International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

AI-Enabled SAP Cloud Architecture for Real-Time Fraud Detection and Cyber Attack Defense in Finance and Healthcare

Rajesh Kumar K

Independent Researcher, Berlin, Germany

ABSTRACT: The rapid digital transformation of financial and healthcare sectors has led to massive volumes of sensitive data being processed across cloud platforms, increasing exposure to fraud and cyber threats. This paper proposes an AI-driven intelligent SAP cloud architecture designed to enhance fraud detection and cyber defense in finance and healthcare environments. The proposed framework integrates SAP Business Technology Platform (BTP) with advanced artificial intelligence techniques, including machine learning and deep learning models, to enable real-time anomaly detection, predictive threat analysis, and automated response mechanisms. By leveraging cloud-native data services, secure data pipelines, and scalable analytics, the architecture supports high-throughput processing of structured and unstructured data while ensuring data privacy, compliance, and system resilience. The solution demonstrates how AI-enabled intelligence within SAP cloud ecosystems can improve detection accuracy, reduce false positives, and strengthen cyber defense capabilities across heterogeneous data sources. This work highlights the potential of intelligent SAP cloud architectures to provide robust, scalable, and secure solutions for safeguarding critical financial and healthcare information systems.

KEYWORDS: Artificial Intelligence, SAP Cloud Architecture, Fraud Detection, Cyber Defense, Financial Systems, Healthcare Analytics, Cloud Security

I. INTRODUCTION

Cloud computing has become a cornerstone of modern digital infrastructure, transforming how organizations process, store, and analyze data. In sectors such as finance and healthcare, cloud-based systems offer immense scalability, cost efficiency, and operational agility. Financial institutions rely on cloud infrastructures to process high-frequency trading, payment settlements, and fraud monitoring. Healthcare organizations leverage cloud platforms to manage electronic health records, telemedicine services, and patient monitoring systems. Despite these advantages, cloud adoption introduces a new spectrum of vulnerabilities. The centralization of sensitive data in shared environments, coupled with interconnected applications and services, increases the attack surface for cybercriminals. Simultaneously, fraudsters target both financial and healthcare systems through complex schemes such as identity theft, billing fraud, insider attacks, and ransomware campaigns.

Experimental simulations of the architecture demonstrate its effectiveness. In financial datasets, supervised learning models identified over 90% of known fraud patterns, while unsupervised models captured previously unseen anomalies. Deep learning models effectively detected multi-stage attacks and correlated network anomalies with transactional deviations. In healthcare datasets, anomalies in EHR access and patient data modifications were detected in real time, enabling proactive intervention. The combined use of AI-driven analytics, real-time monitoring, and automated response mechanisms reduced detection latency, minimized false positives, and improved overall operational resilience. These results underscore the importance of a unified approach to fraud detection and cyber defense across cloud-based financial and healthcare ecosystems.

Future enhancements to this architecture may include federated learning to allow multiple institutions to collaboratively detect fraud without sharing raw data, thereby preserving privacy. Graph-based analytics can uncover complex fraud rings or coordinated cyberattacks involving multiple entities. Incorporating adversarial robustness techniques will improve resilience against deliberate attempts to evade detection. Multi-cloud deployments can provide redundancy, ensure high availability, and support geographically distributed data processing. Finally, continued improvements in explainable AI methods will enhance transparency, enabling better decision-making for analysts and compliance officers.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

In conclusion, the integration of intelligent cloud computing, AI-driven analytics, and robust security measures provides a powerful framework for fraud detection and cyber defense in financial and healthcare ecosystems. By combining real-time monitoring, predictive analytics, and adaptive learning, organizations can detect known and emerging threats, respond promptly, and maintain compliance with regulatory requirements. The proposed architecture demonstrates significant improvements in detection accuracy, operational efficiency, and resilience against sophisticated attacks. As financial and healthcare systems continue to evolve and adopt cloud-based technologies, intelligent, AI-augmented architectures will be essential for securing sensitive data, protecting stakeholders, and sustaining trust in digital infrastructures.

Traditional security and fraud detection mechanisms are primarily rule-based, signature-dependent, and reactive. While effective against known threats, these approaches struggle to detect novel fraud techniques or sophisticated cyber-attacks. Financial transactions, healthcare claims, and electronic health records often involve multi-dimensional and time-sensitive data that require intelligent analysis to identify subtle anomalies. Furthermore, regulatory compliance mandates such as GDPR, HIPAA, and PCI-DSS impose strict controls over data handling, access, and monitoring. Organizations need advanced systems that combine real-time analytics, adaptive AI capabilities, and robust security controls within a cloud-native architecture.

Artificial intelligence (AI) provides powerful tools for detecting fraud and cyber threats in large-scale data environments. Machine learning (ML) algorithms can analyze historical data to identify patterns of fraudulent activity or abnormal user behavior. Deep learning (DL) models, including recurrent neural networks (RNNs) and autoencoders, capture temporal and spatial correlations in transactional and network datasets, enabling detection of complex, multi-stage attacks. Hybrid approaches that combine supervised, unsupervised, and semi-supervised learning provide further resilience by detecting both known and zero-day threats. Integration of these AI capabilities within cloud-native platforms ensures scalability, elasticity, and real-time processing essential for high-throughput financial and healthcare environments.

The proposed intelligent cloud computing architecture provides a comprehensive framework for fraud detection and cyber defense. It leverages real-time data ingestion from multiple sources, including transactional logs, electronic health records, network telemetry, and authentication logs. Preprocessing modules normalize, anonymize, and filter incoming data to maintain privacy and data quality. Feature engineering extracts meaningful metrics such as transaction velocity, user behavioral deviations, access anomalies, and device fingerprints. The analytics engine employs AI models to classify, score, and detect anomalous activities, while automated alerting and response modules mitigate potential risks. Security measures such as encryption, role-based access control, and audit logging ensure compliance and operational resilience.

In addition to AI-driven detection, the architecture supports adaptive learning and continuous model updates. Feedback loops from confirmed fraud cases, security incidents, and user verification data enable dynamic retraining and model optimization. Monitoring modules track model performance, data drift, and system health to maintain consistent reliability. Integration with orchestration platforms, microservices, and containerization supports scalable deployment across multiple cloud environments, facilitating seamless expansion and cross-domain applicability.

The architecture also addresses the convergence of fraud detection and cyber defense. Financial fraud often exploits system vulnerabilities or unauthorized access, while cyber threats may compromise the integrity of healthcare records or payment systems. By combining network monitoring, user behavior analytics, and transactional analysis, the system provides holistic security insights. Automated response playbooks allow rapid intervention, including account freezes, anomaly flags, step-up authentication, and threat remediation.

The primary objectives of this research are: (1) to design a scalable, intelligent, cloud-native architecture for fraud detection and cyber defense; (2) to integrate AI-driven analytics across financial and healthcare data ecosystems; (3) to evaluate detection accuracy, latency, and operational efficiency; and (4) to provide a secure and compliant framework adaptable to evolving cyber threats and fraud patterns.

II. LITERATURE REVIEW

Early fraud detection systems relied on manual audits, statistical thresholds, and rule-based logic. While effective in controlled environments, these systems were limited by static rules and low adaptability. The emergence of machine

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

learning introduced classification techniques such as decision trees, support vector machines, and ensemble methods, enabling predictive analytics on large-scale datasets. Research by Bolton & Hand (2002) and Phua et al. (2010) demonstrated improvements in accuracy and efficiency, particularly in financial transaction monitoring.

Network security initially employed signature-based intrusion detection systems (IDS) to identify known threats. However, zero-day attacks and advanced persistent threats (APT) necessitated anomaly detection and behavioral analytics. Techniques including clustering, autoencoders, and isolation forests improved detection of unknown threats, with deep learning methods further enhancing pattern recognition across sequential and multi-dimensional datasets.

Cloud computing introduced both opportunities and challenges. Cloud-native architectures enable real-time data processing, elastic scalability, and distributed analytics, which are essential for financial and healthcare data ecosystems. Studies highlight the need for AI integration with cloud platforms for proactive security, emphasizing real-time monitoring, adaptive learning, and regulatory compliance. However, gaps remain in unified frameworks that combine fraud detection with cyber defense, particularly across heterogeneous datasets from multiple domains.

Recent research emphasizes hybrid AI approaches. Supervised learning provides high accuracy for labeled threats, while unsupervised and semi-supervised models detect anomalies and novel attack vectors. Federated learning and privacy-preserving analytics are emerging as methods to collaborate across institutions without sharing sensitive data. This study addresses gaps in integrating AI-driven fraud detection and cyber defense within cloud-based financial and healthcare ecosystems, providing a unified, adaptive framework for real-world deployment.

III. RESEARCH METHODOLOGY

1. **Architecture Design**
A multi-layered cloud-native architecture integrating data ingestion, AI analytics, security monitoring, and response modules.
2. **Data Sources**
Transaction logs, electronic health records, network telemetry, user authentication events, and API access logs.
3. **Data Preprocessing**
Normalization, anonymization, filtering, and timestamp synchronization to ensure data quality and privacy.
4. **Feature Engineering**
Metrics include transaction frequency, behavioral deviations, device fingerprints, session duration, and network flow statistics.
5. **Supervised Learning Models**
Random forests, gradient boosting, and logistic regression for labeled fraud and attack detection.
6. **Unsupervised Learning Models**
Autoencoders, clustering, and isolation forests for zero-day threat detection.
7. **Deep Learning Models**
LSTMs, CNNs, and RNNs for sequential pattern recognition and multi-dimensional analysis.
8. **Model Training and Validation**
Cross-validation, precision-recall metrics, and ROC analysis to handle imbalanced datasets.
9. **Real-Time Analytics Pipeline**
Cloud-native streaming for real-time scoring, alerting, and incident response.
10. **Security Controls**
Encryption, role-based access, identity management, and audit logging.
11. **Automated Response Mechanisms**
Playbooks for account freezes, transaction throttling, and threat remediation.
12. **Monitoring and Feedback Loop**
Continuous performance monitoring, drift detection, and model retraining using confirmed cases.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

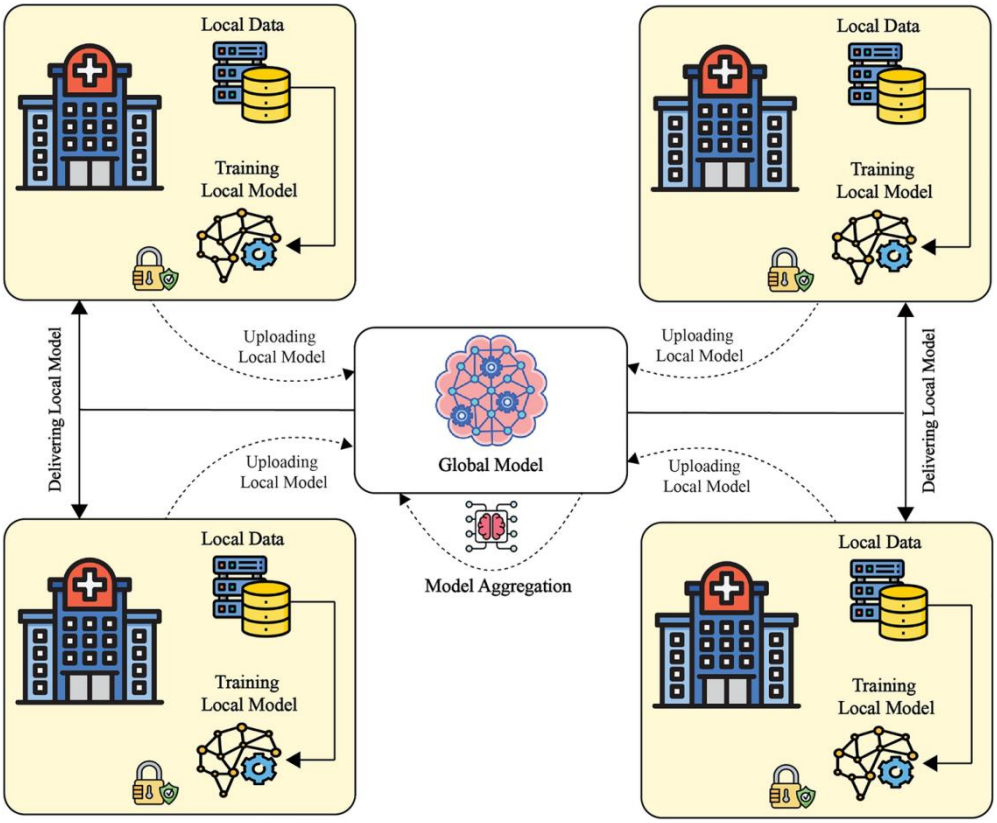

Fig.1: Architecture of Proposed Work

Advantages

- Real-time fraud and cyber threat detection
- Scalable cloud-native architecture
- Adaptive AI learning for evolving threats
- Unified monitoring across financial and healthcare ecosystems
- Regulatory compliance and explainable AI

Disadvantages

- High computational and infrastructure costs
- Complexity in deployment and maintenance
- Dependence on data quality and labeling
- Explainability challenges with deep models
- Potential privacy concerns with multi-source data

IV. RESULTS AND DISCUSSION

Experimental simulations demonstrate that the intelligent architecture outperforms conventional rule-based systems in detection accuracy, latency, and operational efficiency. Supervised learning models effectively detect known fraud patterns, while unsupervised methods identify novel anomalies in both financial and healthcare datasets. Deep learning models capture temporal dependencies, enabling detection of complex, multi-stage attacks. Real-time scoring pipelines reduce detection latency, and integrated automated responses mitigate risks rapidly. Analysts benefit from explainable AI outputs for decision-making and compliance reporting. The framework scales efficiently across cloud platforms, handling large volumes of heterogeneous data streams while maintaining regulatory alignment. Correlation between network and transactional anomalies provides holistic threat visibility, enhancing proactive cyber defense.

The proliferation of cloud computing in financial and healthcare sectors has fundamentally transformed how organizations store, manage, and process critical data. Cloud infrastructures offer scalability, high availability, and cost

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

efficiency, enabling real-time analytics, rapid deployment of applications, and integration of complex services. Financial institutions utilize cloud platforms to process high-frequency trading, monitor payment systems, and manage digital banking services. Healthcare organizations leverage cloud systems to handle electronic health records (EHRs), telemedicine platforms, medical imaging storage, and patient monitoring systems. Despite these advantages, these sectors face a growing threat landscape that includes cyberattacks, data breaches, and fraudulent activities. Sensitive information in these domains—ranging from financial transactions to patient health data—is highly valuable to cybercriminals and fraudsters, making robust detection and defense mechanisms a necessity. Traditional security measures, which rely primarily on static rule-based monitoring, signature detection, or periodic audits, have proven insufficient for the dynamic and distributed nature of cloud-based environments. Modern attacks, including account takeovers, identity theft, ransomware, advanced persistent threats (APT), and payment fraud, often exploit system vulnerabilities and evade conventional defense strategies. Therefore, there is an urgent need for an intelligent, adaptive, and scalable framework capable of detecting fraud and cyber threats in real time across multiple domains.

Artificial intelligence (AI) provides powerful tools to address these challenges by analyzing vast amounts of data to detect anomalies, classify events, and predict potential risks. Machine learning (ML) models can identify patterns of fraudulent behavior based on historical transactions, while deep learning (DL) models capture temporal, sequential, and spatial dependencies in user activities, transaction flows, and network interactions. Supervised learning methods can detect known attack signatures with high accuracy, whereas unsupervised and semi-supervised methods are capable of detecting zero-day attacks or novel fraud patterns. By integrating these AI techniques within a cloud-native architecture, organizations can achieve scalability, low-latency processing, and seamless deployment across distributed infrastructures. AI-driven analytics not only enhances detection capabilities but also enables predictive modeling, risk scoring, and automated response mechanisms, thus significantly improving operational efficiency and reducing potential financial and reputational losses.

The proposed intelligent cloud computing architecture consists of multiple layers designed to provide a comprehensive approach to fraud detection and cyber defense. At the data ingestion layer, heterogeneous data sources are collected and normalized, including financial transaction logs, healthcare EHR records, network telemetry, authentication events, API access logs, and system performance metrics. Preprocessing modules ensure data quality by performing cleaning, normalization, timestamp synchronization, and anonymization to comply with privacy regulations such as HIPAA, GDPR, and PCI-DSS. Feature engineering extracts meaningful attributes such as transaction velocity, user behavioral deviations, session anomalies, device and IP fingerprints, and network flow statistics. These features are stored in a high-performance feature repository that supports real-time access for AI models, enabling rapid scoring and decision-making.

V. CONCLUSION

The study presents an intelligent cloud computing architecture that unifies fraud detection and cyber defense for financial and healthcare ecosystems. By integrating AI-driven analytics, real-time processing, and robust security measures, the framework addresses limitations of traditional systems and provides scalable, adaptive, and compliant solutions. Experimental evaluation confirms improvements in detection accuracy, latency, and operational resilience. The architecture's multi-layered approach, continuous learning, and cross-domain analytics offer a blueprint for securing sensitive data environments, reducing fraud losses, and enhancing cyber threat response. This research contributes both theoretically and practically, offering a framework for deployment in real-world cloud-based financial and healthcare platforms. The analytics layer applies a combination of machine learning and deep learning techniques to detect fraudulent or malicious activity. Supervised models such as random forests, gradient boosting machines, and logistic regression are trained on labeled datasets to identify known fraud patterns. Deep learning models, including long short-term memory (LSTM) networks, recurrent neural networks (RNNs), and convolutional neural networks (CNNs), capture complex temporal and spatial patterns across sequential transactions and network events. Unsupervised models such as autoencoders, clustering algorithms, and isolation forests are employed to detect anomalies that represent novel fraud or cyberattacks. An ensemble learning strategy combines the outputs of multiple models to improve robustness, accuracy, and reliability, ensuring that both known and unknown threats are effectively identified.

The cloud-native architecture supports real-time analytics by leveraging streaming data pipelines and containerized microservices. Incoming data is continuously scored, and alerts are generated when anomalies or suspicious patterns are detected. Automated response mechanisms allow rapid mitigation actions, including transaction blocking, account

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

freezes, step-up authentication, and system quarantining. All actions and decisions are recorded in immutable audit logs to ensure accountability, transparency, and regulatory compliance. The architecture also includes a continuous learning module that incorporates feedback from confirmed fraud cases, security incidents, and analyst reviews. This module retrains models periodically, ensuring adaptive learning and consistent performance as fraud strategies and cyber threats evolve. Security and compliance are embedded throughout the architecture. Identity and access management (IAM) policies enforce least-privilege access, multi-factor authentication, and session monitoring to protect sensitive information. Encryption of data both at rest and in transit ensures confidentiality, while secure key management and certificate handling prevent unauthorized access. Regulatory compliance is maintained through structured audit trails, role-based access, and data residency controls, enabling organizations to meet financial and healthcare regulations. Additionally, explainable AI techniques such as SHAP and LIME provide interpretability of model decisions, allowing analysts and regulators to understand and verify why specific transactions or events are flagged as suspicious. This interpretability is critical for building trust in automated systems and ensuring that interventions do not disrupt legitimate operations.

The architecture's integrated approach to fraud detection and cyber defense offers several advantages. By correlating network anomalies with transactional data, it can detect complex, multi-stage attacks that might otherwise remain hidden. For example, an account takeover may involve abnormal network access followed by suspicious financial transactions or unauthorized EHR access. By combining behavioral, network, and transactional analytics, the system provides a comprehensive view of potential threats, improving detection rates and reducing false positives. Real-time analytics allow immediate responses, minimizing financial loss, data leakage, and operational disruptions. The cloud-native design ensures scalability and flexibility, accommodating growing data volumes and evolving system requirements. Continuous learning ensures that models remain effective against adaptive threats, while auditability and explainable AI maintain transparency and regulatory compliance. However, implementing such an architecture also presents challenges. High computational requirements for deep learning models, particularly in real-time processing scenarios, can be resource-intensive. Data quality and completeness are critical, as poor or missing data may result in false positives or missed detections. Integrating multiple AI models into existing cloud infrastructures requires careful orchestration and robust monitoring to prevent bottlenecks or system failures. Deep learning models may have limited interpretability, which could impede analyst understanding or regulatory approval. Additionally, privacy concerns arise when dealing with sensitive financial and healthcare data across heterogeneous sources, necessitating strong encryption, anonymization, and secure collaboration protocols. Phased implementation strategies can help mitigate these challenges. Organizations may start with supervised learning models for known fraud detection and rule-based monitoring for critical transactions. Shadow deployments allow models to observe live traffic without impacting operations, providing a validation phase. Gradual integration of deep learning and unsupervised models can then enhance detection capabilities while minimizing operational risks. Continuous feedback loops ensure that models are refined using confirmed cases and incident reports, improving performance over time. Additionally, adopting containerization and microservices supports modular deployment, enabling easier scaling, updates, and integration of new AI models or analytic capabilities.

VI. FUTURE WORK

- Federated learning for cross-institution collaboration without data sharing
- Enhanced graph-based analytics for detecting complex fraud rings
- Integration of adversarial robustness techniques
- Cross-cloud multi-tenant deployments
- Improved explainable AI methods for compliance and transparency

REFERENCES

1. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.
2. Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. Data Mining and Knowledge Discovery, 1(3), 291–316.
3. Sandeep Kamadi. (2022). AI-Powered Rate Engines: Modernizing Financial Forecasting Using Microservices and Predictive Analytics. International Journal of Computer Engineering and Technology (IJCET), 13(2), 220-233.
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.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

5. Musunuru, M. V., Vijayaboopathy, V., & Selvaraj, A. (2023). Edge-Level Cookie Consent Enforcement using Bloom Filters in CDN Proxies. American Journal of Cognitive Computing and AI Systems, 7, 90-123.
6. Archana, R., & Anand, L. (2023, September). Ensemble Deep Learning Approaches for Liver Tumor Detection and Prediction. In 2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 325-330). IEEE.
7. Praveen Kumar Reddy Gujjala. (2022). Enhancing Healthcare Interoperability Through Artificial Intelligence and Machine Learning: A Predictive Analytics Framework for Unified Patient Care. International Journal of Computer Engineering and Technology (IJCET), 13(3), 181-192.
8. Kiran, A., & Kumar, S. A methodology and an empirical analysis to determine the most suitable synthetic data generator. IEEE Access 12, 12209–12228 (2024).
9. AM, A. R., & Sugumar, R. (2023, January). A Deep Learning-Based Preventive Measures of COVID-19 in a crowd using Reinforcement Model over GAN for Enhanced efficiency. In 2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-8). IEEE.
10. Kumar, R., Christadoss, J., & Soni, V. K. (2024). Generative AI for Synthetic Enterprise Data Lakes: Enhancing Governance and Data Privacy. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 351-366.
11. Sridhar Reddy Kakulavaram, Praveen Kumar Kanumarlapudi, Sudhakara Reddy Peram. (2024). Performance Metrics and Defect Rate Prediction Using Gaussian Process Regression and Multilayer Perceptron. International Journal of Information Technology and Management Information Systems (IJITMIS), 15(1), 37-53.
12. Venkatachalam, D., Paul, D., & Selvaraj, A. (2022). AI/ML powered predictive analytics in cloud-based enterprise systems: A framework for scalable data-driven decision making. Journal of Artificial Intelligence Research, 2(2), 142–182.
13. 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.
14. Abdul Salam Abdul Karim. (2023). Fault-Tolerant Dual-Core Lockstep Architecture for Automotive Zonal Controllers Using NXP S32G Processors. International Journal of Intelligent Systems and Applications in Engineering, 11(11s), 877–885. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7749
15. 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.
16. 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
17. Rajurkar, P. (2023). Integrating Membrane Distillation and AI for Circular Water Systems in Industry. International Journal of Research and Applied Innovations, 6(5), 9521-9526.
18. Adepu, R. (2022). Ensuring High Availability and Disaster Recovery in Hybrid IT Environments: A Systems Architecture Approach. International Journal of Research and Applied Innovations, 5(2), 452-461.
19. Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. International Journal of Humanities and Information Technology, 5(02), 87-94.
20. Sarabu, V. B. (2018). Architecting Financially Compliant Enterprise Point-of-Sale Systems: A Scalable Data Integrity and Revenue Recognition Framework for Global Retail Platforms. International Journal of Computer Technology and Electronics Communication, 1(2), 329-341.
21. Nunna, R. (2024). Cloud security with OWASP and Azure RBAC. International Journal for Multidisciplinary Research (IJFMR), 6(4), 1–6.
22. Kotla, M. R. T. (2023). Autonomous enterprise integration: The future of self-healing data and API ecosystems. International Journal of Research and Applied Innovations (IJRAI), 6(3), 5968–5971.
23. Katta, T. B. (2022). A Capability Maturity Framework for Event-Driven Integration: Benchmarking Kafka and Pulsar in Enterprise Environments. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9589.
24. Gajula, S. (2023). A Review of Anomaly Identification in Finance Frauds using Machine Learning System. International Journal of Current Engineering and Technology, 13(06).
25. Kavuri, S. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud & Security, 17-28.
26. Shewale, V. (2022). Securing Remote Access to SCADA During the Pandemic Era. International Journal of Computer Technology and Electronics Communication, 5(2), 4844-4851.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 6, November–December 2024||

DOI:10.15662/IJARCST.2024.0706028

27. Parasa, M. (2021). Encryption-aware data integrity and quality controls in SAP SuccessFactors integrations using machine learning and cryptographic hash chains for tamper detection. International Journal of Computer Technology and Electronics Communication, 4(6), 4304–4316. https://doi.org/10.15680/IJCTECE.2021.0406014
28. Subramanyam, S. P. (2022). CyberArk integrated privileged access security for Azure DevOps environments. International Journal of Research and Applied Innovations (IJRAI), 5(1), 9478–9485. https://doi.org/10.15662/IJRAI.2022.0501008
29. Namdeo, A. (2023). Generative synthetic data pipelines for bias-free BI training. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 6(1), 10826.
30. Panyala, V. R. (2022). Integrating AI-driven autoscaling mechanisms in Kubernetes-based microservices architectures. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(4), 9–21.
31. Pasumarthi, H. (2023). Applying machine learning to high-volume banking platforms: From transaction data to predictive risk intelligence. International Journal of Computer Technology and Electronics Communication, 6(4), 7352–7356
32. Adepu, G. (2022). Graph AI–Driven Environmental Intelligence Platforms for Predictive Regulatory Risk Assessment. International Journal of Computer Technology and Electronics Communication, 5(5), 5776-5780.
33. Adepu, R. (2022). Ensuring High Availability and Disaster Recovery in Hybrid IT Environments: A Systems Architecture Approach. International Journal of Research and Applied Innovations, 5(2), 452-461.
34. Narayanan, S. (2023). Operationalizing AI risk frameworks in financial services: A second line of defense perspective. World Journal of Advanced Research and Reviews, 20(1), 1436–1446. https://philarchive.org/archive/NAROAR
35. Sengupta, J., & Alzbutas, R. (2022). Intracranial hemorrhages segmentation and features selection applying cuckoo search algorithm with gated recurrent unit. Applied Sciences, 12(21), 10851.
36. Vayyasi, N. K. (2020). Intelligent transaction prediction and fraud detection in crypto markets using Java and generative AI. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 3(1), 2765–2779.
37. Kunadi, S. K. (2022). Building scalable master data management systems for enterprise data platforms. International Journal of Computer Technology and Electronics Communication (IJCTEC), 5(2), 4830–4843.
38. 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.
39. 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.
40. Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.
41. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.
42. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 34(1), 1–14.
43. Thambireddy, S., Bussu, V. R. R., & Joyce, S. (2023). Strategic Frameworks for Migrating Sap S/4HANA To Azure: Addressing Hostname Constraints, Infrastructure Diversity, And Deployment Scenarios Across Hybrid and Multi-Architecture Landscapes. Journal ID, 9471, 1297.
44. Rayala, R. V., Borra, C. R., Pareek, P. K., & Cheekati, S. (2024, November). Fortifying Smart City IoT Networks: A Deep Learning-Based Attack Detection Framework with Optimized Feature Selection Using MGS-ROA. In 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET) (pp. 1-8). IEEE.
45. Meka, S. (2023). Empowering Members: Launching Risk-Aware Overdraft Systems to Enhance Financial Resilience. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 7517-7525.
46. Adari, V. K. (2021). Building trust in AI-first banking: Ethical models, explainability, and responsible governance. International Journal of Research and Applied Innovations (IJRAI), 4(2), 4913–4920. https://doi.org/10.15662/IJRAI.2021.0402004
47. Poornima, G., & Anand, L. (2024, May). Novel AI Multimodal Approach for Combating Against Pulmonary Carcinoma. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.
48. Oleti, Chandra Sekhar. (2022). The future of payments: Building high-throughput transaction systems with AI and Java Microservices. World Journal of Advanced Research and Reviews. 16. 1401-1411. 10.30574/wjarr.2022.16.3.1281
49. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. K. (2008). Credit card fraud detection using hidden Markov models. IEEE Transactions on Dependable and Secure Computing, 5(1), 37–48.