which helps increase the accuracy of the model, clarity of the effort, and strengthens robust, actionable insights in the ERP risk engine.

3.4. Machine Learning Models

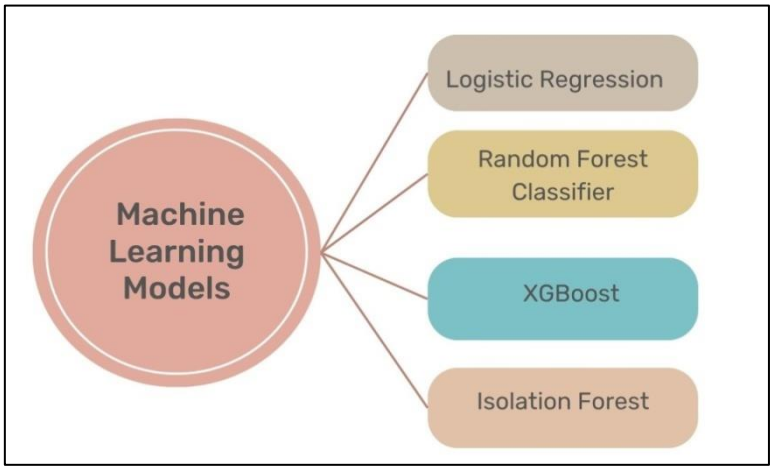

Fig 4: Machine Learning Models

- **Logistic Regression:** Logistic Regression is the simplest and most interpretable approach, which is also effective in binary classification. [15-18] It approximates the chances that a particular transaction or behavior would be risky as a set of linear combinations of the input features. Although it is not robust when dealing with complex patterns, it provides useful information concerning feature importance. It can serve as a baseline against which other, more advanced models will be evaluated.
- **Random Forest Classifier:** This classifier applies the ensemble learning technique, where several decision trees are built during the training process, and the result is returned as the mode of the decision trees. It is specifically effective when dealing with large datasets and extracting non-linear relationships among features. When considering the risk detection associated with ERP, it aids in discovering highly complex interactions amongst various variables, e.g. user behavior and financial anomalies, with a great degree of precision and resilience to overfitting.
- **XGBoost:** The gradient boosting machine implementation, in the form of Extreme Gradient Boosting (XGBoost), is an extremely efficient and scalable machine learning algorithm. It constructs sequential trees that successively improve upon the mistakes of preceding trees, making it suitable for working with imbalanced and noisy data. XGBoost has demonstrated good performance in predicting high-risk transactions, supplier fraud, and policy violations. Compared to traditional models, it has been shown to be both faster and more accurate, with a higher percentage of accuracy.
- **Isolation Forest:** Isolation Forest is a specialised type of unsupervised learning algorithm trained for anomaly detection. Its mode of operation is based on the random, separate isolation of observations that are drastically different to the average. The model can be especially helpful in identifying uncommon and new risk conditions in ERP data, e.g., when suspicious log-in activity or improper journal entries occur, without the need for labelled training data. It supplements the supervised models by identifying outliers that would otherwise be overlooked.

3.5. Model Evaluation Metrics

- **Precision:** This is defined as the fraction of positively identified predictions divided by the total number of positive predictions made. In the ERP risk detection industry, it indicates the number of transactions or individuals flagged as being risky that were indeed risky. This is particularly important when false positives are expensive, e.g., when

withholding a payment to an honest supplier can cause business problems. Accuracy will thus warrant that the model identifies only those transactions that are suspicious.

- **Recall, also referred to as sensitivity, determines the ratio of the actual positive cases that were correctly** classified as such by the model. This is an ERP system's sign of the model's capacity to identify all possible threats or aberrations. With a high recall value, the system has a high likelihood of detecting most actions that are not in line with regulations or indicative of fraud, and critical issues are unlikely to be overlooked. It is especially significant when unnoticed fraud or non-compliance has a dire monetary or regulatory implication.

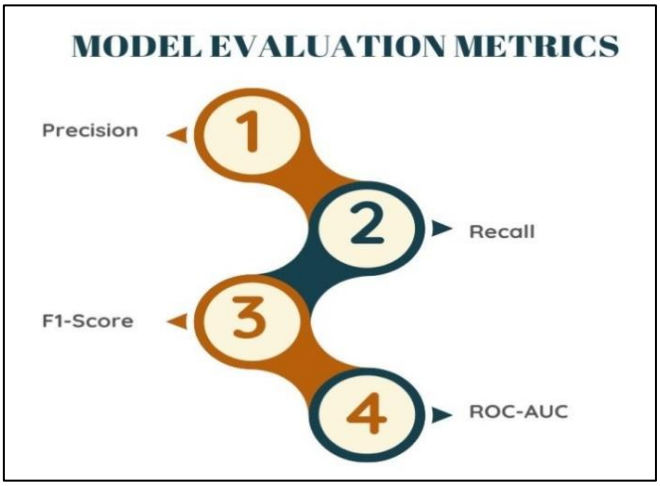

Fig 5: Model Evaluation Metrics

- **F1-Score:** The precision and recall are combined into a harmonic mean, which provides a balanced analysis of the F1-Score's performance. It has become particularly handy where the distribution of risky and non-risky events is not even, which is usually the case with ERP databases. The F1-score is quite high, indicating that the model strikes a balance between not marking too many false positives and not missing real anomalies, thereby forming a solid indicator of the model's overall effectiveness.
- **ROC-AUC:** A score of Receiver Operating Characteristic - Area under Curve (ROC-AUC) measures the performance of the model to differentiate between classes in all possible thresholds of classification. The higher the ROC-AUC value, the more the variation of risky and non-risky events that the model can capture. It provides a bird's-eye view of model performance, disregarding a particular threshold, and is useful in model selection where comparisons between models need to be made.

3.6. Risk Score Interpretation

The ultimate score of a risk in the system is then calculated as a weighted combination of various risk dimensions, which may indicate another source of possible anomaly or compliance non-conformance in the ERP ecosystem. Such elements are Transaction Risk, Supplier Risk and Employee Behavior Risk. Combining all these dimensions, the system ensures that both the detection and the overview of risk involving each entity or activity are not limited to a particular perspective. Transaction Risk represents the potential for anomalies in a specific financial or procurement transaction. This component is based on aspects such as unusually high transaction amounts, inappropriate approval chains, abnormal time schedules, or precedents in prior flagging. For example, a large purchase order placed after business hours or without mandatory approval would result in an elevated transaction risk score. Supplier Risk is the assessment of a vendor's reliability and integrity concerning a transaction. This will be founded on past performance indicators, checks on compliance, and consistency with the master data.

Such features include low delivery scores, recent changes in banking information, duplicate supplier accounts, or an earlier history of participation in flagged transactions, which help make up this component. Suppliers who delay their delivery, have frequent tax ID mismatches, or have been previously audited attract a higher risk weight. Employee Behavior Risk exposes the acts of people using the system of an ERP, especially the initiators or approvers of transactions. Such metrics as the number of logins, the right to access sensitive modules, and abnormalities of behavioral patterns. Examples of such risk increases could be an employee who logs on to the ERP system at an uncommonly late hour or accesses modules that extend beyond their job role. A weighted formula can be adjusted to these three components, allowing the system to prioritise within the organisation. The resultant composite score can be used to prioritise high-risk cases for audit or intervention, as well as to offer a clear and understandable risk picture that is useful for both automated controls and manual exploration.

4. Results and Discussion

4.1. Dataset Overview

In the course of this study, a simulated Oracle Fusion ERP was utilised in the development of data comprising three sets: procurement, finance, and human resources modules. The database covers 12 months, comprising more than 1 million transactional datasets, 5,000 supplier records, and specific log records for approximately 1,200 staff members. The heterogeneous and large quantity of data can describe a broad set of business operations, including the arrival of purchase orders, journal entries, user access events, and supplier ratings, which is a good candidate for developing and testing machine learning models that can support risk detection. The data set contains both structured and semi-structured data. Structured data includes transaction records with well-defined data fields, including transaction ID, amount, date, supplier ID, approval status, and cost centre. Access logs and audit trails are available as semi-structured data, which includes metadata such as timestamps, the module accessed, user ID, and the type of activity carried out. Additionally, the master data, such as that of suppliers (i.e., banking details, tax identification numbers, and date of onboarding) and employees (i.e., role, department, and access level), should be provided to enrich the dataset and introduce context to the analysis of behaviour. To enable supervised learning, a subset of transactions and user actions was marked as either "risky" or "non-risky" based on past audit results and fraud models. These annotated data served as the basis for training and testing classification systems. The remaining data was utilized in unsupervised tasks, like the detection of anomalies, in which Isolation Forests were applied. The feature engineering procedures produced more than 50 variables to input, which accounted behavioral patterns, financial anomalies, and system-access patterns. Data pre-processing steps, which address missing values, encode categorical variables, and scale features, were also applied to numerical features, as well as perform a time consistency check. The final data is consistent in terms of complexity and size, providing a near-real implementation scenario of the risk management based on AI in the ERP environment.

4.2. Model Performance

Table 1: Model Performance

Model	Precision	Recall	F1 Score
Logistic Regression	0.71	0.64	0.67
Random Forest	0.83	0.80	0.81
XGBoost	0.86	0.82	0.84
Isolation Forest	0.60	0.75	0.67

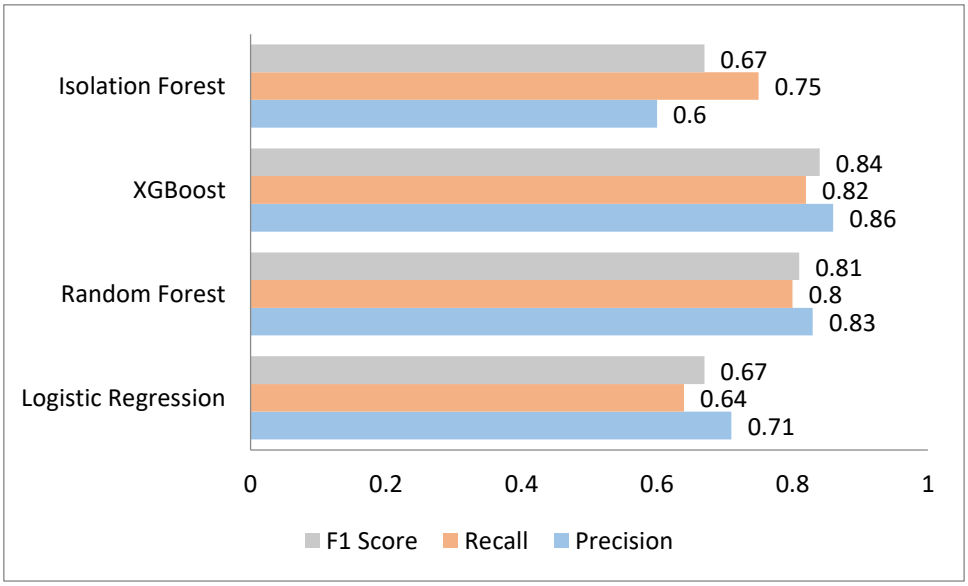

Fig 6: Graph Representing Model Performance

- **Logistic Regression:** In this assessment, the baseline model was Logistic Regression. It achieved an F1 Score of 0.67, with a precision of 0.71 and a recall of 0.64. It is quite easy to conceive and implement, as it is also easy to interpret; however, its linearity limits its use in situations where complex, non-linear patterns need to be observed in the ERP data. It is more appropriate to use it as an entry-level risk flagger, but not in situations where there may be some subtle fraud or behavior anomaly.
- **Random Forest:** When compared to the baseline, the Random Forest classifier showed a marginal improvement, with a precision of 0.83, a recall of 0.80, and an F1 Score of 0.81. It can model feature interactions more effectively due to its ensemble of decision trees. This enabled it to be ideal for tracking various risk indicators in any

procurement transaction, supplier profiles, and employee activity. Lack of notable overfitting and proper generalisation was also demonstrated.

- **XGBoost:** All the other models achieved a precision of 0.86 and a recall of 0.82, with the best F1 Score of 0.84 using XGBoost. Its gradient boosting structure allowed it to correct its previous mistakes more efficiently and perform well even in non-balanced datasets. This was achieved specifically in XGBoost, which proved successful in identifying minor patterns across various ERP modules and served as a solid basis for real-time risk scoring.
- **Isolation Forest:** The Isolation Forest (unsupervised anomaly detection) also achieved a precision of 0.60, a recall of 0.75, but an F1 Score of 0.67. Although it could not be as accurate as supervised models, it was effective in detecting new or unseen anomalies. This was the reason it was very beneficial as a supplement to the supervised models, especially the need to pick up edge cases or changing risk behavior without any labelled training data.

4.3. Case Study: Procurement Risk

The application of the risk engine to procurement data has yielded useful findings regarding vulnerabilities in suppliers within the ERP system. A further examination of this led to the realisation that 3.2 per cent of the suppliers had carried about 80 per cent of the high-risk transactions, a fact that is quite similar to the 80-20 principle, also known as the Pareto Principle. The principle here is that only a few causes can have a disproportionate effect, and in this case, a small number of suppliers cause the most risk exposure. The reason is that these high-risk transactions were identified using aggregated risk scores created by machine learning models that consider, among other factors, transaction values that are out of the ordinary, irregular payment frequencies, inconsistent approval rates, and anomalies in supplier master data. A more detailed examination of these suppliers revealed shared risk signs. Several were unreliable in terms of banking data, had low performance scores, had recently updated their profile data, or had a record of delayed deliveries and disputes. There was also duplication of suppliers, as the same supplier would have more than one ID with minuscule differences in the company name or tax ID, potentially leading to fraud. When matched against employee behaviour records, a similar trend also emerged, indicating that some users were linked to multiple engagements with these high-risk suppliers, which is a red flag for the possibility of collusion or policy violations. The case study demonstrates the practical value of an AI-based risk score ranking in highlighting areas of elevated concern within large and complex procurement systems. Certain patterns may be missed in traditional approaches to auditing because of the vastness of the data and the slightness of the out-of-place variables. The system, however, has the advantage of automating risk identification and ranking of suppliers by multi-dimensional attributes so that organizations can investigate, restrict control on problematic suppliers, and reduce procurement fraud better. Additionally, it does not encourage periodic reviews; instead, it allows for continuous monitoring that is data-driven and more proactive in managing risks.

4.4. Integration with Oracle Fusion ERP

To translate the machine learning models and make the data actionable in the day-to-day activities of the business, the risk scoring system was naturally incorporated into the Oracle Fusion ERP system, utilising both REST APIs and Oracle Integration Cloud (OIC). By doing so, this integration enables real-time interaction between the AI-enabled risk engine and the native ERP modules, particularly in procurement and financial processes. The risk scores produced by the models are then relayed to the ERP environment, where they are used during transaction processing and in decision-making by users. With REST APIs, the system posts risk scores, flags, and model explanations of each transaction or supplier directly into the Oracle Fusion. The workflow rules engine in the ERP, in turn, consumes these data points. To explain further, when a transaction exceeds a set risk limit, the system automatically initiates one of the following processes: sending an alert message to the compliance officer, requiring two approvals, or temporarily blocking the transaction.

This will ensure that activities considered risky are not handled in silence, but rather that oversight is exercised prior to the transaction being carried out. Oracle Integration Cloud (OIC) is a crucial component for end-to-end data movement between the AI engine and ERP modules. It facilitates workflow automation, error response, authentication, and data transformation without interfering with the current system architecture. Integration used to be modular and scalable, allowing it to be expanded later by the addition of new models, risk categories, or connections to other ERP modules, such as Accounts Payable or Human Capital Management. On the whole, such a close integration of AI analytics with operational systems allows for making informed decisions in real-time. It enables Oracle Fusion ERP to become a proactive risk management and transactional system, allowing for quick responses to threats and integrating compliance into core processes.

5. Conclusion and Future Work

This paper introduces a machine learning risk scoring system specifically designed to work with Oracle Fusion ERP, in response to increased requests for intelligent, scalable, and real-time risk management in an enterprise. With the use of structured transactional data, supplier profiles, and user behavior histories, the proposed system uses supervised and unsupervised ML models comparison, including Logistic Regression, Random Forest, XGBoost, and Isolation Forest, to find procurement anomalies, financial frauds, and possible policy-breaking actions. The system demonstrated considerable advancements in the accuracy and responsiveness of traditional rule-based applications, enabling it to detect high-risk activities and prevent them from developing further. Additionally, the risk engine was integrated with Oracle Integration Cloud (OIC) and REST APIs to enhance current workflows, providing risk-based proactive interventions such as automated alerts, dual

signatures, and transaction blocking. This closely integrated AI with working ERP systems, changing the ERP platform from a passive transaction tool to a dynamic risk management solution.

Nevertheless, various challenges deemed important emerged during the implementation. One issue is data security and compliance, particularly in dealing with sensitive financial and employee data. Leaders should ensure that AI models operate within established legal limits, such as the GDPR or SOX. Second, the system may not be as responsive online, as there may be limitations to immediate data processing, including scoring latency and latency integration. Finally, the management of change appeared as a non-technical issue, as stakeholders required training and acceptance of AI-generated risk scores to focus their workflow on them.

Looking to the future, there are many bright directions for future work. The use of Natural Language Processing (NLP) may provide an opportunity to analyse unstructured forms of data, such as descriptions of invoices, clauses of contracts, or notes in procurement, which often contain critical risk indicators. It is possible that federated learning would grant departments or subsidiaries the ability to develop decentralized models that can learn collectively without the exchange of raw data, keeping privacy intact whilst enhancing precision. Also, it will be necessary to implement Explainable AI (XAI) modules to improve transparency and facilitate the work of audit and compliance teams in the quest to determine the basis of the risk scores. These developments will aid in the construction of trust, compliance with the regulation, and the expansion of system capabilities to more enterprise applications, transforming it into the foundation of intelligent and compliant operation of ERP.

References

[1] Bejar, I. I. (2017). Threats to the score's meaning in automated scoring. Validation of score meaning for the next generation of assessments, 75-84.
[2] Williamson, D. M., Bejar, I. I., & Sax, A. (2004). Automated tools for subject matter expert evaluation of automated scoring. Applied Measurement in Education, 17(4), 323-357.
[3] Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Wash. L. Rev., 89, 1.
[4] Parimi, S. S. (2019). Automated Risk Assessment in SAP Financial Modules through Machine Learning. Available at SSRN 4934897.
[5] Rondy Ng et al. (2019) – Oracle extends AI within ERP Cloud and EPM Cloud, including expense reporting assistant, project management digital assistant, advanced financial controls, and supply chain management enhancements.
[6] Aloini, D., Dulmin, R., & Mininno, V. (2012). Risk assessment in ERP projects. information systems, 37(3), 183-199.
[7] Zeng, Y., & Skibniewski, M. J. (2013). Risk Assessment for Enterprise Resource Planning (ERP) System Implementations: A Fault Tree Analysis Approach. Enterprise Information Systems, 7(3), 332-353.
[8] Iskanius, P. (2009). Risk Management in ERP Project in the Context of SMEs. Engineering Letters, 17(4).
[9] Dey, P. K., Clegg, B., & Cheffi, W. (2013). Risk management in enterprise resource planning implementation: a new risk assessment framework. Production Planning & Control, 24(1), 1-14.
[10] Al-Ghofaili, A. A., & Al-Mashari, M. A. (2014, August). ERP system adoption: traditional ERP systems vs. cloud-based ERP systems. In the Fourth edition of the International Conference on the Innovative Computing Technology (INTECH 2014) (pp. 135-139). IEEE.
[11] Boppana, S. B., Moore, C. S., Bodepudi, V., Jha, K. M., Maka, S. R., & Sadaram, G. (2021). AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises.
[12] Zhang, H. (2022). A deep learning model for an ERP enterprise financial management system. Advances in Multimedia, 2022(1), 5783139.
[13] Williamson, D. M., Xi, X., & Breyer, F. J. (2012). A framework for evaluation and use of automated scoring. Educational measurement: issues and practice, 31(1), 2-13.
[14] Poba-Nzaou, P., & Raymond, L. (2011). Managing ERP system risk in SMEs: A multiple case study. Journal of Information Technology, 26(3), 170-192.
[15] Arvidsson, J., & Kojic, D. (2017). Critical Success Factors in ERP Implementation: The Perspective of the Procurement System User.
[16] Oracle updates ERP and EPM with machine learning, finance reporting, AI risk management, and unified projects. ItBrief, 2021. online. https://itbrief.co.nz/story/oracle-updates-erp-and-epm-with-machine-learning-finance-reporting-ai-risk-management-unified-projects
[17] Parisa Golbayani, Ionuț Florescu, Rupak Chatterjee (2020) – A comparative study of forecasting Corporate Credit Ratings using Neural Networks, Support Vector Machines, and Decision Trees.
[18] Gonugunta, K. C. (2018). Apply Machine Learning Oracle Analytics–Combined. The Computertech, 37-44.
[19] Linwei Hu, Jie Chen, Joel Vaughan, Hanyu Yang, Kelly Wang, Agus Sudjianto, Vijayan N. Nair (2020) – Supervised Machine Learning Techniques: An Overview with Applications to Banking.
[20] Rusum, G. P., Pappula, K. K., & Anasuri, S. (2020). Constraint Solving at Scale: Optimizing Performance in Complex Parametric Assemblies. *International Journal of Emerging Trends in Computer Science and Information Technology*, *1*(2), 47-55. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I2P106

[21] Pappula, K. K., & Anasuri, S. (2020). A Domain-Specific Language for Automating Feature-Based Part Creation in Parametric CAD. International Journal of Emerging Research in Engineering and Technology, 1(3), 35-44. https://doi.org/10.63282/3050-922X.IJERET-V1I3P105

[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., Anasuri, S., & Rusum, G. P. (2021). Building Observability into Full-Stack Systems: Metrics That Matter. *International Journal of Emerging Research in Engineering and Technology*, *2*(4), 48-58. https://doi.org/10.63282/3050-922X.IJERET-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. (2021). Data Privacy & Encryption Practices in Cloud-Based Guidewire Deployments. *International Journal of AI, BigData, Computational and Management Studies*, *2*(3), 64-73. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V2I3P108

[27] Rusum, G. P. (2022). WebAssembly across Platforms: Running Native Apps in the Browser, Cloud, and Edge. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(1), 107-115. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I1P112

[28] Pappula, K. K. (2022). Architectural Evolution: Transitioning from Monoliths to Service-Oriented Systems. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 53-62. https://doi.org/10.63282/3050-922X.IJERET-V3I4P107

[29] Jangam, S. K. (2022). Self-Healing Autonomous Software Code Development. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 42-52. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P105

[30] Anasuri, S. (2022). Adversarial Attacks and Defenses in Deep Neural Networks. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 77-85. https://doi.org/10.63282/xs971f03

[31] Rahul, N. (2022). Automating Claims, Policy, and Billing with AI in Guidewire: Streamlining Insurance Operations. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 75-83. https://doi.org/10.63282/3050-922X.IJERET-V3I4P109

[32] Enjam, G. R. (2022). Energy-Efficient Load Balancing in Distributed Insurance Systems Using AI-Optimized Switching Techniques. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 68-76. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I4P108

[33] Rusum, G. P., & Anasuri, S. (2023). Composable Enterprise Architecture: A New Paradigm for Modular Software Design. *International Journal of Emerging Research in Engineering and Technology*, *4*(1), 99-111. https://doi.org/10.63282/3050-922X.IJERET-V4I1P111

[34] Pappula, K. K. (2023). Reinforcement Learning for Intelligent Batching in Production Pipelines. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(4), 76-86. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I4P109

[35] Jangam, S. K., & Pedda Muntala, P. S. R. (2023). Challenges and Solutions for Managing Errors in Distributed Batch Processing Systems and Data Pipelines. *International Journal of Emerging Research in Engineering and Technology*, *4*(4), 65-79. https://doi.org/10.63282/3050-922X.IJERET-V4I4P107

[36] Anasuri, S. (2023). Secure Software Supply Chains in Open-Source Ecosystems. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 62-74. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P108

[37] Rahul, N. (2023). Transforming Underwriting with AI: Evolving Risk Assessment and Policy Pricing in P&C Insurance. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 92-101. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P110

[38] Enjam, G. R. (2023). Modernizing Legacy Insurance Systems with Microservices on Guidewire Cloud Platform. *International Journal of Emerging Research in Engineering and Technology*, *4*(4), 90-100. https://doi.org/10.63282/3050-922X.IJERET-V4I4P109

[39] Pappula, K. K. (2020). Browser-Based Parametric Modeling: Bridging Web Technologies with CAD Kernels. *International Journal of Emerging Trends in Computer Science and Information Technology*, *1*(3), 56-67. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I3P107

[40] Rahul, N. (2020). Vehicle and Property Loss Assessment with AI: Automating Damage Estimations in Claims. *International Journal of Emerging Research in Engineering and Technology*, *1*(4), 38-46. https://doi.org/10.63282/3050-922X.IJERET-V1I4P105

[41] Enjam, G. R., & Chandragowda, S. C. (2020). Role-Based Access and Encryption in Multi-Tenant Insurance Architectures. *International Journal of Emerging Trends in Computer Science and Information Technology*, *1*(4), 58-66. https://doi.org/10.63282/3050-9246.IJETCSIT-V1I4P107

[42] 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

[43] Rahul, N. (2021). AI-Enhanced API Integrations: Advancing Guidewire Ecosystems with Real-Time Data. *International Journal of Emerging Research in Engineering and Technology*, *2*(1), 57-66. https://doi.org/10.63282/3050-922X.IJERET-V2I1P107

[44] Enjam, G. R., Chandragowda, S. C., & Tekale, K. M. (2021). Loss Ratio Optimization using Data-Driven Portfolio Segmentation. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(1), 54-62. https://doi.org/10.63282/3050-9262.IJAIDSML-V2I1P107

[45] Rusum, G. P., & Pappula, K. K. (2022). Federated Learning in Practice: Building Collaborative Models While Preserving Privacy. *International Journal of Emerging Research in Engineering and Technology*, *3*(2), 79-88. https://doi.org/10.63282/3050-922X.IJERET-V3I2P109

[46] Pappula, K. K. (2022). Modular Monoliths in Practice: A Middle Ground for Growing Product Teams. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 53-63. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P106

[47] Jangam, S. K., & Pedda Muntala, P. S. R. (2022). Role of Artificial Intelligence and Machine Learning in IoT Device Security. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 77-86. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P108

[48] Anasuri, S. (2022). Next-Gen DNS and Security Challenges in IoT Ecosystems. *International Journal of Emerging Research in Engineering and Technology*, *3*(2), 89-98. https://doi.org/10.63282/3050-922X.IJERET-V3I2P110

[49] Rahul, N. (2022). Enhancing Claims Processing with AI: Boosting Operational Efficiency in P&C Insurance. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), 77-86. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P108

[50] Enjam, G. R., & Tekale, K. M. (2022). Predictive Analytics for Claims Lifecycle Optimization in Cloud-Native Platforms. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 95-104. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I1P110

[51] Rusum, G. P., & Pappula, K. K. (2023). Low-Code and No-Code Evolution: Empowering Domain Experts with Declarative AI Interfaces. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(2), 105-112. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I2P112

[52] Pappula, K. K., & Rusum, G. P. (2023). Multi-Modal AI for Structured Data Extraction from Documents. *International Journal of Emerging Research in Engineering and Technology*, *4*(3), 75-86. https://doi.org/10.63282/3050-922X.IJERET-V4I3P109

[53] Jangam, S. K., Karri, N., & Pedda Muntala, P. S. R. (2023). Develop and Adapt a Salesforce User Experience Design Strategy that Aligns with Business Objectives. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 53-61. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P107

[54] Anasuri, S. (2023). Confidential Computing Using Trusted Execution Environments. *International Journal of AI, BigData, Computational and Management Studies*, *4*(2), 97-110. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I2P111

[55] Rahul, N. (2023). Personalizing Policies with AI: Improving Customer Experience and Risk Assessment. International Journal of Emerging Trends in Computer Science and Information Technology, 4(1), 85-94. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P110

[56] Enjam, G. R. (2023). AI Governance in Regulated Cloud-Native Insurance Platforms. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 102-111. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P111

[57] 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

[58] Enjam, G. R., & Tekale, K. M. (2020). Transitioning from Monolith to Microservices in Policy Administration. *International Journal of Emerging Research in Engineering and Technology*, *1*(3), 45-52. https://doi.org/10.63282/3050-922X.IJERETV1I3P106

[59] Pappula, K. K., & Anasuri, S. (2021). API Composition at Scale: GraphQL Federation vs. REST Aggregation. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(2), 54-64. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I2P107

[60] Rusum, G. P. (2022). Security-as-Code: Embedding Policy-Driven Security in CI/CD Workflows. *International Journal of AI, BigData, Computational and Management Studies*, *3*(2), 81-88. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I2P108

[61] 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

[62] Pappula, K. K. (2022). Containerized Zero-Downtime Deployments in Full-Stack Systems. International Journal of AI, BigData, Computational and Management Studies, 3(4), 60-69. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I4P107

[63] Jangam, S. K., Karri, N., & Pedda Muntala, P. S. R. (2022). Advanced API Security Techniques and Service Management. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 63-74. https://doi.org/10.63282/3050-922X.IJERET-V3I4P108

[64] Anasuri, S. (2022). Zero-Trust Architectures for Multi-Cloud Environments. International Journal of Emerging Trends in Computer Science and Information Technology, 3(4), 64-76. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I4P107

[65] Rahul, N. (2022). Optimizing Rating Engines through AI and Machine Learning: Revolutionizing Pricing Precision. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(3), 93-101. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I3P110

[66] Enjam, G. R. (2022). Secure Data Masking Strategies for Cloud-Native Insurance Systems. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(2), 87-94. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I2P109

[67] Rusum, G. P. (2023). Large Language Models in IDEs: Context-Aware Coding, Refactoring, and Documentation. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(2), 101-110. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I2P110

[68] Pappula, K. K. (2023). Edge-Deployed Computer Vision for Real-Time Defect Detection. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 72-81. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P108

[69] Jangam, S. K. (2023). Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 82-91. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I3P109

[70] Anasuri, S., & Pappula, K. K. (2023). Green HPC: Carbon-Aware Scheduling in Cloud Data Centers. *International Journal of Emerging Research in Engineering and Technology*, *4*(2), 106-114. https://doi.org/10.63282/3050-922X.IJERET-V4I2P111

[71] Enjam, G. R. (2023). Optimizing PostgreSQL for High-Volume Insurance Transactions & Secure Backup and Restore Strategies for Databases. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(1), 104-111. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I1P112

[72] Pappula, K. K., & Rusum, G. P. (2021). Designing Developer-Centric Internal APIs for Rapid Full-Stack Development. *International Journal of AI, BigData, Computational and Management Studies*, *2*(4), 80-88. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V2I4P108

[73] Rusum, G. P., & Pappula, kiran K. . (2022). Event-Driven Architecture Patterns for Real-Time, Reactive Systems. *International Journal of Emerging Research in Engineering and Technology*, *3*(3), 108-116. https://doi.org/10.63282/3050-922X.IJERET-V3I3P111

[74] Jangam, S. K., & Karri, N. (2022). Potential of AI and ML to Enhance Error Detection, Prediction, and Automated Remediation in Batch Processing. *International Journal of AI, BigData, Computational and Management Studies*, *3*(4), 70-81. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I4P108

[75] Anasuri, S. (2022). Formal Verification of Autonomous System Software. *International Journal of Emerging Research in Engineering and Technology*, *3*(1), 95-104. https://doi.org/10.63282/3050-922X.IJERET-V3I1P110

[76] Rusum, G. P., & Anasuri, S. (2023). Synthetic Test Data Generation Using Generative Models. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(4), 96-108. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I4P111

[77] Jangam, S. K., & Karri, N. (2023). Robust Error Handling, Logging, and Monitoring Mechanisms to Effectively Detect and Troubleshoot Integration Issues in MuleSoft and Salesforce Integrations. *International Journal of Emerging Research in Engineering and Technology*, *4*(4), 80-89. https://doi.org/10.63282/3050-922X.IJERET-V4I4P108

[78] Anasuri, S. (2023). Synthetic Identity Detection Using Graph Neural Networks. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 87-96. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I4P110

[79] Enjam, G. R., Tekale, K. M., & Chandragowda, S. C. (2023). Zero-Downtime CI/CD Production Deployments for Insurance SaaS Using Blue/Green Deployments. *International Journal of Emerging Research in Engineering and Technology*, *4*(3), 98-106. https://doi.org/10.63282/3050-922X.IJERET-V4I3P111