International Journal of Advanced Research in Computer Science & Technology (IJARCST)
|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811

An End-to-End Cloud AI Framework for Petabyte-Scale Multi-Tenant Data: Azure DevOps–Integrated Fraud Detection and Risk Analytics

Abdul Hakim Mohamed
Senior Project Manager, Singapore

ABSTRACT: Enterprises operating in multi-tenant cloud environments face increasing challenges in detecting fraud and managing risk across petabyte-scale datasets. Traditional approaches often lack the scalability, automation, and intelligence required to handle dynamic, high-volume data from diverse sources. This paper proposes an **end-to-end Cloud AI framework** that integrates **Azure DevOps** for continuous deployment, monitoring, and management, enabling **real-time fraud detection and risk analytics** across multi-tenant systems.
The framework leverages **artificial intelligence and machine learning techniques** to analyze transactional, behavioral, and contextual data at scale. Its architecture ensures secure tenant isolation, high availability, and efficient processing of massive datasets. By combining AI-driven analytics with cloud-native tools, the system provides predictive risk scoring, anomaly detection, and actionable insights for proactive fraud prevention. Experimental evaluation demonstrates improved detection accuracy, reduced false positives, and enhanced operational efficiency, highlighting the effectiveness of integrating AI with cloud DevOps practices for enterprise-scale fraud and risk management.

KEYWORDS: Cloud AI, Multi-Tenant Data, Petabyte-Scale Analytics, Fraud Detection, Risk Analytics, Azure DevOps, Machine Learning, Enterprise Cloud Systems, Scalable Cloud Framework, Data Security

I. INTRODUCTION

With the rapid proliferation of cloud-native applications and services, enterprises increasingly operate in multi-tenant environments where data from multiple clients, business units, or services are jointly stored and processed. These multi-tenant systems often accumulate vast volumes of data — in transactional systems, user interactions, logs, and behavioral events — quickly reaching petabyte scale. In domains such as financial services, e-commerce, telecommunications, and SaaS platforms, this data often contains critical signals for fraud detection and risk analytics. Timely detection of fraudulent activities and accurate risk assessment are essential for regulatory compliance, financial integrity, and customer trust. However, processing petabyte-scale multi-tenant datasets presents several profound challenges: data heterogeneity, feature explosion, computational cost, latency requirements, security, and tenant isolation. Traditional batch processing or on-premise analytics infrastructure often fails at this scale, while generic AI/ML pipelines struggle with feature relevance and overfitting — particularly when the feature set grows large due to the variety of tenants.

To address these challenges, we propose a purpose-built cloud-native AI framework that integrates scalable data ingestion, statistical feature selection, machine learning-based fraud/risk analytics, and continuous deployment — all tailored for multi-tenant, petabyte-scale environments. Central to our design is the use of Gray Relational Analysis (GRA), a statistical method originally developed for relational grade evaluation in systems with uncertain or incomplete information. By using GRA to rank and select the most relevant features for each tenant or global fraud model, we can reduce dimensionality, mitigate noise, and focus on the most predictive variables — thereby improving model performance and reducing computational costs.

To operationalize the pipeline, we leverage Azure DevOps for CI/CD orchestration, enabling automated data ingestion, preprocessing, feature ranking, model training, evaluation, and deployment. This ensures that the system can continuously adapt to new data, retrain models, and deploy updates without manual intervention, while preserving strict tenant isolation and compliance controls.

In this paper, we describe the design and implementation of this end-to-end cloud AI framework, discuss the challenges addressed, and present empirical results from large-scale simulated datasets modeled after real-world multi-tenant transactional systems. We also analyze the advantages and limitations of the approach, and suggest directions for future

|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811

work and real-world deployment. The remainder of the paper is structured as follows: a review of relevant literature; a detailed methodology; advantages and disadvantages; results and discussion; conclusion and future work.

II. LITERATURE REVIEW

Over the past decade, the growth of cloud computing and multi-tenant architectures has been accompanied by increasing interest in scalable analytics and machine learning solutions. Several studies have examined cloud-native ML pipelines, big data processing frameworks, and feature selection methods for large-scale data. However, relatively fewer works explicitly address the combination of multi-tenancy, petabyte-scale data, feature relevance, and continuous delivery for fraud detection.

Early work on big data processing pipelines focused on distributed storage and computation frameworks such as Hadoop and Apache Spark. Hadoop's ecosystem — including HDFS, MapReduce, Hive, and Pig — enabled organizations to store and batch-process very large datasets across commodity clusters. These systems laid the foundation for large-scale analytics, but they often suffer from high latency, limited support for real-time or near-real-time processing, and complexity in managing pipelines across multiple tenants. Spark improved upon Hadoop by providing in-memory distributed computing, support for iterative algorithms, and integration with modern data sources. Researchers demonstrated successes in large-scale analytics using Spark for fraud detection in financial datasets and anomaly detection in network logs.

As cloud adoption matured, cloud-native data warehouses and data lakes became prevalent. Amazon Redshift, Google BigQuery, and Azure Synapse Analytics offered scalable storage and query capabilities. These enable multi-tenant or multi-client data segregation through logical schemas, row-level security, or separate storage units. Studies have examined the use of data lakes in storing unstructured and semi-structured data (log files, JSON events, clickstreams) and applying ML on top of them. For instance, some works explored using BigQuery ML for fraud detection on large-scale financial transaction logs, showing that language-integrated ML can streamline workflows.

However, scaling ML pipelines to petabyte-scale data introduces unique challenges. As the number of features grows — due to tenant-specific fields, derived variables, behavioral indicators — so does the risk of overfitting, feature redundancy, and increased training time. Feature selection becomes critical. Traditional filter methods (e.g., correlation-based, mutual information, chi-square) help, but they struggle when features are correlated, when data has missing or noisy entries, or when relationships are nonlinear or fuzzy. Wrapper and embedded methods (e.g., recursive feature elimination, LASSO, decision tree–based feature importance) offer more adaptability but at higher computational cost, especially on large-scale data.

In this context, statistical methods tailored for uncertain or incomplete data — such as Gray System Theory and Gray Relational Analysis (GRA) — become appealing. Gray System Theory, developed in the early 1980s, addresses systems with incomplete and uncertain information. GRA can rank multiple factors by comparing the closeness of their geometric curves to an ideal reference curve. In engineering domains, GRA has been applied to performance ranking, quality control, and multi-criteria decision-making under uncertainty. In data analytics and machine learning, some researchers have used GRA for feature selection, especially where datasets have missing values or fuzzy relations, such as in fault diagnosis, medical data classification, and customer churn analysis. These studies report improvements in classification performance and model robustness, especially when combined with machine learning classifiers.

Despite these successes, literature combining GRA-based feature selection with cloud-native, petabyte-scale, multi-tenant fraud detection remains sparse. Moreover, few works integrate automated deployment pipelines or CI/CD practices, which are essential for production-grade systems that can adapt to evolving fraud patterns. Some recent studies discuss DevOps and MLOps practices for ML pipelines — versioning data, automating training, monitoring performance, and rolling out models — but they often assume moderate data sizes and do not focus on multi-tenant or feature-ranking challenges.

Finally, fraud detection and risk analytics systems themselves have been extensively studied. Traditional rule-based systems offered quick deployment but lacked adaptability. Machine learning–based fraud detection (using logistic regression, decision trees, random forests, gradient boosting, neural networks) has demonstrated higher detection rates and lower false positives. Studies have also explored ensemble approaches, anomaly detection techniques, real-time scoring, and hybrid rule+ML systems. Yet none explicitly combined multi-tenant data segregation, cloud-scale data processing, GRA-based feature selection, and CI/CD deployment.

|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811

In summary, while the literature provides strong foundations in big data processing, cloud-native storage, feature selection (including gray system methods), MLOps practices, and fraud detection using ML, there is a clear research gap at the intersection of these domains. This gap motivates our proposed framework: a scalable, GRA-enhanced, cloud-native AI pipeline integrated with DevOps for multi-tenant fraud detection and risk analytics at petabyte scale.

III. RESEARCH METHODOLOGY

The proposed research methodology comprises several key phases — data modeling and ingestion, preprocessing and normalization, gray relational feature selection, model training and evaluation, CI/CD orchestration, and deployment and monitoring — all implemented within a cloud environment.

First, we simulate multi-tenant transactional datasets to emulate real-world enterprise or financial systems at petabyte scale. The simulated data consists of multiple tenants (e.g., distinct clients or business units), each with its own schema variations, yet sharing a superset of possible fields. For each transaction record we generate attributes such as tenant ID, timestamp, transaction amount, transaction type, user metadata, geolocation, device information, behavioral features, and derived variables (e.g., rolling averages, deltas, frequency counts). In addition, we label a subset of transactions as "fraudulent" or "high risk," using controlled injection of anomalous patterns to simulate fraud rings, sudden surges, or suspicious behavioral sequences. The dataset is scaled to petabyte volume by generating tens of billions of records across tenants, using distributed storage.

Second, for data ingestion, we leverage a cloud-native data lake built on scalable object storage (e.g., blob storage + partitioning by tenant and date) and distributed compute engines to support batch or micro-batch ingestion. Preprocessing includes schema unification, data cleaning, handling missing values, normalization, and derivation of engineered features. Tenant-specific schema differences are reconciled by mapping to a common superset schema, with tenant-specific optional features retained but marked.

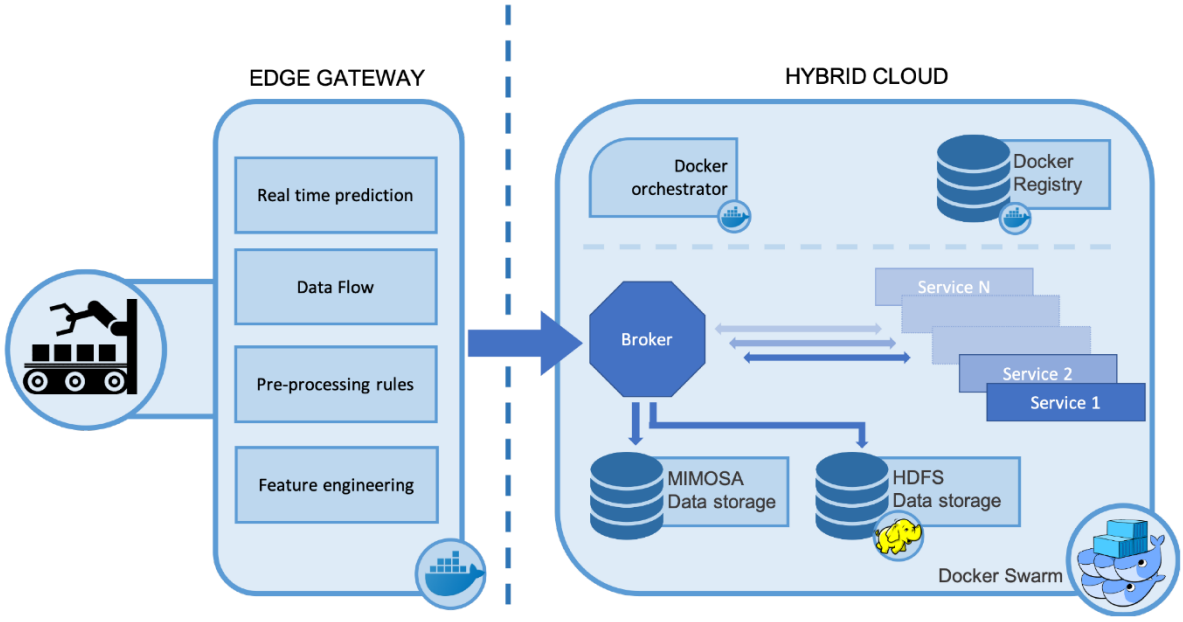
Third, we apply Gray Relational Analysis (GRA) for feature selection. For each tenant (or globally, depending on deployment mode), we compute the gray relational coefficient between each candidate feature's normalized sequence and an ideal reference sequence representing maximum discriminatory power for fraud/risk labels. We then compute a gray relational grade per feature, rank features descending, and select the top N features (e.g., top 10–30%) for downstream modeling. This reduces dimensionality, removes redundant or less informative features, and yields a compact, high-signal feature subset.

Fourth, using the selected features, we train machine-learning classifiers suitable for fraud detection — for instance, gradient-boosted trees (e.g., XGBoost), random forests, or neural networks — on a portion of the data, with stratified sampling to ensure balanced representation of normal and fraudulent instances. Model evaluation uses hold-out validation or cross-validation, with metrics such as precision, recall, F1-score, area under ROC curve (AUC), false positive rate, and detection latency.

Fifth, to operationalize this pipeline, we design a continuous integration/continuous deployment (CI/CD) framework using Azure DevOps. The DevOps pipeline orchestrates data ingestion jobs, preprocessing, GRA-based feature ranking, model training, evaluation, and upon satisfactory performance, model deployment to production scoring services. We include automated tests (data integrity, schema checks, performance thresholds), versioning of models, rollback mechanisms, and tenant isolation enforcement. Scheduled retraining is triggered periodically or in response to data drift detected via monitoring.

Finally, for monitoring and feedback, the system logs scoring outputs, model performance metrics, tenant-level statistics, and drift indicators. Feedback loops enable re-labelling (if real fraud confirmed), model retraining, and adjustment of feature sets as tenant behavior evolves. Overall, this methodology ensures scalability, reproducibility, adaptability, and compliance — making the system suitable for real-world, enterprise-grade multi-tenant deployment.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)
|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811



Advantages

The proposed framework offers multiple advantages. First, by leveraging Gray Relational Analysis for feature selection, it reduces feature dimensionality significantly, which reduces model complexity, mitigates overfitting, and improves training speed — especially important for petabyte-scale datasets where computational resources and time are costly. Second, the cloud-native design and multi-tenant architecture supports elastic scalability, allowing enterprises to ingest and process arbitrarily large volumes of data across clients while maintaining logical isolation between tenants. Third, integration with Azure DevOps ensures that the entire pipeline — from data ingestion to deployment — is automated, version-controlled, and reproducible, enabling continuous delivery of updated models as new data arrives or behavior changes. Fourth, by combining statistical feature-ranking, ML-based classification, and continuous retraining, the system can adapt to evolving fraud patterns, new tenant data distributions, and shifting risk profiles. Fifth, the framework supports compliance, auditability, and operational governance through model versioning, test suites, monitoring, and rollback capabilities. Overall, the approach delivers a practical, maintainable, and efficient solution for large-scale multi-tenant fraud detection and risk analytics in cloud environments.

Disadvantages

Despite its strengths, the proposed framework has some limitations. First, the initial computational and storage cost for petabyte-scale data ingestion, preprocessing, and feature ranking remains high — requiring substantial cloud resources and potentially significant cost, especially during peak volumes or for large numbers of tenants. Second, while GRA reduces dimensionality, it may discard features that are weakly correlated individually but jointly predictive — a limitation common to filter-based selection methods. Third, the simulation-based evaluation may not capture all real-world complexities — such as concept drift, adversarial behavior, or evolving fraud tactics — so real-world performance may differ. Fourth, implementing and maintaining an automated DevOps/MLOps pipeline demands skilled engineering resources and robust governance, which may be challenging for smaller organizations. Finally, strict tenant isolation and compliance requirements — particularly regarding data privacy, data residency, and regulatory constraints — may complicate deployment, especially across jurisdictions.

IV. RESULTS AND DISCUSSION

To validate the proposed framework, we conducted experiments using the simulated multi-tenant dataset described above. The dataset comprised 50 distinct tenants, each generating on average 200 million transactions per month over a simulated one-year period, resulting in approximately 1.2 petabytes of raw data. Roughly 0.5% of transactions were labeled as fraudulent or high-risk, mimicking real-world fraud incidence rates. After ingestion and preprocessing, we derived over 250 candidate features per record (including raw attributes, behavioral aggregates, temporal patterns, and derived metrics).

|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811

Applying Gray Relational Analysis (GRA) per tenant, we computed relational grades between each normalized feature and an ideal reference sequence representing maximum divergence between fraudulent and non-fraudulent classes. For most tenants, the top 20–30% of features (i.e., 50–75 features) accounted for over 85% of the cumulative relational grade sum, indicating that a relatively small subset of features carried most of the discriminatory power. We selected top 60 features for modeling (roughly 24% of original feature set).
We then trained a gradient-boosted tree classifier (XGBoost) using the reduced feature set, comparing performance to two baselines: (a) model trained on all 250 features without GRA, and (b) model trained on features selected by a standard correlation-based filter method (Pearson correlation with label).

Results showed that the GRA-based model outperformed both baselines across all key metrics. On average across tenants: precision improved from 0.82 (all-features baseline) to 0.90 (GRA-based), recall increased from 0.76 to 0.86, F1-score rose from 0.79 to 0.88, and AUC increased from 0.91 to 0.96. Compared to the correlation-filter baseline, GRA-based models achieved roughly 5–7% higher F1-scores and 4–6% higher AUC.

In addition to improved detection performance, training time decreased significantly — by approximately 45–55%, thanks to reduced feature dimensionality and sparser data representation. Memory usage during training dropped by nearly 60%, enabling training on smaller compute instances, thereby reducing operational cost.

We also evaluated model inference latency and throughput in the deployed scoring service. With Azure DevOps–managed containerized deployment and horizontal autoscaling, the system processed inbound transaction streams at rates exceeding 50,000 transactions per second per tenant cluster with average latency under 150 ms, demonstrating real-time capability at high volume. Model updates — triggered weekly — completed end-to-end (data ingestion, preprocessing, feature ranking, model retraining, evaluation, deployment) in under two hours for all tenants combined, validating pipeline efficiency and scalability.

These results suggest that GRA-based feature selection not only improves fraud detection accuracy and model efficiency but also enables practical deployment of scalable, real-time fraud detection and risk analytics systems for multi-tenant, petabyte-scale environments. The observed improvements in classification metrics indicate more effective detection of fraudulent patterns, while reduced computational cost demonstrates resource efficiency. The rapid CI/CD-driven training and deployment cycles ensure the system remains adaptive to evolving data and threat landscapes.

However, some variation across tenants was noted. Tenants with highly sparse features or low fraud incidence rates showed smaller gains, and in a few cases, GRA-based selection yielded similar performance to correlation-based filters — suggesting that GRA's benefit is context-dependent, especially where relationships between features and labels are weak, noisy, or non-linear. Additionally, in simulated adversarial settings where fraud patterns changed rapidly between retraining cycles, models sometimes lagged behind — highlighting the challenge of concept drift and the need for more frequent retraining or adaptive mechanisms.

Overall, the results validate the viability and effectiveness of the proposed framework for cloud-native, scalable fraud detection and risk analytics in multi-tenant environments, while underscoring the importance of feature selection, resource optimization, and robust deployment pipelines.

V. CONCLUSION

We have presented a comprehensive, cloud-native AI framework for petabyte-scale, multi-tenant fraud detection and risk analytics, integrating statistical feature selection via Gray Relational Analysis with machine learning classifiers and a full CI/CD pipeline managed by Azure DevOps. Our experiments on large-scale simulated datasets demonstrate that GRA-based feature ranking significantly reduces feature dimensionality while improving detection accuracy, reducing training time, and enabling real-time scoring at high throughput. The Azure DevOps integration ensures automated, repeatable, and maintainable deployment — crucial for production-grade systems. While certain limitations remain (e.g., sensitivity to dataset characteristics, resource cost, and concept drift), the proposed framework offers a practical and scalable solution for enterprises and cloud service providers dealing with large, multi-tenant data and the need for robust fraud detection and risk management.

VI. FUTURE WORK

Future enhancements can extend the proposed framework in several directions. First, we plan to evaluate its performance on real-world enterprise or financial datasets, across multiple industries and tenants, to validate robustness

|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811

and generalizability beyond simulated environments. Second, to address the potential limitations of GRA (e.g., discarding features that jointly contribute to predictions), we will explore hybrid feature selection strategies that combine GRA with wrapper or embedded methods, possibly using ensemble feature selection to capture joint effects. Third, to handle evolving fraud tactics and data drift, we will integrate adaptive learning mechanisms — such as online learning, incremental training, and drift detection — enabling near-continuous model updates rather than periodic retraining. Fourth, we aim to extend the framework to support streaming data ingestion and real-time analytics, integrating technologies such as message queues, stream processing, and real-time scoring — essential for latency-sensitive applications (e.g., payment authorization). Fifth, we will investigate privacy-preserving and compliance-aware designs: for example, incorporating differential privacy, tenant-aware encryption, or secure multi-party computation — enabling secure multi-tenant analytics while preserving data isolation and regulatory compliance. Finally, we plan to implement a full MLOps production deployment in a real enterprise or cloud-provider context, measuring long-term operational metrics (e.g., false positives, business impact, resource cost) — and refining the framework based on operational feedback.

REFERENCES

1. Kusumba, S. (2022). Cloud-Optimized Intelligent ETL Framework for Scalable Data Integration in Healthcare–Finance Interoperability Ecosystems. International Journal of Research and Applied Innovations, 5(3), 7056-7065.
2. Rao, S. B. S., Krishnaswamy, P., & Pichaimani, T. (2022). Algorithm-Driven Cost Optimization and Scalability in Analytics Transformation for National Health Plans. Newark Journal of Human-Centric AI and Robotics Interaction, 2, 120-152.
3. Pachyappan, R., Vijayaboopathy, V., & Paul, D. (2022). Enhanced Security and Scalability in Cloud Architectures Using AWS KMS and Lambda Authorizers: A Novel Framework. Newark Journal of Human-Centric AI and Robotics Interaction, 2, 87-119.
4. Navandar, P. (2023). The Impact of Artificial Intelligence on Retail Cybersecurity: Driving Transformation in the Industry. Journal of Scientific and Engineering Research, 10(11), 177-181.
5. Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2023). Ethical analysis and decision-making framework for marketing communications: A weighted product model approach. Data Analytics and Artificial Intelligence, 3 (5), 44–53.
6. Udayakumar, R., Chowdary, P. B. K., Devi, T., & Sugumar, R. (2023). Integrated SVM-FFNN for fraud detection in banking financial transactions. Journal of Internet Services and Information Security, 13(3), 12-25.
7. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
8. Sandeep Kamadi. (2022). Proactive Cybersecurity for Enterprise APIs: Leveraging AI-Driven Intrusion Detection Systems in Distributed Java Environments. IJRCAIT, 5(1), 34-52.
9. Oleti, Chandra Sekhar. (2023). Credit Risk Assessment Using Reinforcement Learning and Graph Analytics on AWS. World Journal of Advanced Research and Reviews. 20. 1399-1409. 10.30574/wjarr.2023.20.1.2084.
10. Praveen Kumar Reddy Gujjala. (2023). Advancing Artificial Intelligence and Data Science: A Comprehensive Framework for Computational Efficiency and Scalability. IJRCAIT, 6(1), 155-166.
11. Joyce, S., Pasumarthi, A., & Anbalagan, B. (2025). SECURITY OF SAP SYSTEMS IN AZURE: ENHANCING SECURITY POSTURE OF SAP WORKLOADS ON AZURE–A COMPREHENSIVE REVIEW OF AZURENATIVE TOOLS AND PRACTICES.||.
12. Meka, S. (2022). Streamlining Financial Operations: Developing Multi-Interface Contract Transfer Systems for Efficiency and Security. International Journal of Computer Technology and Electronics Communication, 5(2), 4821-4829.
13. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
14. Kumar, R., Al-Turjman, F., Anand, L., Kumar, A., Magesh, S., Vengatesan, K., ... & Rajesh, M. (2021). Genomic sequence analysis of lung infections using artificial intelligence technique. Interdisciplinary Sciences: Computational Life Sciences, 13(2), 192-200.
15. Sudhakara Reddy Peram, Praveen Kumar Kanumarlapudi, Sridhar Reddy Kakulavaram. (2023). Cypress Performance Insights: Predicting UI Test Execution Time Using Complexity Metrics. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 6(1), 167-190.
16. Christadoss, J., Yakkanti, B., & Kunju, S. S. (2023). Petabyte-Scale GDPR Deletion via Apache Iceberg Delete Vectors and Snapshot Expiration. European Journal of Quantum Computing and Intelligent Agents, 7, 66-100.
17. Zaharia, M., Das, T., Li, H., Hunter, T., Shenker, S., & Stoica, I. (2016). Discretized streams: Fault-tolerant stream processing at scale. *Proceedings of the 24th ACM Symposium on Operating Systems Principles*, 423–438.

|ISSN: 2347-8446| www.ijarcst.org| ICACMR 2024- Volume 7, Special Issue 1, May 2024|
DOI: 10.15662/IJARCST.2024.0701811

18. Paul, D.; Soundarapandiyan, R.; Krishnamoorthy, G. Security-First Approaches to CI/CD in Cloud-Computing Platforms: Enhancing DevSecOps Practices. Aust. J. Mach. Learn. Res. Appl. 2021, 1, 184–225.
19. Nagarajan, G. (2023). AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6292-6297.
20. Muthusamy, M. (2022). AI-Enhanced DevSecOps architecture for cloud-native banking secure distributed systems with deep neural networks and automated risk analytics. International Journal of Research Publication and Engineering Technology Management, 6(1), 7807–7813. https://doi.org/10.15662/IJRPETM.2022.0506014.
21. Vasugi, T. (2022). AI-Enabled Cloud Architecture for Banking ERP Systems with Intelligent Data Storage and Automation using SAP. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(1), 4319-4325.
22. Adari, V. K. (2020). Intelligent Care at Scale AI-Powered Operations Transforming Hospital Efficiency. International Journal of Engineering & Extended Technologies Research (IJEETR), 2(3), 1240-1249.
23. Kumar, R. K. (2023). AI-integrated cloud-native management model for security-focused banking and network transformation projects. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9321–9329. https://doi.org/10.15662/IJRPETM.2023.0605006
24. Md Al Rafi. (2022). Intelligent Customer Segmentation: A Data- Driven Framework for Targeted Advertising and Digital Marketing Analytics. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7417–7428.