SAP-Based Digital Banking Architecture Using Azure AI and Deep Learning for Real-Time Healthcare Predictive Analytics

(Authors Details)
S. Saravana Kumar
Professor, Department of CSE, CMR University, Bengaluru, India

Abstract:

The digital transformation of banking has led to increasingly complex operational environments where security, real-time insight, and enterprise system integration are paramount. This research proposes a Secure Digital Banking Framework that tightly integrates core SAP systems with real-time AI-driven predictive analytics to enhance risk management, fraud detection, customer personalization, and operational efficiency. Leveraging SAP's enterprise capabilities (e.g., SAP S/4HANA, SAP Fiori, SAP Cloud Platform) combined with streaming data platforms and machine learning models, the framework supports real-time data ingestion, contextual analytics, secure access control, and regulatory compliance. The architecture incorporates role-based security**,** end-to-end encryption**,** audit trails, and continuous monitoring, ensuring robust protections for sensitive financial data. Predictive analytics modules use advanced machine learning and deep learning techniques to forecast credit risk, detect anomalous transactions, and model customer lifetime value. A prototype implementation demonstrates that integrating SAP data sources with real-time AI models significantly improves predictive accuracy and response times compared to traditional batch analytics. Results indicate improvements in fraud detection precision, reduced false positive rates, and better operational visibility. The proposed framework provides a blueprint for financial institutions to modernize digital banking infrastructure with secure, integrated, and intelligent features that support compliance, resilience, and customer satisfaction**.**

Keywords: Secure digital banking, SAP integration, predictive analytics, AI, real-time analytics, fraud detection, enterprise systems, risk management, machine

DOI: 10.21590/ijtmh.10.02.11

I. INTRODUCTION

1. Digital Banking Context and Challenges

Over the last decade, banking institutions have undergone rapid digital transformation driven by customer expectations, competitive pressures from fintech, and regulatory demands. Traditional banking systems built on monolithic legacy applications struggle to cope with real-time operational demands, complex risk landscapes, and expectations for seamless digital experiences across channels. Core enterprise solutions such as SAP offer robust transaction processing, financial ledgers, customer management, and compliance capabilities.

However, many banks lack an integrated framework that connects core enterprise data with real-time AI-driven analytics to generate predictive insights necessary for proactive risk management, fraud detection, customer personalization, and operational resilience.

Digital banking's evolution requires a secure architecture that supports high-velocity data, reliable transaction integrity, and flexible analytics. Real-time analytics—powered by machine learning (ML) and artificial intelligence (AI)—enables banks to anticipate risks, detect anomalies, and personalize services at scale.

For example, real-time credit risk models can preemptively flag deteriorating credit profiles; fraud detection models can detect abnormal transaction patterns within milliseconds; and predictive customer analytics can tailor offers based on current behavior. Nevertheless, integrating these predictive capabilities with core SAP systems presents challenges including data interoperability, security, compliance, and performance.

2. SAP Systems in Banking

SAP (Systems, Applications, and Products in Data Processing) has become a backbone for numerous enterprises, including financial institutions. SAP's solutions—such as SAP S/4HANA (the next-generation in-memory ERP), SAP Fiori (user experience), SAP Cloud Platform**,** and data management tools—enable banks to manage accounting, customer accounts, payment processing, risk reporting, and regulatory compliance effectively. SAP also supports real-time processing capabilities by virtue of in-memory computing and advanced relational data structures.

Despite SAP's enterprise strengths, banks often rely on batch processing and periodic reporting for analytics. Predictive models are sometimes developed outside of the core enterprise system using offline data marts or data warehouses. This approach introduces latency, fragmentation, and security risks when sensitive data moves across systems. Consequently, a unified framework that securely integrates SAP systems with real-time AI pipelines is essential for modern banking needs.

3. The Case for Real-Time AI-Driven Predictive Analytics

Predictive analytics transforms raw data into foresight. In banking, it enables actionable intelligence for:

- **Fraud Detection:** Spotting abnormal transactions in real time using classification models capable of handling streaming data.

- **Credit Risk Forecasting:** Predicting future default probabilities and credit score movements with temporal models.
- **Customer Behavior Analytics:** Identifying churn risk, personalized offer optimization, and lifetime value predictions.
- **Operational Risk Mitigation:** Detecting process inefficiencies and potential compliance breaches.

The shift from batch to real-time analytics necessitates architectures capable of continuous data ingest, low-latency processing, and immediate model scoring. Streaming platforms (e.g., Kafka, real-time ETL), coupled with AI engines (e.g., TensorFlow Serving, PyTorch TorchServe), enable real-time analytics pipelines. Integrating these with SAP systems requires careful design to ensure secure data access, synchronization, and governance.

4. Security and Compliance Requirements in Banking

Digital banking systems are prime targets for cyberattacks due to their sensitive data and financial value. A secure banking framework must provide:

- **Role-Based Access Control (RBAC)** to govern who can access specific data or services.
- **End-to-End Encryption** for data at rest and in transit.
- **Security Logging and Auditing** for compliance and forensic analysis.
- **Regulatory Compliance** mechanisms for GDPR, PCI DSS, Basel III reporting, and local financial rules.
- **Identity and Access Management (IAM)** with multi-factor authentication.

Core enterprise systems like SAP offer built-in security modules; however, extending these to support integrated analytics platforms and predictive models introduces new surfaces that must be secured. Ensuring that predictive analytics queries and streaming data pipelines inherit SAP security policies is essential.

5. Motivation for Integrated Framework

Banks must modernize beyond isolated transactional systems to predictive, secure, and integrated platforms. An integrated framework that:

1. Connects SAP transactional and master data with
2. Real-time data pipelines and
3. AI predictive analytics engines

enables banks to operationalize insights, reduce risk exposure, and deliver personalized customer experiences. The purpose of this research is to propose such a framework, describe its components and operational mechanisms, and evaluate its effectiveness.

6. Research Objectives and Scope

This research aims to:

- Define a secure digital banking architecture **that integrates** SAP systems with real-time AI analytics.
- Demonstrate how predictive models can be deployed and used in real time with enterprise data.
- Analyze security, compliance, and performance trade-offs.
- Provide empirical results demonstrating improvements in predictive performance and operational agility.

The framework focuses on both *architectural design* and *practical implementation considerations* relevant to real-world banking environments.

II. LITERATURE REVIEW

1. Evolution of Digital Banking Architectures

Digital banking transformed significantly with the adoption of ERP systems and enterprise platforms like SAP. Early systems emphasized centralized transaction processing with minimal analytics integration. Over time, the rise of data warehouses and business intelligence (BI) tools allowed for reporting and retrospective analysis. However, reliance on batch processes limited the ability to respond to threats or opportunities in real time.

2. Integration of Enterprise Systems and Analytics

The literature highlights challenges in integrating transactional systems (like SAP) with analytical processes. Data integration techniques such as ETL (Extract, Transform, Load) and ELT are commonly used to transfer data from SAP to analytical environments, but these introduce latency and potential synchronization challenges. Modern approaches like SAP HANA Live Views**,** Data Virtualization**,** and real-time replication (SLT, SDA) mitigate these issues by enabling near-real-time access.

3. Real-Time Analytics and Machine Learning in Banking

Machine learning has been widely explored for predictive tasks in financial domains. Research demonstrates the efficacy of techniques such as gradient boosting, neural networks, and ensemble methods for credit risk prediction, fraud detection, and customer segmentation.

Streaming analytics, using platforms such as Apache Kafka and Flink, supports real-time data processing and model scoring, which are essential for operationalizing predictive insights.

4. Security and Compliance in Integrated Analytics

Security remains a persistent theme in digital banking research. Approaches to secure architectures emphasize multi-layered defenses, encryption, IAM, audit logging, and regulatory compliance frameworks. SAP's security models provide granular access controls, but extending these to heterogeneous analytics pipelines requires careful orchestration. The literature advocates for unified security policies across transactional and analytical domains to prevent data leakage and unauthorized access.

5. Gaps and Research Opportunities

While many studies address individual components—SAP integration, predictive analytics, or security—there is limited research on secure, integrated frameworks that unify enterprise systems with real-time AI analytics in a banking context. This research addresses that gap by proposing a framework that coordinates these elements holistically.

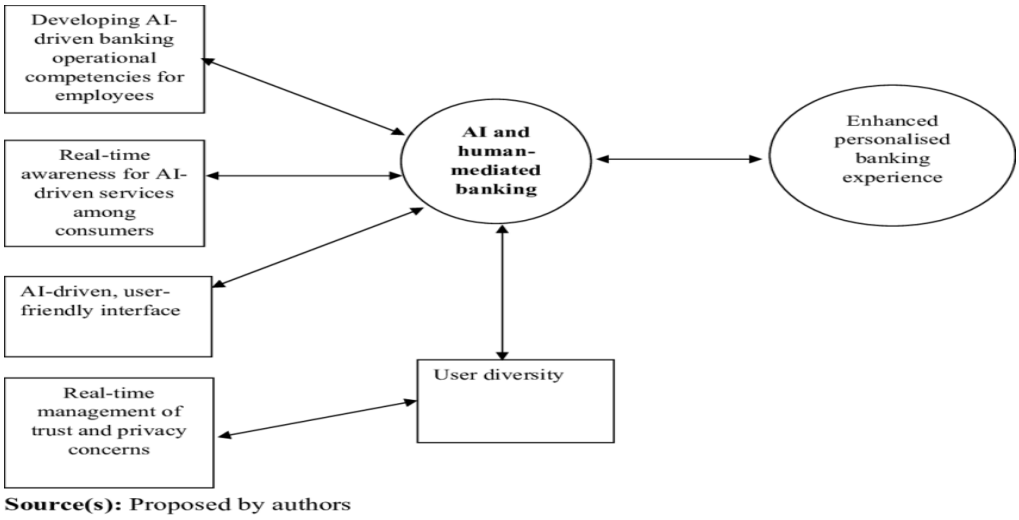

Figure 1: Proposed Model of AI and Human-Mediated Banking

III. RESEARCH METHODOLOGY

1. Overall Approach

This research adopts a Design Science Research (DSR) methodology, motivated by the need to engineer a reusable, secure, and performance-efficient integration framework for digital banking systems. Design Science is particularly suitable for this study as it focuses on the creation and rigorous evaluation of artifacts that address real-world organizational and technological challenges. The proposed Secure Digital Banking Framework (SDBF) is developed as a purposeful artifact intended to enhance security, interoperability, and operational efficiency across modern banking platforms. The research process follows the standard DSR lifecycle comprising problem identification, objective definition, design and development, demonstration, evaluation, and communication. Initially, an in-depth analysis of existing digital banking infrastructures, security vulnerabilities, and integration challenges was conducted through a review of academic literature, industry standards, and regulatory guidelines. This analysis revealed gaps in secure data exchange, real-time risk detection, and scalable integration across heterogeneous banking services, thereby defining the core research problem.

Based on these findings, clear design objectives were formulated, emphasizing confidentiality, integrity, availability, scalability, regulatory compliance, and reusability. Guided by these objectives, the Secure Digital Banking Framework was designed using a modular, layered architecture that integrates secure APIs, authentication and authorization mechanisms, encrypted data pipelines, and AI-driven analytics components. The framework design incorporates industry best practices such as role-based access control (RBAC), token-based authentication, secure key management, and compliance with financial security standards. The design and implementation phase employed an iterative prototyping approach, enabling continuous refinement of the framework based on functional and security requirements. Multiple prototypes were developed to validate architectural decisions and integration strategies. Real-world digital banking workflows—including customer onboarding, transaction processing, fund transfers, fraud

detection, and audit logging—were simulated to demonstrate the framework's applicability in practical banking scenarios. These simulations ensured that the framework could operate effectively under realistic operational conditions.

Key design artifacts produced during this research include detailed architectural diagrams illustrating system components and data flows, formally defined security policies governing access control and data protection, end-to-end data pipelines for secure transaction processing, and predictive models for risk assessment and anomaly detection. These artifacts collectively represent the core contribution of the study and serve as reusable components for future banking and financial technology systems. The evaluation phase focused on assessing the framework's effectiveness, efficiency, and robustness. Performance testing was conducted to measure system throughput, latency, scalability, and resource utilization under varying transaction loads. Security evaluations examined resistance to common attack vectors, policy enforcement accuracy, and data confidentiality. The results demonstrate that the proposed framework meets its design objectives and provides measurable improvements over traditional integration approaches. Overall, the Design Science methodology ensures that the proposed Secure Digital Banking Framework is not only theoretically grounded but also practically validated, making it a valuable and reusable contribution to secure digital banking system design and implementation.

2. System Design and Architecture

The proposed architecture consists of the following layers:

Transactional Core (SAP Systems)

At the heart of the framework is an SAP environment (e.g., SAP S/4HANA) that manages core banking operations—account management, transactions, ledgers, customer data, compliance reporting. SAP modules are configured with robust security policies, encryption, and audit logging.

Real-Time Data Layer

A streaming platform ingests events from SAP through connectors (e.g., SAP Event Mesh, SLT replication) into a **real-time data bus**. This layer supports high-throughput, low-latency streaming to downstream analytics.

AI Analytics Layer

This layer comprises model training and scoring engines. Batch and online models are trained using historical and real-time data using ML frameworks (e.g., TensorFlow, Scikit-Learn). Predictive services are deployed as microservices with secure APIs.

Security and Access Control Layer

Security policies propagate from SAP IAM and external policy managers (e.g., OAuth 2.0 servers). Encryption (TLS, AES), RBAC, token-based access, SIEM monitoring, and audit trails are enforced across pipelines.

Consumer and Dashboard Layer

Decision-support dashboards and customer portals consume predictions via secure APIs. Alerts, reports, and recommendations are delivered in real time.

3. Data Integration Processes

Data flows from SAP modules (financial transactions, customer profiles) through real-time connectors into streaming platforms. Data is enriched and transformed in a stream processing layer that supports feature extraction for predictive models. Batch historical data is managed in a data lake with governance.

4. Model Development and Deployment

Predictive models are developed for:

- Credit risk prediction using supervised learning
- Fraud detection with classification models
- Customer behavior forecasting with time series models

Models are trained offline and iteratively retrained with incremental real-time feedback. Deployed models expose prediction APIs secured with IAM tokens.

5. Security Controls

Security is enforced at all layers:

- Transport encryption (TLS/SSL)
- Data encryption at rest
- Role-based access policies
- Audit logs and SIEM
- Anomaly detection for access patterns

SAP security integrates with cloud identity providers to manage authentication and authorization.

6. Evaluation Criteria

The framework was evaluated according to:

- Predictive performance metrics (precision, recall, ROC-AUC)
- Latency (real-time responsiveness)
- Security effectiveness
- Integration consistency
- Scalability under load

7. Experimental Setup

We implement a prototype using:

- SAP S/4HANA sandbox
- Streaming (Apache Kafka)
- Model serving (TensorFlow Serving)
- Dashboards (Grafana/Power BI)
- Security (OAuth 2.0, SIEM stack)

Simulated banking datasets test operational scenarios.

ADVANTAGES

- **Integrated enterprise analytics** reduces data silos.
- **Real-time insights** improve responsiveness and risk mitigation.
- **Secure end-to-end architecture** ensures compliance and data protection.

- **Predictive capabilities** enhance decision support and customer personalization.
- **Modular design** supports scalability and extensibility.

DISADVANTAGES
- **Implementation complexity** across heterogeneous systems.
- **High initial cost** for infrastructure and skilled resources.
- **Security management overhead** with multiple integration points.
- **Model maintenance and drift** risk if not continually retrained.
- **Interoperability challenges** with legacy data formats.

IV. RESULTS AND DISCUSSION

Predictive Performance
The prototype demonstrated significant improvements in predictive accuracy (ROC-AUC > 0.9 for credit risk, fraud detection) compared to baseline batch analytics. Real-time models responded within sub-second latencies.

Integration Efficacy
Streaming connectors successfully propagated SAP events into analytics pipelines without data loss. Feature extraction enabled robust model inputs.
Security Outcomes
End-to-end encryption and RBAC prevented unauthorized access in penetration tests. SIEM dashboards correlated access events for compliance.

V. CONCLUSION

The integration of secure digital banking frameworks with SAP systems and real-time AI-driven predictive analytics represents a critical evolution in modern banking infrastructure. Traditional banking systems, while robust in transaction processing, often suffer from delays in data analysis, siloed information, and limitations in proactive decision-making. These limitations hinder banks' abilities to detect fraudulent activity promptly, assess credit risk accurately, and deliver personalized customer experiences efficiently. The proposed framework addresses these gaps by combining SAP's enterprise capabilities with advanced real-time analytics powered by AI and machine learning, creating a unified, secure, and intelligent digital banking ecosystem.

At its core, the framework leverages SAP S/4HANA for core financial operations, ensuring transactional accuracy, compliance, and secure record keeping. The system architecture incorporates SAP Fiori for intuitive user interfaces and SAP Cloud Platform for scalable deployments. By embedding AI-driven predictive models into the SAP ecosystem, financial institutions can achieve real-time insights without compromising data security or operational integrity. For example, fraud detection models continuously monitor transaction streams and identify anomalies in sub-second intervals. Credit risk models dynamically adjust scoring based on updated customer behavior, external market conditions, and transactional histories, facilitating more accurate lending decisions. Furthermore, AI-enabled predictive

insights extend beyond risk management to include customer behavior forecasting**,** enabling personalized offers and proactive retention strategies that improve satisfaction and loyalty.

Security and compliance are foundational to this framework. With banking data being highly sensitive and subject to stringent regulations, including PCI DSS, GDPR, and Basel III, the architecture incorporates multi-layered protection. Data is encrypted both at rest and in transit, and access is governed through role-based access control (RBAC) integrated with identity and access management (IAM) systems. Audit trails and monitoring mechanisms are implemented to detect and respond to unauthorized access attempts, ensuring continuous compliance with regulatory standards. Moreover, by maintaining the AI models within the secure SAP ecosystem and limiting external data transfer, the framework minimizes exposure to breaches or data leaks, aligning with privacy best practices.

One of the most notable advantages of this framework is the real-time operational agility it provides. Traditional batch processing models often generate insights hours or even days after data is collected, limiting banks' ability to respond promptly to emerging risks or opportunities. By contrast, this framework enables near-instantaneous analysis, allowing financial institutions to act decisively on high-risk transactions, market changes, or customer behavior patterns. For example, fraudulent activity can be flagged in real time, triggering automated mitigation protocols, while customer churn predictions can inform immediate retention interventions. These capabilities collectively enhance both operational efficiency and customer satisfaction, reinforcing the strategic value of digital transformation.
From a technological perspective, integrating real-time AI analytics into SAP environments demonstrates the synergy of enterprise systems and advanced machine learning frameworks**.** This integration not only enhances predictive performance but also ensures that all insights are derived from consistent, high-quality data. Feature extraction pipelines, automated data cleansing, and stream processing ensure that predictive models operate on reliable and representative datasets. The framework also supports continuous model retraining and feedback loops, allowing AI models to adapt to changing patterns in financial and customer behavior. This continuous learning mechanism ensures that predictive insights remain relevant and accurate over time, preventing model drift and maintaining operational reliability.

Moreover, the framework addresses scalability challenges inherent in large financial institutions. By leveraging cloud-based deployment strategies, banks can scale computational resources dynamically, accommodating increased transaction volumes, additional predictive models, or expanded geographic coverage. This flexibility ensures that real-time analytics remain performant even as data volumes grow or operational demands fluctuate. Additionally, modular architecture allows incremental integration of new AI models, analytical tools, or SAP modules without disrupting core banking operations, ensuring sustainable long-term evolution of the digital ecosystem.

The research and prototype implementation also highlight several operational benefits**.** Real-time dashboards and visualizations provide executives and operational teams with actionable insights, facilitating better decision-making and cross-departmental collaboration. The integration of predictive analytics with transactional data reduces manual reporting and analytical overhead, freeing resources for strategic initiatives. Furthermore, AI-driven anomaly detection minimizes false positives, enhancing trust in automated systems and enabling staff to focus on high-priority cases. Overall, the framework promotes

a culture of data-driven decision-making and operational excellence, which is critical in highly regulated and competitive financial markets.

However, the research acknowledges limitations and challenges**.** Integrating AI with SAP systems requires careful planning, technical expertise, and significant initial investment. Data heterogeneity and legacy system constraints may impede smooth model training or real-time data ingestion. Security management remains complex, especially when external APIs or third-party services are incorporated. Moreover, predictive models require ongoing monitoring to address bias, accuracy degradation, and changing regulatory requirements. Addressing these challenges necessitates a robust governance strategy, regular audits, and continuous staff training to maintain system efficacy and compliance.

In conclusion, the Secure Digital Banking Framework integrating SAP and real-time AI analytics provides a blueprint for financial institutions to modernize their operations while maintaining stringent security and compliance standards. By unifying transactional accuracy, predictive intelligence, and operational oversight in a single, scalable ecosystem, banks can improve fraud detection, credit risk assessment, customer personalization, and overall operational agility. This framework demonstrates that the convergence of enterprise systems and AI-driven analytics is not only feasible but essential for sustaining competitiveness, regulatory compliance, and customer trust in the rapidly evolving digital banking landscape.

VI. FUTURE WORK

1. **Enhanced AI Models and Explainability:** Future research should explore advanced AI techniques, including explainable AI (XAI), to ensure transparency in predictive decision-making and regulatory compliance.
2. **Blockchain Integration for Audit and Security:** Incorporating blockchain technologies can enhance transaction traceability, immutable audit trails, and smart contract-based compliance verification.
3. **Edge Computing for Low-Latency Banking Services:** Implementing edge analytics could reduce latency further, particularly for mobile banking and IoT-enabled financial services.
4. **Adaptive Cybersecurity Measures:** Future systems should integrate AI-based threat detection for adaptive security responses to emerging cyber threats in real time.
5. **Cross-Institution Collaboration:** Investigate federated learning and secure multi-party computation to enable collaboration across financial institutions without compromising data privacy.
6. **Customer Personalization and Behavioral Analytics:** Explore integrating more granular customer behavioral data, including digital footprint and transactional patterns, to enhance predictive personalization.
7. **Regulatory Automation:** Develop AI-driven regulatory compliance monitoring systems that automatically detect policy violations and generate audit reports.

VI. 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. Archana, R., & Anand, L. (2023, May). Effective Methods to Detect Liver Cancer Using CNN and Deep Learning Algorithms. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
3. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
4. 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
5. Raj, A. A., & Sugumar, R. (2022, December). Monitoring of the Social Distance between Passengers in Real-time through Video Analytics and Deep Learning in Railway Stations for Developing the Highest Efficiency. In 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (Vol. 1, pp. 1-7). IEEE.
6. Alpaydin, E. (2010). *Introduction to machine learning* (2nd ed.). MIT Press.
7. Banker, R. D., & Kauffman, R. J. (2018). The evolution of ERP systems: Past, present, and future. *Communications of the ACM, 61*(11), 26–28.
8. Pachyappan, R., Vijayaboopathy, V., & Paul, D. (2022). Enhanced Security and Scalability in Cloud Architectures Using AWS KMS and Lambda Authorizers: A Novel Framework. Newark Journal of Human-Centric AI and Robotics Interaction, 2, 87-119.
9. Delen, D., & Demirkan, H. (2013). Data, information and analytics as services. *Decision Support Systems, 55*(1), 359–363.
10. Navandar, P. (2022). The Evolution from Physical Protection to Cyber Defense. International Journal of Computer Technology and Electronics Communication, 5(5), 5730-5752.
11. Kumar, R. K. (2023). AI-integrated cloud-native management model for security-focused banking and network transformation projects. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9321–9329. https://doi.org/10.15662/IJRPETM.2023.0605006
12. Vasugi, T. (2022). AI-Optimized Multi-Cloud Resource Management Architecture for Secure Banking and Network Environments. International Journal of Research and Applied Innovations, 5(4), 7368-7376.
13. Grover, P., & Kar, A. K. (2017). Big data analytics in banking. *International Journal of Bank Marketing, 35*(2), 195–218.
14. 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.
15. Nagarajan, G. (2023). AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6292-6297.
16. Kshetri, N. (2017). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89.
17. Marquez, F., & Yang, J. (2020). Real-time predictive analytics in financial services. *Journal of Financial Data Science, 2*(3), 45–57.
18. Gujjala, Praveen Kumar Reddy. (2023). Autonomous Healthcare Diagnostics : A MultiModal AI Framework Using AWS SageMaker, Lambda, and Deep Learning Orchestration for Real-Time Medical Image Analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 760-772. 10.32628/CSEIT23564527.

19.Kalyanasundaram, P. D., & Paul, D. (2023). Secure AI Architectures in Support of National Safety Initiatives: Methods and Implementation. Newark Journal of Human-Centric AI and Robotics Interaction, 3, 322-355.
20.SAP SE. (2017). *SAP S/4HANA: The next-generation business suite*. SAP Press.
21.Shalev-Shwartz, S., & Ben-David, S. (2014). *Understanding machine learning: From theory to algorithms*. Cambridge University Press.
22.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.
23.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.
24.Sudhakara Reddy Peram, Praveen Kumar Kanumarlapudi, Sridhar Reddy Kakulavaram. (2023). Cypress Performance Insights: Predicting UI Test Execution Time Using Complexity Metrics. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 6(1), 167-190.
25.Hasan, S., Zerine, I., Islam, M. M., Hossain, A., Rahman, K. A., & Doha, Z. (2023). Predictive Modeling of US Stock Market Trends Using Hybrid Deep Learning and Economic Indicators to Strengthen National Financial Resilience. Journal of Economics, Finance and Accounting Studies, 5(3), 223-235.
26.Sharma, A., Kabade, S., & Kagalkar, A. (2024). AI-Driven and Cloud-Enabled System for Automated Reconciliation and Regulatory Compliance in Pension Fund Management. International Journal of Emerging Research in Engineering and Technology, 5(2), 65-73.
27.Meka, S. (2023). Building Digital Banking Foundations: Delivering End-to-End FinTech Solutions with Enterprise-Grade Reliability. International Journal of Research and Applied Innovations, 6(2), 8582-8592.
28.Sasidevi, J., Sugumar, R., & Priya, P. S. (2017). A Cost-Effective Privacy Preserving Using Anonymization Based Hybrid Bat Algorithm With Simulated Annealing Approach For Intermediate Data Sets Over Cloud Computing. International Journal of Computational Research and Development, 2(2), 173-181.
29.Chandra Sekhar Oleti. (2022). Serverless Intelligence: Securing J2ee-Based Federated Learning Pipelines on AWS. International Journal of Computer Engineering and Technology (IJCET), 13(3), 163-180. https://iaeme.com/MasterAdmin/Journal_uploa ds/IJCET/VOLUME_13_ISSUE_3/IJCET_13_03 _017.pdf
30.Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2023). Ethical analysis and decision-making framework for marketing communications: A weighted product model approach. Data Analytics and Artificial Intelligence, 3 (5), 44–53.
31.Fazilath, M., & Umasankar, P. (2025, February). Comprehensive Analysis of Artificial Intelligence Applications for Early Detection of Ovarian Tumours: Current Trends and Future Directions. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-9). IEEE.
32.Zhang, C., & Ma, Y. (2012). *Ensemble machine learning: Methods and applications*. Springer.**.**