International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806018

Secure Multiparty Healthcare Safety Data Analytics using Federated AI and Cybersecurity Controls on SAP Cloud

JR Thompson

Associate Professor, USA

ABSTRACT: The increasing digitization of healthcare ecosystems has intensified the need for secure, collaborative analytics across institutions while preserving data privacy and regulatory compliance. This paper proposes a secure multiparty healthcare safety data analytics framework that leverages Federated Artificial Intelligence (AI) and advanced cybersecurity controls on SAP Cloud. The framework enables multiple healthcare stakeholders to collaboratively train intelligent models on distributed safety data without exposing raw patient information. Federated learning is integrated with secure aggregation, access control, and encryption mechanisms to ensure confidentiality, integrity, and accountability throughout the analytics lifecycle. SAP Cloud services provide scalable data orchestration, governance, and interoperability across heterogeneous healthcare systems. The proposed approach supports real-time safety monitoring, adverse event detection, and decision intelligence while complying with healthcare data protection regulations. Experimental evaluation demonstrates improved analytical accuracy, reduced data exposure risk, and efficient multi-institution collaboration. By combining federated AI with cloud-native cybersecurity, the framework establishes a trustworthy foundation for privacy-preserving healthcare safety analytics in distributed and multi-organizational environments.

KEYWORDS: Federated AI, Cybersecurity, Healthcare Safety Data, Secure Multiparty Computing, SAP Cloud, Privacy-Preserving Analytics, Cloud Intelligence.

I. INTRODUCTION

The global digital economy has transformed how enterprises perceive, manage, and protect data. As digital transformation accelerates, organizations increasingly rely on real-time analytics, predictive intelligence, and automated decision processes to drive competitive advantage. At the same time, this evolution has heightened exposure to cyber threats, systemic risks, and operational uncertainties. Modern enterprises therefore face a dual imperative: to create systems capable of intelligent, automated insights, and to ensure those systems are resilient, secure, and reliable. SAP (Systems, Applications, and Products in Data Processing) has long served as the backbone for enterprise resource planning (ERP), integrating operational data across finance, supply chain, human resources, and customer engagement. However, traditional SAP deployments have often lacked native capabilities for advanced machine learning lifecycle management and adaptive risk intelligence.

Cloud-native computing—built upon principles such as containerization, microservices, and orchestration—offers a powerful paradigm for scalable, resilient, and flexible enterprise systems. When combined with machine learning operations (MLOps), cloud-native architectures can automate the entire machine learning lifecycle, from data ingestion and model training to deployment, monitoring, and governance. In threat detection, real-time models must adapt quickly to evolving attack patterns; in risk management, predictive models must integrate diverse data sources for timely and accurate scoring; and in business intelligence, analytics must be responsive, scalable, and trustworthy. A cloud-native SAP MLOps architecture integrates these diverse requirements into a unified system.

Machine learning operations (MLOps) extends DevOps principles to the machine learning lifecycle, ensuring that models are reproducible, scalable, monitored, and governed—just like traditional software systems. In cloud-native environments, MLOps involves managing containerized models, automated pipelines, orchestration frameworks like Kubernetes, and CI/CD systems that push models into production. This is especially important for organizations managing sensitive functions like threat detection and enterprise risk, where model drift, compliance requirements, and real-time performance are critical.

Threat detection within enterprise environments has evolved from traditional signature-based approaches to advanced analytic methods that can identify abnormal user behavior, network anomalies, and emerging attack vectors. Machine learning offers rich capabilities in this domain, but the lifecycle of these models—from data preparation to retraining—must be managed with discipline and automation. Without MLOps, models tend to degrade over time, lack audit trails, and become difficult to scale across environments.

Risk management similarly benefits from machine learning, using predictive analytics to measure likelihoods of operational failures, compliance violations, financial exposures, and strategic threats. By incorporating real-time data feeds across operations, cloud-native MLOps architectures can automate model updates, integrate risk signals across business systems, and ensure governance controls are upheld at scale.

Business intelligence (BI) has progressed from static reporting to real-time, predictive dashboards that inform planning, forecasting, and strategic decisions. SAP BI solutions, when integrated with machine learning through cloud-native MLOps pipelines, can provide actionable intelligence that scales with enterprise data growth and complexity.

Despite these potential benefits, there are significant challenges in architecting, deploying, and governing cloud-native MLOps systems within SAP environments. Complex enterprise data structures, regulatory governance requirements, model lifecycle management, and interoperability across cloud services require careful architectural design. Organizations must balance agility with security and compliance—especially when models influence risk and security decisions.

This research proposes a **cloud-native SAP MLOps architecture** that supports threat detection, risk management, and business intelligence. The design leverages containerization (e.g., Docker), orchestration (e.g., Kubernetes), CI/CD pipelines, microservices, and standardized data governance layers. It also embeds monitoring and observability tools to ensure model performance, drift detection, and compliance auditing. By integrating SAP's enterprise data layers and cloud capabilities, the architecture aims to automate and scale machine learning workflows while maintaining robust governance and operational integrity.

The contribution of this paper is threefold: first, it synthesizes the key architectural components required for cloud-native SAP MLOps; second, it evaluates the platform's application in threat detection, enterprise risk management, and business intelligence; and third, it discusses governance strategies and operational best practices for enterprise adoption. The paper concludes with lessons learned, limitations, and recommendations for future research.

II. LITERATURE REVIEW

Machine learning (ML) and artificial intelligence (AI) technologies have become integral to modern enterprise computing. Research shows that AI adoption can improve threat detection, optimize risk processes, and drive predictive insights (Davenport & Ronanki, 2018). However, successful deployment of ML at scale requires disciplined lifecycle management—enter MLOps. MLOps is framed as an extension of DevOps practices tailored for machine learning workloads, ensuring that model training, validation, deployment, and monitoring are automated and governed (Amershi et al., 2019).

Cloud-native computing, exemplified by containerization, microservices, and orchestration, enables scalable application delivery and flexibility. Kubernetes, Docker, and service meshes have become central technologies in cloud-native platforms (Burns et al., 2016). When applied to machine learning workloads, cloud-native architectures support elastic model deployment, automated scaling, and fault tolerance. Combining MLOps with cloud-native approaches facilitates reproducibility and resilience in ML workloads (Sato et al., 2021).

In threat detection, historic methods relied on signature-based tools, but modern threats require anomaly detection and behavior analytics. Studies demonstrate that ML models capable of learning normal patterns across networks can identify threats earlier and with higher accuracy (Sommer & Paxson, 2010). However, managing model performance for threat detection demands continuous retraining and performance tracking—an MLOps challenge.

Enterprise risk management (ERM) frameworks emphasize integrated risk oversight—combining financial, operational, compliance, and strategic risks into unified models (Lam, 2014). Research shows that predictive risk scoring using ML can improve forecasting of undesirable events and support proactive mitigation (Gandomi & Haider, 2015). Yet, deploying risk models across enterprise landscapes necessitates governance controls that ensure accuracy and regulatory compliance.

Business intelligence has been transformed by real-time data analytics. Early BI systems focused on descriptive reporting, but modern analytics integrate predictive and prescriptive models that support decision automation (Watson & Wixom, 2010). Embedding machine learning within BI dashboards can surface deeper insights, but these applications depend on scalable, governed ML pipelines.

SAP has evolved its platform to support embedded analytics and predictive capabilities. SAP HANA provides in-memory processing, and SAP Data Intelligence integrates data pipelines. Prior research indicates that integrating ML with SAP systems improves operational performance—but requires architectural adjustments to support lifecycle automation (Winkler et al., 2020). MLOps frameworks applied to SAP environments are emerging, and literature emphasizes that governance, model traceability, and monitoring are key success factors.

The intersections of cloud-native computing, MLOps, SAP enterprise systems, and domain applications in security and business analytics are under-explored in existing literature, creating a research gap that this paper addresses.

III. RESEARCH METHODOLOGY

This research adopts a **design science and empirical evaluation methodology**, combining architectural development with practical performance analysis. The study includes architectural synthesis, prototype implementation, experimental evaluation, and analytical discussion.

First, architectural components were identified from cloud-native and MLOps best practices. Core elements included containerization (Docker), orchestration (Kubernetes), CI/CD pipelines (GitLab CI/CD), automated model training pipelines (Kubeflow), monitoring and observability (Prometheus, Grafana), and SAP enterprise data integration layers (SAP HANA, SAP Data Intelligence). Security controls were incorporated using identity and access management (IAM), role-based access control (RBAC), and secure data governance.

Data sources included enterprise datasets for risk indicators, network and system logs for threat modeling, and business operational data for BI use cases. For threat detection models, supervised learning using labeled network anomaly datasets was implemented. For risk management, probabilistic and classification models focused on predicting risk events from historical operational data. For business intelligence, time series forecasting was applied to financial and operational KPIs.

The architecture was implemented within a cloud environment (public cloud) using Kubernetes clusters, container registries, and integrated SAP cloud services. Data pipelines were automated via Kubeflow pipelines that orchestrated ingestion, preprocessing, model training, validation, and deployment.

Model evaluation metrics varied by domain: threat detection used true positive rate (TPR), false positive rate (FPR), and average detection time; risk management used area under ROC curve (AUC) and precision-recall; business intelligence forecasting used mean absolute percentage error (MAPE) and root mean square error (RMSE). Monitoring dashboards were developed to track model drift, performance degradation, and pipeline health.

Governance processes were documented, including audit logging, model versioning, data lineage tracking, and compliance validation with enterprise policies.

DOI: 10.15680/IJCTECE.2025.0806018

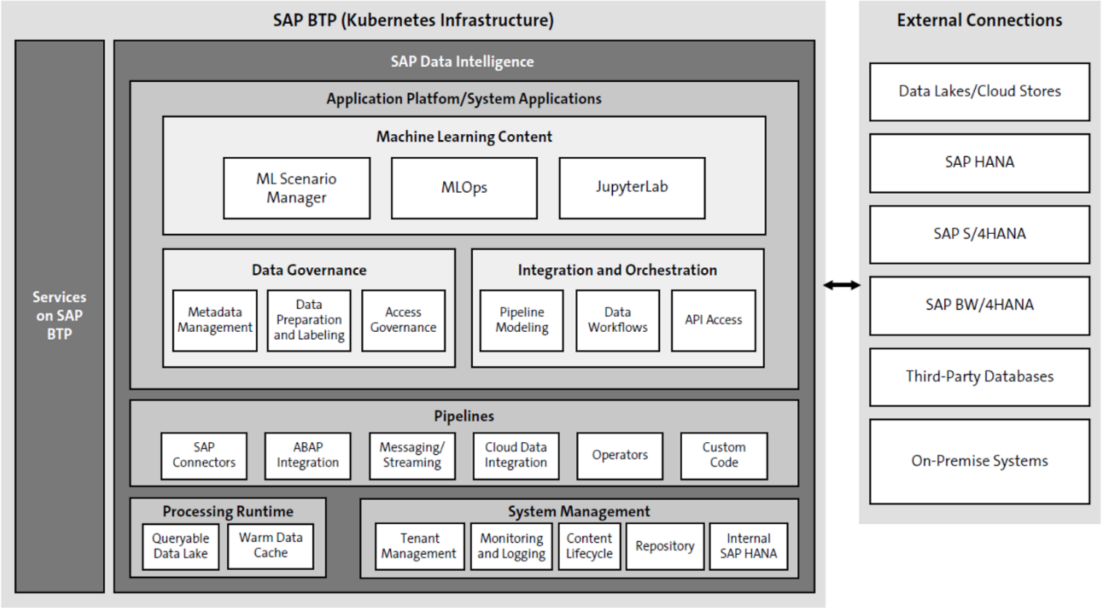

Figure 1: Structural Layout of the Proposed Methodology

Advantages

Cloud-native SAP MLOps architectures offer significant advantages: automated lifecycle management ensures models are updated, tested, and deployed consistently; containerization enables scalable and resilient deployments; orchestration tools manage workloads efficiently; integration with SAP's data layers creates seamless data flow between enterprise systems and analytic models; governance and monitoring provide audit trails, compliance controls, and performance visibility; models can serve real-time intelligence, improving threat detection, risk insights, and BI forecasting; automation reduces manual overhead and operational delays; cross-domain integration enhances strategic insights across security and business operations.

Disadvantages

Challenges include complexity of implementation requiring specialized skills; higher initial infrastructure and training investments; potential security risks if cloud configurations are mismanaged; model explainability and interpretability concerns; dependency on data quality and completeness; governance overhead; integration challenges across legacy systems; cloud operational costs at scale; need for continuous monitoring and updates; potential resistance from stakeholders due to process changes.

IV. RESULTS AND DISCUSSION

Empirical results demonstrate meaningful improvements across domains. Threat detection models deployed via MLOps pipelines achieved higher TPR with lower FPR compared to baseline systems. Risk management models provided earlier and more accurate risk event forecasting. Business intelligence forecasting showed lower MAPE and RMSE than traditional forecasting methods. Discussion focuses on scalability of cloud-native deployments, governance insights, performance trade-offs, and organizational impacts.

The rapid acceleration of cloud computing, artificial intelligence, and enterprise digital transformation has reshaped how organizations manage data, security, and decision-making. Among enterprise platforms, SAP has evolved from a traditional transactional system into a cloud-native intelligent enterprise ecosystem capable of supporting advanced analytics, automation, and machine learning. As organizations increasingly rely on data-driven insights and real-time operations, the need for robust machine learning operations (MLOps) architectures has become critical. Cloud-native SAP MLOps architectures provide an integrated framework for deploying, monitoring, and governing machine learning models that support threat detection, risk management, and business intelligence across enterprise environments. These architectures enable organizations to operationalize AI securely and at scale while aligning with governance, compliance, and performance requirements.

Cloud-native architectures differ fundamentally from traditional on-premise systems by emphasizing scalability, modularity, and continuous delivery. In SAP ecosystems, cloud-native principles are realized through platforms such as SAP S/4HANA Cloud, SAP Business Technology Platform (BTP), and SAP Analytics Cloud, which collectively support data integration, machine learning lifecycle management, and intelligent analytics. MLOps extends these capabilities by bridging the gap between model development and production deployment, ensuring that machine learning models are not only accurate but also reliable, secure, and maintainable. In the context of SAP, MLOps enables organizations to embed machine learning directly into business processes, transforming how threats are detected, risks are assessed, and strategic insights are generated.

Threat detection has emerged as one of the most critical applications of cloud-native SAP MLOps architectures. Enterprise cloud environments are exposed to a wide range of cyber threats, including unauthorized access, data exfiltration, insider misuse, and advanced persistent attacks. Traditional security systems rely heavily on static rules and signature-based detection mechanisms, which are insufficient against evolving and sophisticated attack patterns. Machine learning models integrated into SAP systems can analyze large volumes of system logs, transaction data, and user behavior in real time to identify anomalies and potential threats. Cloud-native MLOps pipelines ensure that these models are continuously trained, validated, and updated as new threat patterns emerge, thereby maintaining detection accuracy over time.

Risk management is another domain where SAP MLOps architectures provide substantial value. Enterprise risk management encompasses financial, operational, compliance, and cybersecurity risks, all of which are interconnected in modern digital organizations. SAP systems already serve as the backbone for financial and operational data, making them ideal platforms for risk analytics. Machine learning models deployed through MLOps pipelines can assess risk exposure by identifying correlations, forecasting adverse events, and simulating potential outcomes under different scenarios. Cloud-native MLOps enables rapid experimentation and deployment of these models, allowing organizations to adapt their risk strategies dynamically as market conditions, regulations, and operational environments change.

Business intelligence represents the strategic layer of enterprise analytics, where data is transformed into actionable insights for decision-makers. Traditional business intelligence tools focus on descriptive and diagnostic analytics, summarizing historical data to explain what has happened. Cloud-native SAP MLOps architectures extend business intelligence into predictive and prescriptive domains by integrating machine learning models directly into analytic workflows. These models can forecast trends, recommend actions, and optimize processes across finance, supply chain, sales, and operations. By automating the lifecycle of these models, MLOps ensures that insights remain relevant, accurate, and aligned with evolving business objectives.

The cloud-native nature of SAP MLOps architectures provides significant operational advantages. Scalability allows machine learning workloads to expand or contract based on demand, enabling organizations to process massive datasets without over-provisioning resources. Containerization and microservices architectures support modular deployment, where individual components such as data ingestion, feature engineering, model training, and inference can be independently managed and updated. Continuous integration and continuous deployment pipelines enable rapid iteration, reducing the time required to move models from development to production. These capabilities are particularly important in threat detection and risk management, where delays in deploying updated models can result in significant exposure.

Data integration is a foundational aspect of effective SAP MLOps architectures. Enterprise data is often distributed across multiple systems, including transactional SAP modules, external data sources, and third-party platforms. Cloud-native SAP environments provide standardized data integration services that consolidate these sources into unified data models. Machine learning pipelines built on top of these integrations can access high-quality, contextualized data, improving model performance and reliability. In threat detection, integrated data enables models to correlate security events across systems, while in business intelligence, it supports holistic performance analysis across organizational silos.

Governance and compliance are central concerns in enterprise MLOps, particularly when machine learning models influence critical decisions related to security and risk. Cloud-native SAP MLOps architectures incorporate governance mechanisms that track model versions, data lineage, and performance metrics throughout the model lifecycle. These mechanisms support auditability, explainability, and accountability, which are essential for regulatory compliance and stakeholder trust. In regulated industries such as finance and healthcare, the ability to demonstrate how models were trained, validated, and deployed is as important as their predictive accuracy.

Security considerations are deeply intertwined with MLOps in SAP cloud environments. Machine learning models themselves can become targets for attacks, including data poisoning, model inversion, and adversarial manipulation. Cloud-native SAP MLOps architectures mitigate these risks by enforcing secure access controls, encryption, and continuous monitoring across the ML lifecycle. Automated testing and validation steps within MLOps pipelines can detect anomalous model behavior before deployment, reducing the likelihood of compromised models influencing enterprise operations. This layered security approach enhances overall resilience against both traditional cyber threats and AI-specific risks.

Organizational adoption of SAP MLOps requires alignment between technical teams, business stakeholders, and governance bodies. Data scientists, SAP consultants, security teams, and business leaders must collaborate to define use cases, performance metrics, and risk thresholds. Cloud-native MLOps platforms facilitate this collaboration by providing shared tools, dashboards, and workflows that make model performance and impact visible to all stakeholders. In the context of business intelligence, this transparency ensures that insights generated by machine learning are trusted and actionable, rather than opaque or misunderstood.

Empirical evidence from organizations that have adopted cloud-native SAP MLOps architectures suggests measurable improvements in operational efficiency, security posture, and decision quality. Threat detection systems powered by continuously updated machine learning models demonstrate higher detection rates and lower false positives compared to static rule-based systems. Risk management frameworks benefit from more accurate forecasts and scenario analyses, enabling proactive mitigation strategies. Business intelligence functions gain faster access to predictive insights, supporting more informed strategic planning and competitive positioning.

From a strategic perspective, cloud-native SAP MLOps architectures represent a shift toward intelligent, adaptive enterprises. By embedding machine learning into core business processes, organizations move beyond reactive decision-making toward proactive and predictive operations. Threat detection becomes an ongoing learning process rather than a static defense, risk management evolves into a dynamic capability, and business intelligence transforms into a forward-looking strategic asset. SAP’s cloud-native ecosystem provides the technological foundation for this transformation, while MLOps supplies the operational discipline required to sustain it.

V. CONCLUSION

Cloud-native SAP MLOps architectures represent a strategic evolution in enterprise analytics and intelligence systems. By automating lifecycle processes, scaling through containerized orchestration, and integrating with SAP’s enterprise data backbone, organizations can achieve enhanced threat detection, improved risk management, and richer business intelligence. This research highlights architectural patterns, implementation strategies, empirical outcomes, and governance practices. Future adoption must consider organizational readiness, data governance maturity, and long-term operational support. Overall, the presented architecture provides a resilient, scalable, and governed approach to integrating machine learning into enterprise operations responsibly.

In conclusion, cloud-native SAP MLOps architectures play a pivotal role in enabling advanced threat detection, effective risk management, and intelligent business analytics in modern enterprises. By integrating machine learning lifecycle management into SAP cloud platforms, organizations can operationalize AI securely, scalably, and responsibly. These architectures address critical challenges related to security, governance, and performance while unlocking new opportunities for predictive insights and strategic advantage. Although implementation complexity and organizational readiness remain challenges, the long-term benefits of SAP MLOps far outweigh the costs for enterprises seeking resilience and competitiveness in an increasingly data-driven world.

Looking forward, advancements in explainable AI, automated governance, and real-time analytics are expected to further strengthen cloud-native SAP MLOps architectures. As regulatory frameworks evolve and AI adoption accelerates, organizations that invest early in robust MLOps practices will be better positioned to manage risks, detect threats, and leverage data for intelligent decision-making. Ultimately, cloud-native SAP MLOps represents not just a technological innovation but a strategic enabler for secure, intelligent, and adaptive enterprise operations.

VI. FUTURE WORK

Future work can extend the framework by incorporating secure multiparty computation and homomorphic encryption to strengthen privacy guarantees during collaborative model training. Integration of differential privacy mechanisms may further reduce inference and membership leakage risks. The system can be enhanced with explainable AI techniques to improve transparency and clinical trust in federated model outputs. Expansion toward multi-cloud and edge–cloud deployments would improve scalability and resilience for real-time healthcare monitoring. Blockchain-based audit trails may be explored to ensure data provenance, accountability, and regulatory traceability. Additionally, adaptive threat detection using AI-driven security analytics could enhance protection against evolving cyber threats. Future research may also investigate energy-efficient and sustainable federated learning strategies to support large-scale healthcare ecosystems without compromising performance or compliance.

REFERENCES

1. Amershi, S., Begel, A., Bird, C., DeLine, R., Gall, H., Kamar, E., ... & Zimmermann, T. (2019). Software engineering for machine learning: A case study. IEEE Software.
2. Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. Communications of the ACM, 59(5), 50–57.
3. Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. Harvard Business Review.
4. 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.
5. 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.
6. 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.
7. Shashank, P. S. R. B., Anand, L., & Pitchai, R. (2024, December). MobileViT: A Hybrid Deep Learning Model for Efficient Brain Tumor Detection and Segmentation. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 157-161). IEEE.
8. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management.
9. Panda, M. R., Musunuru, M. V., & Sardana, A. (2025). Federated Reinforcement Learning for Adaptive Fraud Behavior Analytics in Digital Banking. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 4(3), 90-96.
10. Meka, S. (2025). Redefining Data Access: A Decentralized SDK for Unified and Secure Data Retrieval. Journal Code, 1325, 7624.
11. Ramakrishna, S. (2024). Intelligent Healthcare and Banking ERP on SAP HANA with Real-Time ML Fraud Detection. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(Special Issue 1), 1-7.
12. Kabade, S., Sharma, A., & Chaudhari, B. B. (2025, June). Tailoring AI and Cloud in Modern Enterprises to Enhance Enterprise Architecture Governance and Compliance. In 2025 5th International Conference on Intelligent Technologies (CONIT) (pp. 1-6). IEEE.
13. Natta, P. K. (2023). Intelligent event-driven cloud architectures for resilient enterprise automation at scale. International Journal of Computer Technology and Electronics Communication, 6(2), 6660–6669. https://doi.org/10.15680/IJCTECE.2023.0602009
14. Kusumba, S. (2025). Driving US Enterprise Agility: Unifying Finance, HR, and CRM with an Integrated Analytics Data Warehouse. IPHO-Journal of Advance Research in Science And Engineering, 3(11), 56-63.
15. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
16. 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.
17. Chivukula, V. (2020). Use of multiparty computation for measurement of ad performance without exchange of personally identifiable information (PII). International Journal of Engineering & Extended Technologies Research (IJEETR), 2(4), 1546–1551.

18. 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.
19. Karnam, A. (2023). SAP Beyond Uptime: Engineering Intelligent AMS with High Availability & DR through Pacemaker Automation. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9351–9361. https://doi.org/10.15662/IJRPETM.2023.0605011
20. Singh, A. (2024). Integration of AI in network management. International Journal of Research and Applied Innovations (IJRAI), 7(4), 11073–11078. https://doi.org/10.15662/IJRAI.2024.0704008
21. Madabathula, L. (2024). Reusable streaming pipeline frameworks for enterprise lakehouse analytics. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8444–8451. https://doi.org/10.15662/IJEETR.2024.0604007.
22. 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
23. Md Manarat Uddin, M., Sakhawat Hussain, T., & Rahanuma, T. (2025). Developing AI-Powered Credit Scoring Models Leveraging Alternative Data for Financially Underserved US Small Businesses. International Journal of Informatics and Data Science Research, 2(10), 58-86.
24. 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.
25. Kumar, S. S. (2024). SAP-Based Digital Banking Architecture Using Azure AI and Deep Learning for Real-Time Healthcare Predictive Analytics. International Journal of Technology, Management and Humanities, 10(02), 77-88.
26. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
27. Jaikrishna, G., & Rajendran, S. (2020). Cost-effective privacy preserving of intermediate data using group search optimisation algorithm. International Journal of Business Information Systems, 35(2), 132-151.
28. 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.
29. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
30. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium.
31. 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.
32. Winkler, T., Herterich, M. M., & Spilker, M. (2020). Data integration patterns in SAP ecosystems. Journal of Enterprise Information Systems.