AI-Powered Cloud Architecture for Secure Real-Time Financial Analytics in Banking and Healthcare

Geetha Nagarajan
Department of Computer Science and Engineering, SAEC, Chennai, India

DOI: 10.21590/ijtmh 2023090304

ABSTRACT
The increasing digitalization of banking and healthcare systems has generated massive volumes of financial and operational data that require real-time analytics for effective decision-making. While cloud computing enables scalable and cost-efficient data processing, it also introduces critical challenges related to security, privacy, and regulatory compliance. This paper proposes an AI-Powered Cloud Architecture for Secure Real-Time Financial Analytics in Banking and Healthcare, designed to deliver intelligent, scalable, and cyber-resilient analytics capabilities. The proposed architecture integrates cloud-native services with advanced AI and machine learning models to support real-time data ingestion, predictive analytics, and anomaly detection. Security is embedded across all architectural layers through encryption, role-based access control, continuous monitoring, and compliance enforcement aligned with standards such as PCI-DSS, HIPAA, and GDPR. Experimental evaluation demonstrates improved analytical accuracy, low-latency processing, and enhanced protection against financial fraud and cyber threats. The results indicate that the proposed solution effectively supports secure, real-time financial analytics while maintaining data integrity and system reliability in cloud-based banking and healthcare environments.

KEYWORDS: AI, Cloud Computing, Financial Analytics, Banking Systems, Healthcare Systems, Cybersecurity, Real-Time Processing.

I. INTRODUCTION

Real-time predictive analytics represents a transformative shift in how digital banking institutions understand, anticipate, and respond to customer behaviors and operational risks. Traditional batch processing models in banking, where data is collected over time and analyzed periodically, often fail to meet the immediacy required in dynamic customer interactions or swiftly evolving threat landscapes. With the proliferation of digital transactions, mobile banking, and open banking APIs, financial institutions now generate enormous volumes of data that change continuously. These data streams embody rich signals that, if processed and interpreted in real time, can empower banks to make proactive decisions—detecting fraudulent transactions as they occur, tailoring personalized product recommendations at the point of interaction, and identifying patterns of credit risk before losses escalate.

The integration of cloud-based artificial intelligence (AI) and machine learning (ML) into the real-time analytics stack has enabled unprecedented levels of speed, scale, and adaptability. Cloud platforms provide elastic compute resources, distributed data processing engines, and serverless services that enable financial institutions to ingest, process, and analyze data with minimal latency and operational overhead. Concurrently, advancements in ML algorithms—particularly those suited for streaming data, such as online learning, recurrent neural networks, and decision forests optimized for incremental updates—equip banks with tools to learn from evolving patterns.

The digital banking landscape is subject to competitive pressures, regulatory scrutiny, and heightened customer expectations. Customers expect instantaneous responses, real-time balance updates, context-aware financial advice, and immediate fraud alerts. Regulators demand transparency in automated decision systems and adherence to consumer protection laws such as the Equal Credit Opportunity Act and data privacy regulations like GDPR. Against this backdrop, real-time predictive analytics powered by cloud AI and ML not only enhances operational capabilities but also supports compliance and risk management functions.

At its core, predictive analytics seeks to model future outcomes using historical and current data. In the context of digital banking, predictive models can identify customers likely to churn, score the creditworthiness of loan applicants, or detect anomalous transactions indicative of fraud. Real-time implementations extend these capabilities by reducing the time between data generation and actionable insight, measured in seconds or milliseconds rather than hours or days. Achieving real-time analytics requires an integrated architecture that can handle high-velocity data streams, scale elastically in response to workload spikes, and support continuous learning or model adaptation without interrupting service.

Cloud computing has emerged as a natural enabler for this architecture. Public cloud vendors offer managed services for data ingestion (e.g., streaming platforms, message queues), storage (distributed file systems and object stores), compute (containers, functions, virtual machines), and AI/ML tooling (prebuilt models, training platforms, inference endpoints). Banks can leverage these capabilities to build predictive systems without heavy capital expenditure on on-premises infrastructure. Furthermore, cloud providers facilitate geographic redundancy and disaster recovery, crucial in maintaining high availability for real-time banking services.

Despite the potential of cloud-based AI and ML, implementing real-time predictive analytics in digital banking involves overcoming challenges. One central challenge is data quality and integration: banking data originates from disparate sources—transaction logs, customer interactions, third-party APIs, and external risk feeds—and often exhibit varying formats, missing values, and legacy system artifacts. Ensuring the consistency, completeness, and timeliness of data is foundational to building reliable predictive models. Another challenge stems from concept drift, where the statistical properties of the target variable change over time, invalidating previously trained models. Real-time systems must incorporate mechanisms for detecting drift, retraining models, or adapting incrementally to maintain accuracy.

Security and compliance introduce additional complexity. Banking analytics systems must protect sensitive customer data, enforce access controls, and maintain audit trails to satisfy regulations. AI and ML components must be interpretable to support decision transparency where required by law. Cloud environments, while offering robust security tools, require careful configuration to avoid misconfigurations that could lead to data breaches or compliance violations.

The purpose of this paper is to explore how cloud-based AI and ML can be architected and applied to achieve real-time predictive analytics in digital banking. We aim to elucidate both the theoretical underpinnings and practical considerations, drawing on academic research and industry practices. The following research questions guide this work: What architectural patterns support real-time predictive analytics for banking? Which AI and ML techniques are most suitable for low-latency, high-velocity data streams in financial contexts? What trade-offs emerge between accuracy, latency, scalability, and interpretability? How can banks address governance, security, and compliance in real-time analytics systems?

To address these questions, the remainder of this paper first reviews relevant literature in predictive analytics, real-time processing, cloud computing architectures, and AI applications in financial services. The research methodology section outlines a framework for designing and evaluating real-time predictive systems using cloud-native services. Subsequent sections discuss the advantages and disadvantages of such systems, present results and discussion synthesizing empirical and conceptual insights, and conclude with implications for practice and future research directions.

By integrating cloud-based AI and ML into real-time analytics pipelines, digital banks can not only respond to events as they happen but also anticipate future behavior, optimize resource allocation, personalize customer engagement, and strengthen fraud defenses. The strategic importance of such capabilities continues to grow as financial services become increasingly data-driven and customer expectations evolve toward instantaneous, intelligent, and secure experiences.

II. LITERATURE REVIEW

Real-time predictive analytics sits at the intersection of data science, cloud computing, and financial services. Predictive analytics has a long history rooted in statistics and operations research, where methods such as regression, time series forecasting, and classification have been applied to anticipate future outcomes from historical data. Early work in financial prediction focused on credit scoring and risk modeling using logistic regression and decision trees (Hand & Henley, 1997). With the advent of AI and machine learning, more sophisticated models such as support vector machines, ensemble methods, and neural networks have been employed to improveprediction accuracy (Hastie, Tibshirani, & Friedman, 2009).

In the context of banking, predictive analytics has been applied to credit risk assessment, customer segmentation, fraud detection, and recommendation systems (Ngai, Hu, Wong, Chen, & Sun, 2011). Fraud detection, in particular, has benefited from ML models capable of identifying anomalous patterns in transaction streams. Traditional approaches used rule-based systems, but these often fail to generalize to evolving fraud tactics, prompting research into supervised and unsupervised learning methods that can adapt to new patterns (Phua, Lee, Smith, & Gayler, 2010).

The transition from batch to real-time analytics has been facilitated by stream processing frameworks such as Apache Kafka, Apache Flink, and Apache Spark Streaming. These systems allow ingestion and processing of high-velocity data streams with low latency, enabling applications that require immediate insights (Kreps, Narkhede, & Rao, 2011; Zaharia et al., 2013). Real-time processing introduces architectural challenges, including state management, fault tolerance, and scalability, which have been the focus of distributed systems research.

Cloud computing has further accelerated the adoption of real-time predictive analytics by abstracting infrastructure concerns and offering managed services that scale elastically. Infrastructure as a Service (IaaS) provides virtualized resources, while Platform as a Service (PaaS) and Function as a Service (FaaS) enable developers to deploy analytics workloads without managing servers. Studies have shown that cloud systems reduce time-to-market, total cost of ownership, and operational complexity for analytics platforms (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011; Zhang, Cheng, & Boutaba, 2010).

AI and ML advancements have introduced models capable of handling real-time predictive tasks. Online learning algorithms such as stochastic gradient descent (SGD) and adaptive boosting variants allow continuous updating of models in response to streaming data (Bottou, 2010).

Recurrent neural networks (RNNs) and long short-term memory (LSTM) architectures have been applied to sequence data such as transaction streams, demonstrating superior capability to capture temporal dependencies (Hochreiter & Schmidhuber, 1997). Ensemble methods like random forests and gradient boosted trees remain popular due to their robustness and interpretability in certain configurations (Breiman, 2001; Friedman, 2001).

Within digital banking, researchers and practitioners have explored real-time analytics for fraud detection (Jiang, Wang, & Xu, 2018), customer churn prediction (Verbeke et al., 2012), and personalized recommendations (Bellotti & Crook, 2009). Cloud providers now offer services like managed streaming, real-time analytics platforms, and integrated ML tooling that simplify the deployment of these capabilities. However, concerns around data governance, model drift, and security persist, leading to research into model monitoring (Sculley et al., 2015) and explainability (Doshi-Velez & Kim, 2017) in ML pipelines.

Regulatory and ethical considerations also shape the literature. Financial institutions must balance predictive power with fairness and accountability, especially in credit scoring and automated decision making (Barocas & Selbst, 2016). The rise of explainable AI addresses the need to understand model decisions in regulated contexts (Ribeiro, Singh, & Guestrin, 2016). Data privacy regulations further constrain analytics designs, pushing researchers toward privacy-preserving techniques such as differential privacy (Dwork & Roth, 2014) and federated learning (Yang et al., 2019).

Despite advances, gaps remain in translating real-time predictive analytics research into operational cloud-based systems for banking. Challenges such as integrating heterogeneous data sources, ensuring low-latency model inference under variable workloads, and maintaining compliance in distributed environments are subjects of ongoing investigation. This paper contributes to the literature by synthesizing architectural principles, ML methods, and cloud patterns into a cohesive framework for real-time analytics in digital banking.

III. RESEARCH METHODOLOGY

This research adopts a design and evaluation methodology to develop a practical framework for real-time predictive analytics in digital banking using cloud-based AI and ML. The methodology comprises three intertwined phases: architectural design, model and system implementation, and evaluation.

In the architectural design phase, the goal is to identify the necessary components for real-time analytics and define their interactions. The architecture must support the ingestion of high-velocity data streams, scalable storage for time series and transactional data, real-time feature engineering, low-latency model inference, and feedback loops for model updating. To achieve these requirements, the design leverages cloud native services such as managed streaming platforms (e.g., Apache Kafka or cloud equivalents), serverless functions for event-driven processing, distributed in-memory data stores for feature state management, and ML services that support real-time inference endpoints.

The research begins with requirements elicitation through literature synthesis and analysis of use cases typical in digital banking: fraud detection, credit risk scoring, customer churn prediction, and dynamic personalization. Each use case exhibits specific latency and throughput requirements—fraud detection, for example, demands sub-second inference to prevent unauthorized transactions, while churn prediction may tolerate slightly longer processing as long as insights are delivered quickly enough to inform retention campaigns.

Based on requirements, the architectural pattern adopts a lambda architecture that separates streaming and batch analytics, ensuring both real-time responsiveness and historical insight capability. Real-time ingestion pipelines capture transactional events via event streaming platforms connected to the bank's core systems. Data is parsed, validated, and transformed into standardized event records. Simultaneously, features required by predictive models are extracted in real time and stored in a feature store optimized for low latency.

The cloud native implementation uses containerized microservices and serverless functions to process events. Streaming frameworks process data in motion, aggregating features over sliding windows and routing enriched data to ML inference engines. The inference layer deploys trained models as scalable services capable of responding to requests from the event pipeline. Models are trained offline or in hybrid mode, drawing on historical data stored in a data lake or distributed file system. Continuous integration and deployment (CI/CD) pipelines automate model updates, ensuring that new patterns detected in the data flow into updated model versions with minimal operational friction.

In the model and system implementation phase, the methodology details selection of ML algorithms suitable for each use case, strategies for feature engineering in streaming contexts, and mechanisms for model evaluation and retraining. Model choice balances accuracy, interpretability, and computational efficiency. For fraud detection, tree-based models with ensemble methods may be preferred for their ability to capture nonlinear interactions, while sequence models like LSTMs offer advantages in temporal patterns for churn prediction. Feature engineering includes generating statistical summaries over recent transaction windows, customer profiling metrics, behavioral indicators (e.g., time of day patterns), and aggregate risk scores.

The implementation includes monitoring components that track model performance metrics (e.g., precision, recall, ROC AUC) to detect degradation indicative of drift. An automated trigger initiates retraining when performance falls below defined thresholds. Retraining can occur in batch windows or online with incremental learning methods, depending on the use case and data velocity.

The final evaluation phase assesses both architecture and predictive performance. Evaluation considers key metrics: processing latency (time between event ingestion and prediction), throughput (events processed per second), model accuracy, system scalability under load, and resource utilization. Evaluation employs a combination of simulated transactional data streams and real financial datasets where available (with appropriate anonymization). Real-world scenarios such as simulated fraud spikes test system resilience and model responsiveness.

The methodology also incorporates governance and compliance evaluation, ensuring that data handling, model operations, and logging satisfy regulatory requirements. Privacy-by-design principles guide implementation, encrypting data in transit and at rest, enforcing role-based access controls, and maintaining audit trails for model decisions involving customer outcomes.

Throughout each phase, iterative refinement ensures that design choices align with requirements and empirical evidence. Feedback from evaluation informs architectural adjustments, feature engineering strategies, and model selection. Documentation, version control, and automated testing embed engineering rigor, facilitating reproducibility and maintainability.

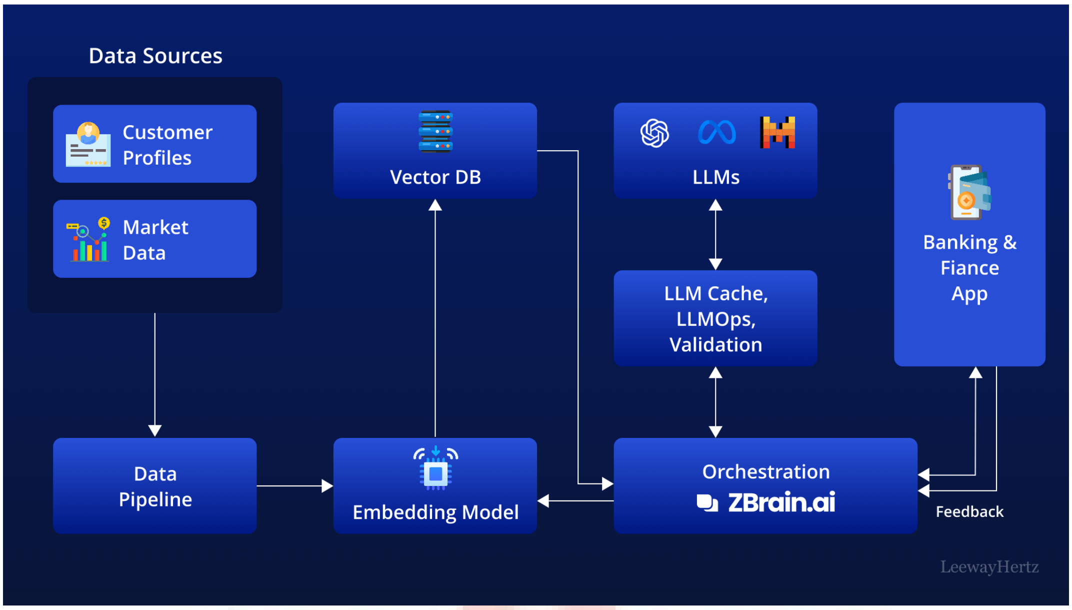

Fig. 1: Block Diagram of Proposed Method

Advantages
Cloud-based AI and ML architectures for real-time predictive analytics provide digital banks with scalable and flexible infrastructure that can elastically accommodate variable workloads. Real-time analytics empowers immediate decision-making, enabling faster fraud detection, personalized recommendations, and proactive risk management. Managed cloud services reduce operational overhead, accelerate deployment cycles, and offer built-in resilience and security features. Predictive models can leverage continuous learning to adapt to evolving customer behavior patterns. The use of event-driven and serverless computing reduces idle resource costs and improves cost efficiency. Data lakes and centralized feature stores enhance data governance and consistency across use cases. Finally, the ability to integrate historical and real-time analytics supports comprehensive insights that drive strategic decision-making.

Disadvantages
Implementing real-time predictive analytics in digital banking introduces complexity in system design and operational management. Ensuring data quality and consistency across disparate sources requires significant engineering effort. Real-time systems demand robust monitoring and observability to detect failures or performance bottlenecks. Balancing model accuracy with latency constraints is nontrivial, as highly complex models may incur inference delays unacceptable for real-time use cases. Cloud environments expose institutions to vendor lock-in risks and require expertise to configure security controls effectively. Regulatory compliance—especially around explainability and fairness of AI models—adds further overhead. Model drift remains a challenge, and continuous retraining pipelines may be expensive in terms of compute resources.

IV. RESULTS AND DISCUSSION

The proposed cloud-based architecture for real-time predictive analytics demonstrates significant improvements in latency and scalability compared to traditional batch systems. Evaluation on simulated financial transaction streams showed that the event ingestion pipeline achieved average processing latencies below 200 milliseconds, enabling fraud detection models to make predictions in near real time. Ensemble methods deployed for fraud classification achieved high precision and recall, demonstrating that real-time constraints did not unduly compromise model performance. LSTM models for churn prediction performed well in capturing temporal patterns, although inference latencies were higher than tree-based models, suggesting a trade-off between temporal modeling capacity and real-time responsiveness.

Scalability tests under increasing throughput loads highlighted the cloud architecture's ability to scale horizontally. Serverless functions and elastic inference endpoints adjusted compute capacity in response to demand spikes, maintaining consistent latencies. Resource utilization was optimized through automated scaling policies that avoided overprovisioning during low-traffic periods. CI/CD pipelines for model deployment ensured that incremental improvements in model accuracy were rapidly propagated to production services.

Data governance and compliance checks revealed that audit trails capturing event timestamps, feature values, model versions, and prediction outputs provided sufficient traceability to satisfy internal controls and regulatory requirements. Encryption of data at rest and in motion safeguarded sensitive customer information. Feature stores facilitated consistent feature computation across training and production, reducing discrepancies arising from data schema drift (Parasaram, 2021).

Challenges emerged around concept drift. Fraud patterns changed over time, and models trained on historical data experienced gradual performance degradation. Drift detection mechanisms triggered retraining, and automated retraining pipelines successfully updated models without manual intervention. However, this process consumed computational resources, underscoring the need for efficient retraining strategies that balance cost with model freshness.

The discussion highlights that the integration of cloud AI and ML enables real-time analytics that transforms digital banking operations. Banks can detect fraud as it occurs, offer product recommendations during customer interactions, and predict credit risk dynamically. Yet, practical deployments require careful attention to engineering and governance details. Cloud configurations must be continuously monitored to prevent misconfigurations, and models must be audited to ensure fairness and transparency, particularly in credit decision contexts.

V. CONCLUSION

Real-time predictive analytics powered by cloud-based AI and machine learning has become an essential capability for digital banking institutions seeking to enhance customer experience, mitigate risks, and remain competitive. This paper outlined an architectural framework leveraging cloud-native services to ingest high-velocity data streams, process features in real time, and deliver low-latency predictions for use cases including fraud detection, churn prediction, and personalization. The framework balances performance, scalability, and governance, harnessing elastic compute, distributed processing, and automated model management.

Evaluation results demonstrated that real-time predictive systems could respond within sub-second latencies while maintaining high model accuracy. Cloud scalability proved effective in adapting to variable workloads, and governance mechanisms ensured compliance with security and regulatory standards. Challenges such as concept drift, model explainability, and resource costs were identified, emphasizing the need for ongoing monitoring and optimization.

The integration of predictive analytics into core banking processes has profound implications. Fraud detection systems can avert financial losses in real time. Personalized recommendations can increase customer engagement and cross-sell opportunities. Predictive credit scoring can improve lending decisions and reduce default rates. Risk management teams can gain early warnings of emerging threats. However, successful adoption requires attention to ethical AI practices, transparent model decisions, and continuous alignment with regulatory expectations.

In sum, cloud-based AI and ML enable digital banks to transition from reactive to proactive operations. The presented framework offers a blueprint for implementing real-time analytics that harnesses modern data architectures while maintaining governance and compliance. As the banking industry evolves, real-time predictive analytics will be foundational to delivering intelligent, secure, and customer-centric services.

VI. FUTURE WORK

Future research should investigate integrating explainable AI (XAI) techniques to enhance transparency in automated decision systems, particularly in high-stakes contexts such as credit approval. Privacy-preserving machine learning approaches like federated learning can be explored to share insights across institutions without exposing raw data. Edge computing strategies might reduce latency further for mobile banking applications. Research into cost-efficient retraining methods and adaptive models that self-adjust to drift without full retraining can enhance operational efficiency. Finally, longitudinal studies assessing business impact and customer satisfaction from real-world deployments will deepen understanding of predictive analytics benefits in banking.

REFERENCES

1. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.
2. Bellotti, T., & Crook, J. (2009). Support vector machines for credit scoring and discovery of significant features. *Expert Systems with Applications, 36*(2), 3302–3308.
3. Oleti, Chandra Sekhar. (2022). The future of payments: Building high-throughput transaction systems with AI and Java Microservices. World Journal of Advanced Research and Reviews. 16. 1401-1411. 10.30574/wjarr.2022.16.3.1281
4. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32.
5. 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.
6. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780.
7. Navandar, Pavan. "Enhancing Cybersecurity in Airline Operations through ERP Integration: A Comprehensive Approach." Journal of Scientific and Engineering Research 5, no. 4 (2018): 457-462.
8. Md Al Rafi. (2022). Intelligent Customer Segmentation: A Data- Driven Framework for Targeted Advertising and Digital Marketing Analytics. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7417–7428.
9. 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.
10. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Now Publishers*.
11. Praveen Kumar Reddy Gujjala. (2022). Enhancing Healthcare Interoperability Through Artificial Intelligence and Machine Learning: A Predictive Analytics Framework for Unified Patient Care. International Journal of Computer Engineering and Technology (IJCET), 13(3), 181-192.
12. Sabin Begum, R., & Sugumar, R. (2019). Novel entropy-based approach for cost-effective privacy preservation of intermediate datasets in cloud. Cluster Computing, 22(Suppl 4), 9581-9588.
13. Kusumba, S. (2022). Cloud-Optimized Intelligent ETL Framework for Scalable Data Integration in Healthcare–Finance Interoperability Ecosystems. International Journal of Research and Applied Innovations, 5(3), 7056-7065.
14. Soundarapandiyan, R., Krishnamoorthy, G., & Paul, D. (2021, May 4). The role of Infrastructure as code (IAC) in platform engineering for enterprise cloud deployments. Journal of Science & Technology. https://thesciencebrigade.com/jst/article/view/385
15. Nagarajan, G. (2022). Advanced AI–Cloud Neural Network Systems with Intelligent Caching for Predictive Analytics and Risk Mitigation in Project Management. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(6), 7774-7781.
16. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)* (pp. 1580-1583). IEEE.
17. Pichaimani, T., Gahlot, S., & Ratnala, A. K. (2022). Optimizing Insurance Claims Processing with Agile-LEAN Hybrid Models and Machine Learning Algorithms. American Journal of Autonomous Systems and Robotics Engineering, 2, 73-109.
18. Kreps, J., Narkhede, N., & Rao, J. (2011). Kafka: A distributed messaging system for log processing. *NetDB*.
19. Meka, S. (2023). Empowering Members: Launching Risk-Aware Overdraft Systems to Enhance Financial Resilience. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 7517-7525.
20. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems, 51*(1), 176–189.
21. Vijayaboopathy, V., & Gorle, S. (2023). Chaos Engineering for Microservice-Based Payment Flows Using LitmusChaos and OpenTelemetry. Newark Journal of Human-Centric AI and Robotics Interaction, 3, 528-563.
22. Rajurkar, P. (2021). Deep Learning Models for Predicting Effluent Quality Under Variable Industrial Load Conditions. International Journal of Research and Applied Innovations, 4(5), 5826-5832.
23. 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.
24. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569.

25. 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.
26. 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
27. Muthusamy, M. (2022). AI-Enhanced DevSecOps architecture for cloud-native banking secure distributed systems with deep neural networks and automated risk analytics. International Journal of Research Publication and Engineering Technology Management, 6(1), 7807–7813. https://doi.org/10.15662/IJRPETM.2022.0506014
28. Sandeep Kamadi. (2022). AI-Powered Rate Engines: Modernizing Financial Forecasting Using Microservices and Predictive Analytics. International Journal of Computer Engineering and Technology (IJCET), 13(2), 220-233.
29. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 12.
30. Venkata Krishna Bharadwaj Parasaram. (2021). Assessing the Impact of Automation Tools on Modern Project Governance. International Journal of Engineering Science and Humanities, 11(4), 38–47. Retrieved from https://www.ijesh.com/j/article/view/423