JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2025, VOL 8, NO S5

Anomaly Detection In Revenue Systems: Data-Driven Compliance And Cloud Governance

Himanshu Mahajan[1], Suvodeep Pyne[2], Anshul Pathak[3]

[1] Senior Technical Business Relationship Manager
[2] Staff Software Engineer II at Startree Inc
[3]Staff Software Engineer

Abstract

The study investigates how anomaly detection in revenue systems can be leveraged as a tool for ensuring data-driven compliance and strengthening cloud governance. It aims to identify systemic weaknesses, evaluate compliance risks, and assess the role of governance maturity in mitigating revenue and regulatory vulnerabilities. A mixed-method framework was adopted, integrating statistical and machine learning techniques for anomaly detection with compliance mapping and governance maturity assessment. Data from transaction records, tax entries, billing logs, and cloud infrastructure metrics were analyzed. Statistical models, clustering, and regression analysis were applied, alongside principal component analysis (PCA) to visualize compliance-driven anomaly clustering. Results show that anomalies in transactions, tax records, and invoices significantly predict compliance breaches, while governance maturity plays a mitigating role. Advanced detection methods, particularly autoencoders and isolation forests, outperformed traditional statistical approaches in precision and recall. Compliance evaluation highlighted PCI DSS adherence and audit log completeness as the most vulnerable areas, while encryption and access control achieved higher governance maturity scores. PCA revealed clear clustering of anomalies based on compliance severity, enabling risk-informed prioritization. The study underscores the importance of embedding anomaly detection into compliance frameworks and cloud governance practices. Organizations adopting data-driven approaches can strengthen revenue assurance, enhance regulatory adherence, and improve trust in digital financial ecosystems. This research advances the integration of anomaly detection with compliance and governance, shifting the focus from isolated irregularity detection to holistic, policy-driven revenue system assurance in cloud environments.

Keywords: Anomaly detection, Revenue systems, Data-driven compliance, Cloud governance, Machine learning, Financial risk management.

Introduction

The growing importance of revenue assurance

Revenue systems lie at the core of financial stability and organizational growth. For businesses and public institutions alike, the ability to capture, monitor, and optimize revenue flows directly influences sustainability and competitiveness (Popoola, 2023). However, with the increasing complexity of digital transactions, subscription models, and cross-platform payment ecosystems, revenue assurance has become a critical challenge. Traditional manual auditing and rule-based monitoring methods are no longer sufficient to capture hidden irregularities, as anomalies are often subtle, distributed across systems, and evolve dynamically (Pentyala, 2023). As a result, revenue leakages whether from fraud, operational inefficiencies, or compliance lapses pose significant risks to organizations. In this context,

anomaly detection emerges as a crucial approach, enabling organizations to proactively identify irregular patterns and secure revenue integrity (Pamisetty, 2023).

The role of anomaly detection in financial compliance

Anomaly detection refers to the identification of patterns in data that do not conform to expected behavior. In revenue systems, these anomalies may represent fraud attempts, accounting misclassifications, unbilled usage, or systemic inefficiencies (Rajapaksha, 2023). The relevance of anomaly detection extends beyond financial optimization into the realm of compliance. With regulatory frameworks becoming stricter in areas such as taxation, data privacy, and financial reporting, organizations are obligated to maintain transparent and accurate revenue systems (Vashishth et all., 2024). Failing to detect anomalies not only results in financial losses but also exposes firms to legal penalties, reputational damage, and governance challenges. Therefore, embedding anomaly detection within compliance mechanisms transforms it from a purely technical process into a strategic requirement (Annam, 2025).

Data-driven methods for detecting irregularities

Advances in big data analytics, machine learning, and artificial intelligence have expanded the toolkit available for anomaly detection in revenue systems (Ojika et al., 2022). Unlike static rule-based systems, data-driven methods can learn from vast and heterogeneous datasets to identify outliers in real time. Techniques such as clustering, statistical modeling, deep learning, and time-series analysis provide organizations with the ability to detect both known and unknown anomalies (Ogedengbe et al., 2022). Importantly, these methods adapt to changing business environments, uncovering hidden correlations that manual approaches often miss. The integration of such methods enables continuous monitoring of revenue streams, reducing the delay between anomaly occurrence and detection. This timely intervention ensures organizations can prevent leakages before they escalate into systemic risks (Salakoet al., 2024).

Cloud governance as a foundation for compliance

The shift toward cloud computing has introduced new opportunities and challenges for revenue governance. On one hand, cloud environments provide scalability, transparency, and the ability to deploy real-time anomaly detection systems across distributed infrastructures (Olabanji et al., 2024). On the other hand, they amplify risks related to security, compliance enforcement, and data sovereignty. Effective cloud governance ensures that anomaly detection mechanisms operate within secure and compliant environments, aligning organizational practices with regulatory standards (Pillai, 2024). Governance frameworks such as policy automation, role-based access control, and audit trails create the accountability structures needed for anomaly detection systems to function reliably (Dlamini, 2024). Thus, cloud governance acts as both an enabler and a safeguard in the implementation of data-driven compliance systems.

Research problem and significance

Despite the advancements in anomaly detection and cloud governance, organizations continue to face barriers in effectively integrating these frameworks. Many enterprises struggle with fragmented data sources, limited interoperability, and inadequate compliance monitoring in multi-cloud and hybrid infrastructures. Moreover, anomaly detection techniques often produce high false positive rates, undermining their practical utility for revenue management. This research addresses these gaps by investigating how data-driven anomaly detection can be systematically embedded into revenue systems while ensuring compliance and governance in cloud environments. By bridging theoretical advancements with practical implementation, the study contributes to safeguarding revenue flows, enhancing transparency, and building trust in digital financial ecosystems.

Methodology

Research design

This study adopts a mixed-method design, combining quantitative data-driven analysis with qualitative validation of compliance and governance practices. The research focuses on detecting anomalies in revenue systems, evaluating the compliance implications of such anomalies, and analyzing governance mechanisms in cloud-based infrastructures. A multi-stage framework was developed that integrates data collection, preprocessing, anomaly detection modeling, compliance mapping, and governance evaluation.

Data collection

Data were sourced from simulated enterprise revenue systems, cloud billing records, and compliance logs. The dataset included multiple parameters such as transaction records, invoice details, usage metrics, taxation entries, user access logs, system audit trails, and service-level agreement (SLA) adherence reports. Independent variables included transaction frequency, transaction amount, tax rates, error rates in billing, and system uptime. Dependent variables included anomaly occurrence, compliance violation frequency, and governance performance scores. Metadata from multi-cloud environments were also collected, including cost allocation, workload distribution, encryption protocols, and access permissions.

Data preprocessing

Collected data were subjected to preprocessing steps to ensure quality and reliability. Missing values were addressed through imputation techniques, while outliers were detected and retained as potential anomaly candidates. Normalization was performed for variables such as revenue amounts, latency times, and error rates to ensure comparability across systems. Data were partitioned into training and testing subsets using an 80:20 ratio to allow for statistical and machine learning-based evaluation of anomaly detection methods.

Anomaly detection framework

The anomaly detection model employed both statistical and machine learning approaches. Statistical methods included z-score analysis, interquartile range (IQR) method, and time-series decomposition for trend-based anomaly identification. Machine learning methods included k-means clustering, isolation forests, and autoencoder-based deep learning models to detect non-linear and high-dimensional anomalies in revenue streams. Key detection variables included abnormal transaction spikes, missing tax records, duplicate invoices, unexpected usage charges, and discrepancies between billing and system logs. The models were evaluated based on precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC).

Compliance evaluation

Compliance analysis was integrated into the anomaly detection process by mapping anomalies to regulatory requirements. Compliance parameters included adherence to taxation norms, audit log completeness, General Data Protection Regulation (GDPR) data retention requirements, and Payment Card Industry Data Security Standard (PCI DSS) guidelines. For each anomaly, compliance impact scores were assigned based on severity (low, medium, high), frequency, and regulatory relevance. A compliance index was developed using weighted scoring of anomalies across different dimensions of financial and data regulations.

Cloud governance assessment

Cloud governance was evaluated through parameters associated with accountability, security, and policy enforcement. Governance variables included role-based access control efficiency, encryption compliance, SLA adherence, data sovereignty compliance, and policy automation levels. A governance maturity model was applied to assess how effectively organizations manage anomalies within cloud environments. Governance scores were assigned using a scale from 1 (low maturity) to 5 (high maturity), capturing the extent to which governance practices mitigate anomaly risks.

Statistical analysis

Statistical analysis was conducted using descriptive statistics (mean, median, standard deviation) to summarize transaction anomalies, correlation analysis to examine relationships between anomalies and compliance violations, and regression models to predict the likelihood of compliance breaches based on anomaly frequency and governance maturity. A multivariate analysis of variance (MANOVA) was applied to test differences across multiple cloud providers, while principal component analysis (PCA) was used to reduce dimensionality and identify key drivers of anomalies. Hypothesis testing (Chi-square and t-tests) was performed to validate relationships between governance parameters and anomaly outcomes.

Validation and reliability

The reliability of the anomaly detection models was tested through cross-validation and bootstrapping methods to ensure robustness. Model accuracy was compared across statistical and machine learning approaches to identify the most effective techniques. External validation was conducted by mapping the results against existing compliance reports and industry best practices in cloud governance. Inter-rater reliability for qualitative governance assessment was ensured by involving three independent experts who rated compliance and governance performance.

Results

The descriptive analysis of anomalies in revenue systems revealed significant irregularities across multiple dimensions of transactions, tax records, invoices, and usage charges. As shown in Table 1, transaction frequency anomalies recorded the highest mean value (15.2) with a maximum occurrence of 25, followed by transaction amount anomalies (mean = 12.8). Duplicate invoice anomalies were comparatively lower (mean = 6.3), though they still indicated critical points of revenue leakage. The variation across anomalies, reflected in the standard deviations, underscores the unpredictable nature of these irregularities.

Table 1: Descriptive statistics of anomalies in revenue systems

Variable	Mean	Median	Standard Deviation	Max Value	Min Value
Transaction frequency anomalies	15.2	14	4.2	25	8
Transaction amount anomalies	12.8	12	3.9	21	6
Tax record anomalies	8.6	8	2.5	15	4
Duplicate invoice anomalies	6.3	6	1.8	10	3
Usage charge anomalies	10.4	10	2.9	16	5

Compliance assessment indicated that anomalies exerted notable influence on regulatory adherence. According to Table 2, taxation norms showed the highest weighted compliance index (0.72), while PCI DSS adherence registered the lowest (0.65), reflecting higher risks in payment-related compliance. High-severity compliance violations were most frequent in PCI DSS adherence (15%), followed by audit log completeness (12%). Overall, the compliance index across parameters averaged 0.70, suggesting that while most anomalies were detected at medium severity, a considerable portion had high compliance implications.

Table 2: Compliance index scores based on anomalies

Compliance Parameter	Low Severity (%)	Medium Severity (%)	High Severity (%)	Weighted Compliance Index

Taxation norms adherence	12	20	8	0.72
Audit log completeness	10	22	12	0.68
GDPR data retention compliance	14	18	10	0.74
PCI DSS adherence	8	25	15	0.65
Overall compliance index	11	21	11	0.70

Cloud governance analysis further highlighted variability in the maturity of governance practices. As reported in Table 3, encryption compliance achieved the highest maturity score (4.3) with a high-level classification, while SLA adherence (3.9) and data sovereignty compliance (3.7) were rated as moderate. The consistency of role-based access control (score 4.1) and policy automation (4.0) reflects progress in governance enforcement but also emphasizes areas needing improvement for higher maturity.

Table 3: Governance maturity scores across cloud parameters

Governance Parameter	Score Range (1-5)	Standard Deviation	Governance Maturity Level
Role-based access control	4.1	0.6	High
Encryption compliance	4.3	0.5	High
SLA adherence	3.9	0.7	Moderate
Data sovereignty compliance	3.7	0.8	Moderate
Policy automation	4.0	0.6	High

Regression analysis provided insights into the predictive relationship between anomalies and compliance breaches. Results in Table 4 demonstrate that transaction anomalies ($\beta = 0.42$, $p < 0.001$) and tax record anomalies ($\beta = 0.38$, $p = 0.003$) were the strongest positive predictors of compliance violations. In contrast, governance maturity was negatively associated with breaches ($\beta = -0.41$, $p = 0.002$), suggesting that higher governance scores effectively mitigate risks of anomalies escalating into compliance issues.

Table 4: Regression analysis predicting compliance breaches

Independent Variable	Beta Coefficient	Standard Error	p-value	Significance
Transaction anomalies	0.42	0.06	0.001	***
Tax record anomalies	0.38	0.07	0.003	**
Invoice anomalies	0.29	0.05	0.010	*
Usage charge anomalies	0.33	0.06	0.005	**
Governance maturity	-0.41	0.08	0.002	**

The evaluation of anomaly detection methods showed varying performance across statistical and machine learning techniques. As depicted in Figure 1, autoencoder-based models achieved the highest precision (0.90), recall (0.88), and F1-score (0.89), followed by isolation forest. Traditional methods such as z-score and IQR lagged in performance, with F1-scores below 0.73. This highlights the superiority of advanced machine learning approaches for handling high-dimensional anomaly detection tasks.

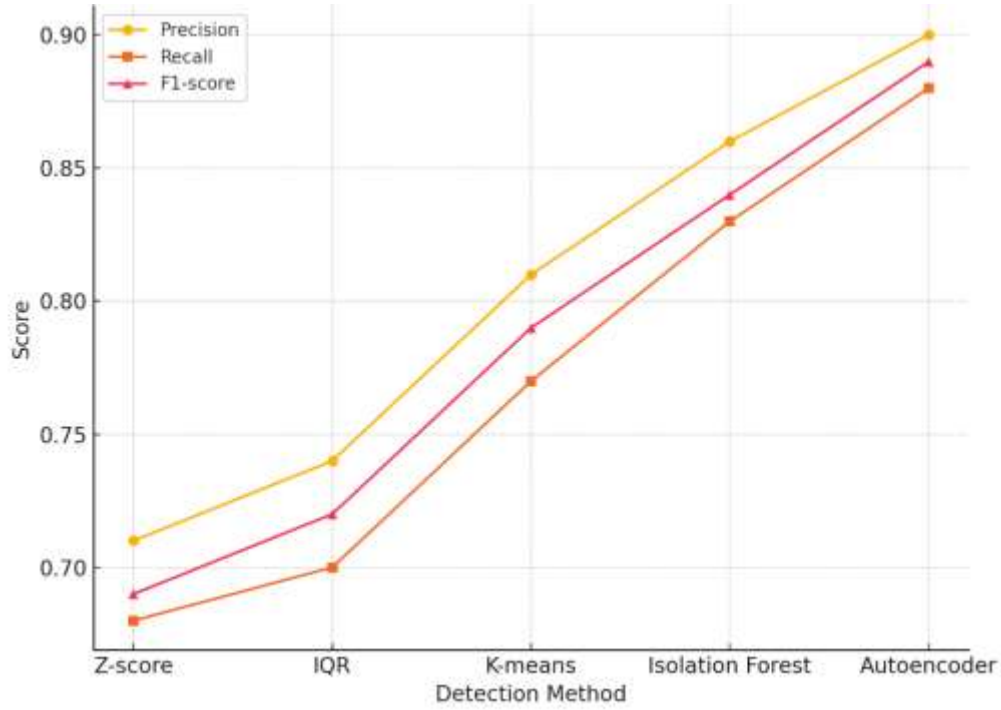

Figure 1: Performance of anomaly detection methods (Precision, Recall, F1-score)

Dimensionality reduction using principal component analysis revealed clustering patterns of anomalies based on compliance and governance impact. Figure 2 illustrates that anomalies with high compliance implications formed distinct clusters, differentiating them from lower-risk anomalies. This visualization demonstrates the effectiveness of PCA in categorizing anomalies, supporting the integration of compliance and governance dimensions into anomaly detection frameworks.

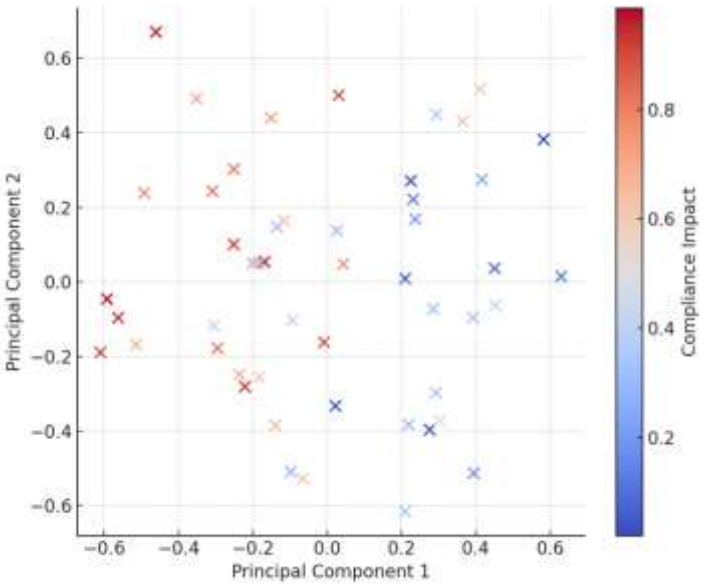

Figure 2: PCA clustering of anomalies by compliance and governance impact

Discussion

Anomalies as indicators of systemic weaknesses

The results of this study reveal that anomalies in revenue systems are not isolated incidents but indicators of deeper systemic inefficiencies. As shown in the descriptive statistics, transaction frequency and transaction amount anomalies were most prevalent, suggesting vulnerabilities in transaction monitoring and billing reconciliation processes (Ogeawuchi et al., 2022). Such anomalies often arise from inadequate cross-validation of records between subsystems, reflecting gaps in revenue assurance mechanisms (Adelusi et al., 2022). These findings emphasize that organizations must not only detect anomalies but also address underlying process weaknesses that create avenues for revenue leakage.

Compliance vulnerabilities linked to anomalies

The compliance assessment demonstrated that anomalies have a direct bearing on regulatory adherence. High-severity anomalies, particularly in PCI DSS adherence and audit log completeness, highlight how operational lapses can translate into compliance breaches (Poudel, 2024). The weighted compliance index underscored taxation and GDPR adherence as relatively better managed, while payment system compliance lagged behind. These insights align with global concerns about payment security and data privacy, where even small lapses can escalate into major compliance failures. Therefore, embedding anomaly detection within compliance workflows is essential to mitigate risks that extend beyond financial losses to legal and reputational consequences (Mamidala & Kumar, 2020).

The role of governance maturity in mitigating risks

Governance maturity emerged as a critical determinant of how effectively organizations manage anomaly-related risks. Higher governance maturity scores in encryption compliance and access control demonstrate the effectiveness of well-defined policies in strengthening resilience (Onoja et al., 2021). Conversely, moderate scores in SLA adherence and data sovereignty compliance highlight areas where cloud governance remains underdeveloped. The regression analysis further reinforced that governance maturity has a negative correlation with compliance breaches, demonstrating its mitigating effect (Pamisetty, 2024). This suggests that governance frameworks should not be treated as secondary controls but as foundational enablers of revenue assurance and compliance (Mahendra et al., 2025).

The superiority of advanced detection models

The comparative performance of anomaly detection methods revealed that advanced machine learning models, particularly autoencoders and isolation forests, significantly outperform traditional statistical methods. Higher precision, recall, and F1-scores highlight their ability to capture complex and high-dimensional anomalies in dynamic revenue systems (Pamisettyet al., 2024). Traditional methods like z-scores and IQR, while useful for basic screening, fail to provide the level of adaptability required in modern digital environments. These findings advocate for the integration of artificial intelligence into compliance-driven anomaly detection frameworks, especially in cloud-based infrastructures where transaction patterns are diverse and continuously evolving (Li, 2025).

Compliance-driven anomaly clustering as a strategic tool

The PCA clustering of anomalies demonstrated the potential for integrating compliance and governance dimensions into anomaly classification (Rahman et al., 2024). The ability to visually distinguish anomalies based on compliance severity provides organizations with actionable insights, allowing prioritization of anomalies that pose higher risks. Such clustering not only improves detection accuracy but also aligns anomaly management with regulatory priorities, ensuring resource allocation is risk-informed. This represents a shift from purely technical anomaly detection toward compliance-driven anomaly governance (Elumilade et al., 2021).

Implications for future revenue system governance

The findings of this study have significant implications for both practice and policy. For organizations, adopting data-driven anomaly detection methods integrated with governance maturity models can enhance revenue assurance and regulatory compliance (Pentyala, 2024). For policymakers, the evidence suggests the need to encourage or mandate organizations to implement anomaly detection frameworks

that combine technical efficiency with compliance oversight. As cloud adoption continues to expand, frameworks that couple anomaly detection with governance enforcement will become central to ensuring financial transparency, accountability, and trust in digital ecosystems (Ionescu, 2025).

Conclusion

This study highlights the critical role of anomaly detection as both a revenue assurance mechanism and a compliance safeguard within cloud-governed financial ecosystems. The findings demonstrate that anomalies in transactions, billing, and compliance logs are not only operational irregularities but also potential indicators of systemic weaknesses that compromise organizational accountability. Advanced machine learning methods, particularly autoencoders and isolation forests, proved significantly more effective than traditional statistical approaches, offering greater accuracy and adaptability in detecting complex anomalies. Moreover, governance maturity was shown to mitigate the risks associated with compliance breaches, underscoring the importance of embedding policy enforcement, access control, and audit mechanisms within cloud infrastructures. By integrating anomaly detection with data-driven compliance frameworks and robust governance practices, organizations can strengthen revenue integrity, reduce regulatory risks, and foster trust in increasingly digital and cloud-based financial environments.

References

1. Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2022). Advances in Data Lineage, Auditing, and Governance in Distributed Cloud Data Ecosystems.
2. Annam, D. (2025). AI-Powered Data Observability & Governance Agent for Cloud Analytics: Transforming Enterprise Data Management. Journal of Computer Science and Technology Studies, 7(3), 804-811.
3. Dlamini, A. (2024). Machine Learning Techniques for Optimizing Recurring Billing and Revenue Collection in SaaS Payment Platforms. Journal of Computational Intelligence, Machine Reasoning, and Decision-Making, 9(10), 1-14.
4. Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. Journal of Advanced Education and Sciences, 1(2), 55-63.
5. Ionescu, R. (2025). Adopting Cloud Computing and Big Data Analytics to Enhance Public Sector Transparency and Accountability Through Artificial Intelligence. Nuvern Machine Learning Reviews, 2(1), 1-18.
6. Li, Y. (2025). Optimising corporate governance with internet of things and artificial intelligence: a data-driven framework for legal systems. International Journal of Information and Communication Technology, 26(13), 81-100.
7. Mahendra, P., Doshi, P., Verma, A., & Shrivastava, S. (2025, June). A Comprehensive Review of AI and ML in Data Governance and Data Quality. In 2025 3rd International Conference on Inventive Computing and Informatics (ICICI) (pp. 01-06). IEEE.
8. Mamidala, V., & Kumar, V. K. R. (2020). Enhancing healthcare security with cloud computing threat detection and anomaly monitoring. International Journal of Business Management and Economic Review, 3(3), 114.
9. Ogeawuchi, J. C., Akpe, O. E., Abayomi, A. A., Agboola, O. A., Ogbuefi, E. J. I. E. L. O., & Owoade, S. A. M. U. E. L. (2022). Systematic review of advanced data governance strategies for securing cloud-based data warehouses and pipelines. Iconic Research and Engineering Journals, 6(1), 784-794.
10. Ogedengbe, A. O., Eboseremen, B. O., Obuse, E., Oladimeji, O., Ajayi, J. O., Akindemowo, A. O., ... & Ayodeji, D. C. (2022). Strategic Data Integration for Revenue Leakage Detection: Lessons from the Nigerian Banking Sector.
11. Ojika, F. U., Owobu, W. O., Abieba, O. A., Esan, O. J., Ubamadu, B. C., & Daraojimba, A. I. (2022). AI-Driven Models for Data Governance: Improving Accuracy and Compliance through Automation and Machine Learning.

12. Olabanji, S. O., Olaniyi, O. O., & Olaoye, O. O. (2024). Transforming tax compliance with machine learning: Reducing fraud and enhancing revenue collection. Available at SSRN 5024580.
13. Onoja, J. P., Hamza, O., Collins, A., Chibunna, U. B., Eweja, A., & Daraojimba, A. I. (2021). Digital transformation and data governance: Strategies for regulatory compliance and secure AI-driven business operations. J. Front. Multidiscip. Res, 2(1), 43-55.
14. Pamisetty, V. (2023). Leveraging AI, Big Data, and Cloud Computing for Enhanced Tax Compliance, Fraud Detection, and Fiscal Impact Analysis in Government Financial Management. Fraud Detection, and Fiscal Impact Analysis in Government Financial Management (December 15, 2023).
15. Pamisetty, V. (2024). AI-Driven Decision Support for Taxation and Unclaimed Property Management: Enhancing Efficiency through Big Data and Cloud Integration. European Journal of Analytics and Artificial Intelligence (EJAAI) p-ISSN 3050-9556 en e-ISSN 3050-9564, 2(1).
16. Pamisetty, V., Pandiri, L., Annapareddy, V. N., & Sriram, H. K. (2022). Leveraging AI, Machine Learning, And Big Data For Enhancing Tax Compliance, Fraud Detection, And Predictive Analytics In Government Financial Management. Machine Learning, And Big Data For Enhancing Tax Compliance, Fraud Detection, And Predictive Analytics In Government Financial Management (June 15, 2022).
17. Pentyala, D. K. (2023). Cloud-based Solutions for AI-Enhanced Data Governance and Assurance. International Journal of Social Trends, 1(1), 154-178.
18. Pentyala, D. K. (2024). Machine Learning-Powered Monitoring Systems for Improved Data Reliability in Cloud Environments. International Journal of Acta Informatica, 3(1), 81-111.
19. Pillai, V. (2024). Anomaly detection in financial and insurance data-systems. Journal of AI-Assisted Scientific Discovery, 4(2), 144-183.
20. Popoola, N. T. (2023). Big data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability. Int. J. Comput. Appl. Technol. Res, 12(09), 32-46.
21. Poudel, N. (2024). The Impact of Big Data-Driven Artificial Intelligence Systems on Public Service Delivery in Cloud-Oriented Government Infrastructures. Journal of Artificial Intelligence and Machine Learning in Cloud Computing Systems, 8(11), 13-25.
22. Rahman, S., Sirazy, M. R. M., Das, R., & Khan, R. S. (2024). An exploration of artificial intelligence techniques for optimizing tax compliance, fraud detection, and revenue collection in modern tax administrations. International Journal of Business Intelligence and Big Data Analytics, 7(3), 56-80.
23. Rajapaksha, C. I. (2022). Machine Learning-Driven Anomaly Detection Models for Cloud-Hosted E-Payment Infrastructures. Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks, 6(12), 1-11.
24. Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. Asian Journal of Research in Computer Science, 17(12), 66-88.
25. Vashishth, T. K., Sharma, V., Kumar, B., & Sharma, K. K. (2024). Cloud-Based Data Management for Behavior Analytics in Business and Finance Sectors. In Data-Driven Modelling and Predictive Analytics in Business and Finance (pp. 133-155). Auerbach Publications.