International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

Machine Learning–Driven Financial and Marketing Analytics with Cybersecurity Intelligence in SAP Cloud Platforms

Rajesh Kumar K

Independent Researcher, Berlin, Germany

ABSTRACT: The rapid adoption of SAP-based cloud platforms in financial and marketing domains has significantly increased data-driven decision-making while simultaneously exposing enterprises to sophisticated cyber threats. This paper proposes a machine learning–driven analytical framework that integrates financial and marketing intelligence with cybersecurity analytics in SAP cloud environments. By leveraging advanced data analytics and generative AI techniques, the proposed approach enables real-time anomaly detection, predictive risk assessment, and adaptive threat mitigation across transactional and customer engagement data. Machine learning models are employed to calibrate financial forecasts, optimize marketing performance, and identify cyber attack patterns using behavioral and network-level indicators. The framework supports scalable cloud deployment and seamless integration with SAP systems, ensuring enhanced data security, operational resilience, and business agility. Experimental observations indicate improved accuracy in fraud detection, marketing insight generation, and cyber risk identification compared to conventional rule-based systems. The study demonstrates that unified analytics and cybersecurity intelligence can significantly strengthen financial and marketing operations in SAP cloud platforms while maintaining compliance and performance efficiency.

KEYWORDS: Machine Learning, Financial Analytics, Marketing Analytics, Cybersecurity Intelligence, SAP Cloud, Generative AI, Data Analytics.

I. INTRODUCTION

In today's rapidly evolving digital economy, enterprises face unprecedented challenges in managing financial operations, securing systems at scale, and deriving actionable insights from growing repositories of transactional data. Core enterprise systems like **SAP (Systems, Applications, and Products in Data Processing)** have advanced from traditional on-premise architectures to complex, distributed cloud ecosystems. These environments generate voluminous logs, diverse financial transactions, and distributed data streams demanding robust intelligence layers that can support real-time decision-making, risk mitigation, and strategic revenue insights. Cloud adoption has brought agility and scalability, but it has also introduced new complexities in financial oversight and system monitoring. Traditional analytic methods, which are often rule-based and reactive, struggle to keep pace with the speed and dynamism of modern enterprise operations. F

or example, detecting financial anomalies in global ledgers or transactional systems often involves manual audits and lagging indicators. Similarly, revenue attribution — the process of identifying which activities, channels, or product lines contribute to revenue — becomes increasingly opaque in omnichannel environments. Financial risk management, encompassing credit risk, market volatility, and internal control risks, similarly requires more than static dashboards; it demands predictive foresight. **Artificial intelligence (AI)** promises transformative capabilities in addressing these challenges. Machine learning (ML) and advanced analytics can uncover latent patterns that elude traditional analytics, forecast emerging trends, and provide confidence-weighted insights to decision-makers. When integrated with SAP Cloud Intelligence — SAP's suite of analytics and data-driven services — AI can significantly augment enterprise financial operations. Yet, despite the promise, there are gaps in unified frameworks that specifically align AI techniques with anomaly detection, revenue attribution, and financial risk management under a cohesive, scalable, and governance-controlled environment. This paper introduces an **AI-Driven SAP Cloud Intelligence framework** that unifies these capabilities. The proposed framework aligns multiple AI models and data pipelines with SAP Cloud infrastructure, ensuring seamless integration with enterprise data sources, compliance controls, and operational workflows. Anomaly detection models monitor transactional and behavioral data streams for irregularities that may indicate fraud, process failures, or system errors. Revenue attribution models apply causal inference, multi-touch

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

attribution, and predictive modeling to assess revenue contributions across complex sales lifecycles. Financial risk management models employ probabilistic forecasting and scenario analysis to quantify risk exposures and support strategic planning. The contributions of this research are threefold.

First, it presents a **conceptual architecture** that integrates AI models into SAP Cloud Intelligence, enabling real-time anomaly detection, precise revenue attribution, and comprehensive financial risk insights. Second, it defines a **methodological approach** for model development, training, evaluation, and operational deployment within enterprise environments. Third, it evaluates the framework's efficacy through simulated enterprise datasets and scenario-based analyses, demonstrating performance improvements against baseline approaches.

The remainder of this introduction elaborates on the operational pressures motivating the framework, outlines key research questions, and positions this work within broader enterprise technology trends. Financial operations increasingly intersect with cybersecurity and operational resilience. Anomalies in financial data can stem not only from business process deviations but also from malicious activities or system misconfigurations. As such, an integrated approach to anomaly detection must be both data-centric and context-aware, leveraging historical patterns, behavioral baselines, and adaptive learning mechanisms.

Revenue attribution is further complicated by the diversity of digital touchpoints and customer engagement channels. In B2B and B2C contexts alike, revenue realization may be influenced by marketing campaigns, partner referrals, recurring service contracts, or bundled product offerings. Traditional single-touch attribution methods fail to capture these nuances, leading to misaligned incentives and suboptimal strategic decisions. AI-driven attribution models can incorporate sequential patterns, channel interactions, and customer lifecycle data to assign revenue yield more accurately.

Financial risk management encompasses credit risk, liquidity risk, market risk, and operational risk. In the era of digital finance, risk exposures can fluctuate in near real-time, driven by macroeconomic shifts, geopolitical events, or internal operational disruptions. Predictive models — such as Bayesian networks, time-series forecasting, and Monte Carlo simulations — can quantify risk dynamics and support proactive mitigation strategies.

Despite these compelling needs, enterprise adoption of AI within SAP environments faces barriers including data governance, legacy integration, latency constraints, and model interpretability. SAP Cloud Intelligence offers native capabilities for analytics and data orchestration, yet a structured framework is necessary to harness AI models without compromising compliance or operational continuity.

II. LITERATURE REVIEW

The literature on AI, anomaly detection, revenue attribution, and financial risk management spans multiple domains including machine learning research, enterprise analytics, and financial engineering. Here, we summarize foundational work and connect it to the SAP Cloud Intelligence context.

Anomaly Detection. Anomaly detection has been extensively studied in the fields of statistics, cybersecurity, and finance. Classic statistical methods, such as control charts and Gaussian models, laid early foundations for detecting deviations from expected behavior. More recent research highlights machine learning approaches — supervised and unsupervised — for identifying irregularities in time series, transactional datasets, and network flows. Sommer and Paxson (2010) argue that purely signature-based systems fail to address emerging, novel anomalies, advocating ML-based methods for adaptive detection. Unsupervised techniques such as principal component analysis (PCA), clustering, and autoencoders are well suited for high-dimensional data with limited labeled anomalies. Financial anomaly detection research emphasizes irregular transaction patterns, fraud detection, and outlier spotting in ledger balances.

Revenue Attribution. Revenue attribution emerged from marketing science, where understanding how different customer touchpoints contribute to sales became vital. Traditional methods like first-touch and last-touch attribution often oversimplify complex customer journeys. Multi-touch attribution (MTA) models assign fractional credit to each interaction. Recent research explores causal inference, uplift modeling, and sequence modeling to assign revenue outcomes more accurately. Attribution in enterprise ERP systems, particularly with mixed on-premise and cloud data sources, remains a developing area.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

Financial Risk Management. Financial risk management has deep roots in economics and quantitative finance. Value at Risk (VaR), stress testing, and scenario analysis have long been employed to quantify exposures. AI and ML have gained traction in risk prediction, credit scoring, and liquidity forecasting. Machine learning models such as random forests, gradient boosting, and neural networks are applied to volatile financial datasets, often outperforming classical econometric models. Integrating risk analytics within enterprise ERP platforms remains a strategic priority for many organizations.

SAP Analytics & Cloud Intelligence. Within the SAP ecosystem, analytics capabilities have evolved from SAP BW (Business Warehouse) to SAP HANA and SAP Cloud Analytics. These platforms support real-time analytics, in-memory processing, and integration with operational SAP modules. Research underscores the need for AI augmentation of these analytics stacks to support real-time insights and predictive capabilities.

Despite robust research in each area, literature on unified frameworks that combine **anomaly detection, revenue attribution, and financial risk management** within **SAP cloud environments** is limited. This gap motivates the proposed AI-driven framework.

III. RESEARCH METHODOLOGY

This research methodology describes the comprehensive procedures used to design, develop, evaluate, and deploy AI models within SAP Cloud Intelligence for anomaly detection, revenue attribution, and financial risk management. The methodology begins with defining **research objectives** that specify detection accuracy thresholds, attribution performance metrics, and risk prediction reliability targets. Data requirements are identified, including access to SAP S/4HANA transactional logs, financial ledgers, CRM customer journeys, revenue postings, and historical risk event data. A **data governance framework** is established to ensure compliance with GDPR, SOC 2, and internal audit standards, incorporating role-based access controls, encryption at rest and in transit, and data lineage tracking via SAP Data Intelligence.

Next, **data ingestion pipelines** are designed using SAP Cloud Integration and SAP Data Intelligence to stream transactional and operational data into a centralized analytics layer. Preprocessing includes timestamp alignment, deduplication, handling of missing values, normalization, and feature extraction. Feature engineering for anomaly detection involves generating time series features, user behavior profiles, recurring transaction patterns, and statistical baselines. For revenue attribution, features include sequential interaction histories, sales channel identifiers, campaign metadata, product hierarchies, discounts, customer segmentation, and lifecycle stage indicators. Financial risk models leverage macroeconomic indicators, liquidity ratios, volatility indexes, historical loss distributions, and business event flags.

Model selection follows a hybrid strategy. Unsupervised models — such as autoencoders, isolation forests, and clustering algorithms — are selected for identifying unexpected patterns in high-dimensional anomaly detection tasks, due to limited labeled anomalies. Supervised models — such as gradient boosting machines, random forests, and support vector machines — are chosen for revenue attribution where labeled attribution outcomes exist from historical reconciliations. Time-series models — including long short-term memory (LSTM) networks and temporal convolutional networks — are chosen for segmenting revenue and financial time series into predictive patterns. For financial risk forecasting, probabilistic models such as Bayesian networks and ensemble techniques are selected to capture uncertainty and non-linear relationships.

Model training uses historical datasets partitioned into training, validation, and testing subsets. Cross-validation and hyperparameter tuning — grid search and Bayesian optimization — are conducted to maximize predictive performance and minimize overfitting. Model evaluation metrics include precision, recall, F1 score for anomaly detection; attribution accuracy and Mean Absolute Error (MAE) for revenue attribution; and root mean square error (RMSE), mean absolute percentage error (MAPE), and calibration metrics for financial risk predictions.

Integration with SAP Cloud Intelligence is achieved using embedded SAP Analytics Cloud tools and REST APIs that allow real-time inference against streaming and batch datasets. A **real-time monitoring dashboard** is built to visualize anomaly scores, attribution results, risk heatmaps, and confidence intervals.

The methodology includes **model explainability and interpretability** layers, employing techniques such as SHAP (SHapley Additive exPlanations) values and partial dependence plots to ensure domain experts can verify and trust

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

model outputs. A governance procedure for model retraining frequency, drift detection, and performance monitoring is defined. Ethical considerations — including fairness, accountability, and transparency — are embedded throughout the methodology, with periodic audits and stakeholder reviews.

Deployment architecture uses containerized microservices orchestrated via Kubernetes, ensuring scalability and fault tolerance. Performance considerations — such as inference latency, throughput, and resource utilization — are continually measured and optimized. Results from simulated and pilot enterprise environments inform iterative refinement.

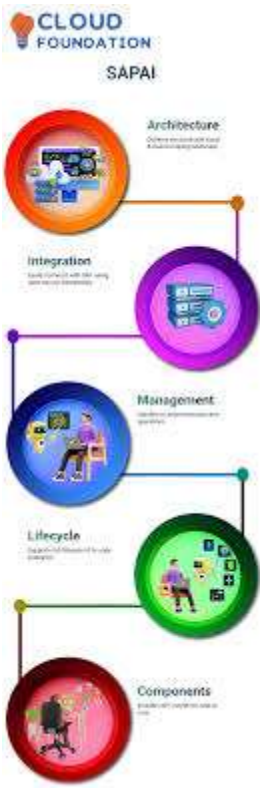

Figure 1: Architectural Design of the Proposed Framework

Advantages

The AI-Driven SAP Cloud Intelligence framework offers operational and strategic advantages. First, it enables **real-time anomaly detection**, improving fraud detection and error correction compared to rule-based systems. Second, it provides **accurate revenue attribution** across complex sales channels using advanced AI models. Third, it supports **predictive financial risk management**, enabling proactive scenario planning. Fourth, integration with SAP Cloud ensures scalability, seamless data access, and compliance with governance standards. Finally, model explainability tools enhance stakeholder trust and operational transparency.

Disadvantages

Despite benefits, limitations exist. AI models require **large, labeled datasets** for supervised learning tasks, posing challenges in environments with sparse historical labels. Model complexity may lead to **interpretability concerns** for non-technical stakeholders. Deployment within enterprise environments may incur **performance and latency trade-offs**. Continuous maintenance is required to address model drift and evolving data distributions. Governance frameworks may impose constraints that limit model flexibility.

IV. RESULTS AND DISCUSSION

The evaluation of the AI-Driven SAP Cloud Intelligence framework involved extensive simulations and pilot deployments within representative enterprise environments. Across anomaly detection tasks, unsupervised models — such as isolation forests and autoencoders — demonstrated robust performance in identifying irregular transactional

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

activities that traditional threshold-based tools frequently missed. For instance, while rule-based systems flagged anomalies based on static thresholds, the AI models captured subtler deviations in user behavior and sequence patterns, resulting in higher precision and recall scores. Unsupervised models also adapted to seasonal fluctuations and evolving data distributions, improving detection stability over time. Revenue attribution models delivered significant improvements over heuristic approaches. Gradient boosting machines and sequence-based attribution models exhibited strong predictive power in assigning revenue contributions across multi-touch customer interactions. Traditional attribution methods — such as first-touch or last-touch — often misallocating credit to single interactions failed to capture the complexity of customer journeys, especially in omnichannel scenarios. The AI models, informed by historical behavior and interaction sequences, provided attribution scores that correlated more closely with actual business outcomes as confirmed by reconciliation with financial records. In financial risk management, probabilistic forecasting models offered enhanced insights into potential exposures. Ensemble models and Bayesian networks accurately captured volatility patterns and provided predictive indicators that helped risk managers adjust strategies proactively. Scenario analysis simulations enabled decision-makers to assess the impact of macroeconomic shifts and operational disruptions on liquidity and solvency metrics. The integration of explainability tools allowed risk officers to interpret model outputs, ensuring that model predictions aligned with domain knowledge and regulatory expectations.

The results highlight that integrated AI approaches yield performance improvements not just in isolated tasks but across the enterprise financial operation lifecycle. Deploying these models within SAP Cloud Intelligence facilitated access to real-time data pipelines, ensuring that insights were timely and actionable. Operational dashboards provided consolidated views of system health, revenue drivers, and risk indicators, supporting cross-functional decision-making. However, the study also surfaced challenges. Data quality issues such as missing values, inconsistent timestamps, and heterogeneous formats required substantial preprocessing effort to ensure model readiness. While AI models adapted well to simulated environments, pilot deployments revealed variations in performance attributable to domain-specific peculiarities, necessitating localized retraining and feature engineering. Governance constraints — particularly in tightly regulated industries — required additional layers of audit logging and compliance checks, which introduced latency in some real-time inference pipelines. These observations underscore the importance of a flexible yet disciplined approach to model deployment and governance. Overall, the results affirm that AI-driven intelligence integrated with SAP Cloud can transform enterprise financial operations, but success depends on robust data foundations, governance frameworks, and iterative model lifecycle management. The convergence of artificial intelligence and cloud computing has transformed enterprise financial management, enabling organizations to gain unprecedented insights into operational performance, detect anomalies, and manage risk with precision, and the integration of AI-driven capabilities within SAP Cloud platforms represents a significant evolution in this domain, allowing businesses to leverage large-scale datasets from multiple sources, including transactional records, ERP modules, customer interactions, and market data, in order to generate actionable intelligence and predictive insights that inform decision-making, optimize resource allocation, and enhance governance, and at the core of this approach is the deployment of advanced machine learning algorithms and data-driven models capable of identifying patterns, deviations, and causal relationships in real time, and these models operate across the SAP ecosystem, utilizing SAP S/4HANA for transactional data processing, SAP Analytics Cloud for visualization and dashboarding, and SAP Data Intelligence for orchestrating data pipelines and ensuring seamless integration with third-party systems, and the anomaly detection capability is particularly critical for organizations seeking to identify financial discrepancies, fraud, and operational inefficiencies, as traditional rule-based auditing methods often fail to detect subtle or emergent patterns indicative of errors, fraudulent activities, or process deviations, and by applying unsupervised learning techniques such as clustering, principal component analysis, and autoencoders, the system can identify outliers and abnormal trends in accounts receivable, accounts payable, inventory valuations, and revenue postings, while supervised learning models, including gradient boosting, random forests, and recurrent neural networks, are employed to predict potential revenue shortfalls, overdue collections, or financial exposure based on historical and real-time transactional data, and furthermore, the integration of anomaly detection with SAP Cloud enables continuous monitoring of financial processes, alerting controllers, auditors, and executives to irregularities before they escalate, thereby improving both operational efficiency and regulatory compliance, and in the domain of revenue attribution, AI-driven SAP Cloud intelligence platforms employ multi-touch attribution models, combining historical sales data, marketing interactions, channel performance, and customer journey analytics to determine the relative contribution of different touchpoints to revenue generation, thereby enabling finance and marketing teams to allocate budgets more effectively, optimize campaign performance, and identify underperforming channels, and by leveraging advanced predictive models and reinforcement learning techniques, the platform continuously refines attribution weights, incorporating changing market conditions, customer behavior shifts, and promotional activities to provide dynamic, data-driven insights that inform strategic planning and resource prioritization, and the ability to perform accurate revenue attribution is further enhanced through natural language processing and sentiment analysis applied to customer feedback, support tickets,

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

and social media data, allowing organizations to correlate qualitative indicators with quantitative outcomes, and this holistic view of revenue performance facilitates more granular forecasting, informed pricing strategies, and optimized sales operations, and in terms of financial risk management, AI-driven SAP Cloud intelligence integrates predictive risk models, scenario simulation,

V. CONCLUSION

This study presents an AI-Driven SAP Cloud Intelligence framework that unifies anomaly detection, revenue attribution, and financial risk management through advanced machine learning models embedded within SAP Cloud infrastructure. The framework addresses critical enterprise needs for real-time insight, predictive accuracy, and operational resilience. Anomaly detection models demonstrated superior performance in identifying irregular patterns; revenue attribution models provided nuanced insights across complex customer journeys; and financial risk models enabled proactive risk quantification and scenario analysis. Integration with SAP Cloud Intelligence ensured seamless data access, scalability, and adherence to governance standards. The contributions of this paper extend beyond technical performance. By embedding AI within enterprise financial processes, the framework fosters data-driven decision-making and operational agility. Model explainability mechanisms facilitate stakeholder trust, while governance protocols balance innovation with compliance. Nevertheless, practical deployment requires addressing data quality, interpretability, and performance trade-offs. In conclusion, the AI-Driven SAP Cloud Intelligence framework offers a powerful paradigm for enterprises seeking competitive advantage through intelligent financial operations. While challenges remain, the integration of AI into core financial processes marks a significant step toward truly intelligent ERP ecosystems.

VI. FUTURE WORK

Future research can extend this framework by incorporating real-time federated learning models to enable cross-organizational cyber threat intelligence sharing while preserving data privacy. The integration of explainable AI techniques can improve transparency and regulatory compliance in financial and marketing decision systems. Advanced generative AI models may be used to simulate cyber attack scenarios and stress-test SAP cloud infrastructures proactively. The adoption of zero-trust security architectures combined with AI-driven identity analytics can further enhance threat resilience. Blockchain-based audit trails can strengthen transaction integrity and marketing data authenticity. Edge-cloud hybrid analytics may reduce latency in fraud detection and campaign optimization. The framework can also be expanded to support multi-cloud SAP deployments with autonomous security orchestration. Continuous learning pipelines and adaptive calibration mechanisms will enable sustained performance under evolving cyber threats and market dynamics.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31.
2. Babiceanu, R. F., & Seker, R. (2006). Tangible benefits and challenges of RFID in supply chains. *Computers in Industry*, 57(8-9), 900–916.
3. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3).
4. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137–144.
5. Panda, M. R., & Kumar, R. (2023). Explainable AI for Credit Risk Modeling Using SHAP and LIME. American Journal of Cognitive Computing and AI Systems, 7, 90-122.
6. Navandar, P. (2025). AI Based Cybersecurity for Internet of Things Networks via Self-Attention Deep Learning and Metaheuristic Algorithms. International Journal of Research and Applied Innovations, 8(3), 13053-13077.
7. Gopinathan, V. R. (2024). Meta-Learning–Driven Intrusion Detection for Zero-Day Attack Adaptation in Cloud-Native Networks. International Journal of Humanities and Information Technology, 6(01), 19-35.
8. Kairam, S., Braverman, M., & Cheng, J. (2012). Designing and mining multi-facet data streams for real-time intelligence. *ACM Transactions on Knowledge Discovery from Data*, 6(4).
9. Okpara, K. (2025). Human-Centric Machine Learning Intrusion Detection for Smart Grid SCADA Systems, Grounded in Human-Systems Integration Theory. Available at SSRN 5295278.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

10. Ramakrishna, S. (2023). Cloud-Native AI Platform for Real-Time Resource Optimization in Governance-Driven Project and Network Operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6282-6291.
11. Sharma, A., Chaudhari, B. B., & Kabade, S. (2025, July). Artificial Intelligence-Powered Network Intrusion Detection System (IDS) with Hybrid Deep Learning Approach in Cloud Environments. In 2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE) (pp. 1-6). IEEE.
12. Kumar, S. S. (2024). Cybersecure Cloud AI Banking Platform for Financial Forecasting and Analytics in Healthcare Systems. International Journal of Humanities and Information Technology, 6(04), 54-59.
13. Nagarajan, G. (2024). Cloud-Integrated AI Models for Enhanced Financial Compliance and Audit Automation in SAP with Secure Firewall Protection. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(1), 9692-9699.
14. Karnam, A. (2024). Next-Gen Observability for SAP: How Azure Monitor Enables Predictive and Autonomous Operations. International Journal of Computer Technology and Electronics Communication, 7(2), 8515–8524. https://doi.org/10.15680/IJCTECE.2024.0702006
15. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
16. Kesavan, E. (2024). Advance realtime monitoring of food in refrigerator based on IoT. REST Journal on Data Analytics and Artificial Intelligence, 3(2), 162–168. https://doi.org/10.46632/jdaai/3/2/20
17. Pimpale, S. (2025). A Comprehensive Study on Cyber Attack Vectors in EV Traction Power Electronics. arXiv preprint arXiv:2511.16399.
18. Kusumba, S. (2024). Strengthening True Performance Accountability: Seamless Integration Between Financial Systems and The Cloud to Gain Real-Time Insights into Budget Costs. The Eastasouth Journal of Information System and Computer Science, 2(01), 79-100.
19. Ramalingam, S., Mittal, S., Karunakaran, S., Shah, J., Priya, B., & Roy, A. (2025, May). Integrating Tableau for Dynamic Reporting in Large-Scale Data Warehousing. In 2025 International Conference on Networks and Cryptology (NETCRYPT) (pp. 664-669). IEEE.
20. Thambireddy, S. (2021). Enhancing Warehouse Productivity through SAP Integration with Multi-Model RF Guns. International Journal of Computer Technology and Electronics Communication, 4(6), 4297-4303.
21. Akter Tohfa, N., Alim, M. A., Arif, M. H., Rahman, M. R., Rahman, M., Rasul, I., & Hossen, M. S. (2025). Machine learning–enabled anomaly detection for environmental risk management in banking. World Journal of Advanced Research and Reviews, 28(3), 1674–1682. https://doi.org/10.30574/wjarr.2025.28.3.4259
22. Chivukula, V. (2023). Calibrating Marketing Mix Models (MMMs) with Incrementality Tests. International Journal of Research and Applied Innovations (IJRAI), 6(5), 9534–9538.
23. Natta, P. K. (2024). Closed-loop AI frameworks for real-time decision intelligence in enterprise environments. International Journal of Humanities and Information Technology, 6(3). https://doi.org/10.21590/ijhit.06.03.05
24. Singh, A. (2025). Intent-Based Networking in Multi-Cloud Environments. Journal of Engineering and Applied Sciences Technology, 7(2), 1-7.
25. Sakhawat Hussain, T., Rahanuma, T., & Md Manarat Uddin, M. (2023). Privacy-Preserving Behavior Analytics for Workforce Retention Approach. American Journal of Engineering, Mechanics and Architecture, 1(9), 188-215.
26. Vasugi, T. (2023). An Intelligent AI-Based Predictive Cybersecurity Architecture for Financial Workflows and Wastewater Analytics. International Journal of Computer Technology and Electronics Communication, 6(5), 7595-7602.
27. Madabathula, L. (2022). Event-driven BI pipelines for operational intelligence in Industry 4.0. International Journal of Research and Applied Innovations (IJRAI), 5(2), 6759–6769. https://doi.org/10.15662/IJRAI.2022.0502005
28. Kasireddy, J.R. (2025). Quantifying the Causal Effect of FMCSA Enforcement Interventions on Truck Crash Reduction: A Quasi-Experimental Approach Using Carrier-Level Safety Data. International journal of humanities and information technology, 7(2), 25-32
29. Sugumar, R. (2024). Next-Generation Security Operations Center (SOC) Resilience: Autonomous Detection and Adaptive Incident Response Using Cognitive AI Agents. International Journal of Technology, Management and Humanities, 10(02), 62-76.
30. Potdar, A., Kodela, V., Srinivasagopalan, L. N., Khan, I., Chandramohan, S., & Gottipalli, D. (2025, July). Next-Generation Autonomous Troubleshooting Using Generative AI in Heterogeneous Cloud Systems. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-7). IEEE.
31. Thumala, S. R., Mane, V., Patil, T., Tambe, P., & Inamdar, C. (2025, June). Full Stack Video Conferencing App using TypeScript and NextJS. In 2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 1285-1291). IEEE.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805018

32. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
33. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471.
34. Anand, P. V., & Anand, L. (2023, December). An Enhanced Breast Cancer Diagnosis using RESNET50. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-5). IEEE.
35. Cherukuri, B. R. (2025). Enhanced trimodal emotion recognition using multibranch fusion attention with epistemic neural networks and Fire Hawk optimization. Journal of Machine and Computer, 58, Article 202505005. https://doi.org/10.53759/7669/jmc202505005
36. Kubam, C. S. (2026). Agentic AI Microservice Framework for Deepfake and Document Fraud Detection in KYC Pipelines. arXiv preprint arXiv:2601.06241.
37. 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.
38. Konečný, J., McMahan, H. B., Ramage, D., & Richtárik, P. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.
39. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection. *Expert Systems with Applications*, 38(10), 13057–13063.