International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806002

Cloud-Native Risk-Aware AI and Machine Learning Models for Banking Operations, Trade Safety, and 5G-Enabled Web Services

Luca Francesco Romano

Senior Software Engineer, Italy

ABSTRACT: The financial and trade sectors are experiencing unprecedented growth in **digital transactions, cross-border operations, and high-frequency trading**, creating critical challenges in risk management, fraud detection, and operational safety. Conventional systems are increasingly inadequate to address **complex, evolving threats**, necessitating the adoption of advanced AI and machine learning frameworks. This study proposes **cloud-native risk-aware AI and machine learning models** for banking operations, trade safety, and 5G-enabled web services. The framework integrates **predictive machine learning for anomaly detection, generative AI for simulating rare high-risk scenarios, and risk-aware scoring mechanisms** to prioritize critical events. Cloud-native deployment ensures **elastic scalability, fault tolerance, and low-latency processing**, while 5G connectivity facilitates real-time analytics across geographically distributed systems. Secure ETL pipelines and privacy-preserving techniques, including **differential privacy and secure multi-party computation (SMPC)**, ensure compliance with regulatory standards such as GDPR and PCI DSS. Experimental evaluation on synthetic and real-world datasets demonstrates detection accuracy exceeding 95%, significant reductions in false positives, and improved operational efficiency. The proposed framework provides a **comprehensive, adaptive, and secure solution** for modern banking and trade environments, enabling **real-time decision-making, enhanced risk mitigation, and privacy-preserving analytics** in web-based services

KEYWORDS: Cloud-Native AI, Risk-Aware Machine Learning, Banking Operations, Trade Safety, 5G Web Services, Predictive Analytics, Generative AI, Privacy-Preserving, Secure ETL, Fraud Detection

I. INTRODUCTION

The financial services and trade sectors are undergoing a transformative digital evolution fueled by **cloud computing, artificial intelligence (AI), machine learning (ML), and high-speed 5G networks**. Modern banking operations involve high-volume, real-time transaction processing, while trade systems require secure monitoring and risk assessment of cross-border financial and logistical operations. While digitalization enhances operational efficiency and service delivery, it simultaneously increases the exposure to **fraud, cyberattacks, compliance breaches, and operational risks**. Traditional systems relying on manual audits, static rules, and conventional analytics are no longer adequate for managing the complexity and scale of modern banking and trade environments.

AI and machine learning models provide a means of proactively detecting anomalies, predicting risk, and improving operational resilience. Predictive ML models, including random forests, gradient boosting machines, and LSTM networks, enable **real-time detection of suspicious activities and fraud patterns** in structured transactional data. However, these models are often insufficient for rare, high-impact scenarios that occur infrequently but can cause substantial financial or reputational damage. To address this limitation, **generative AI models** such as GANs and VAEs are incorporated to simulate complex rare-event scenarios, providing synthetic data that improves model robustness and supports **stress-testing of banking and trade systems**.

Risk-aware scoring mechanisms are critical for translating predictive outputs into actionable intelligence. By assigning dynamic risk scores based on probability, potential impact, and scenario simulations, these mechanisms allow financial institutions to **prioritize high-risk transactions, allocate resources efficiently, and respond promptly to threats**. Integration with cloud-native architectures enables scalable deployment, elastic resource allocation, and robust fault tolerance. By leveraging microservices, containerized applications, and distributed computing frameworks, cloud-native environments support **real-time analytics and low-latency response**, essential for high-frequency banking and trade operations.

5G network technology further enhances the performance and applicability of AI-powered systems by enabling ultra-low latency, high bandwidth, and reliable connectivity for distributed banking and trade systems. This allows real-time

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806002

processing and monitoring of large-scale transactions across geographies, supporting **instant risk assessment, anomaly detection, and operational continuity** in a highly dynamic environment.

Privacy and regulatory compliance are integral to any financial or trade analytics system. Secure ETL pipelines are employed to **extract, transform, and load sensitive financial data** while ensuring anonymization, encryption, and adherence to data protection regulations such as GDPR, PCI DSS, and other regional standards. Advanced privacy-preserving techniques, including **differential privacy and secure multi-party computation (SMPC)**, allow collaborative analytics across institutions without exposing raw customer data.
This paper presents a **cloud-native, risk-aware AI and ML framework** that integrates predictive analytics, generative simulation, risk-aware scoring, privacy-preserving pipelines, and 5G-enabled web services. The framework is designed to:

1. Detect and mitigate fraud and operational risks in banking operations and trade systems.
2. Simulate rare, high-impact scenarios to enhance predictive accuracy and preparedness.
3. Interpret and process both structured and unstructured data through AI and ML models.
4. Ensure privacy and compliance through ETL pipelines, differential privacy, and SMPC.
5. Deliver real-time analytics and visualization through 5G-enabled web services.

By combining cloud-native architecture, AI/ML capabilities, and advanced privacy mechanisms, the proposed framework addresses key gaps in current banking and trade risk management systems, providing a **comprehensive, adaptive, and scalable solution** for next-generation financial operations.

II. LITERATURE REVIEW

Historically, banking and trade analytics relied on **rule-based systems and manual audits**, which were limited in their ability to detect complex fraud and operational anomalies (Bolton & Hand, 2002). Supervised ML models, including decision trees, random forests, and gradient boosting, have improved detection for known fraud patterns, while unsupervised learning methods like clustering and autoencoders have enabled detection of previously unseen anomalies (Ngai et al., 2011).

Deep learning approaches, including LSTM and CNN architectures, have been adopted to model sequential dependencies and temporal patterns in transactional data, significantly improving detection rates for high-frequency transactions (Jurgovsky et al., 2018). Despite these advancements, rare-event scenarios and evolving fraud techniques often elude traditional predictive models.

Generative AI models such as GANs and VAEs are increasingly used to generate synthetic high-risk scenarios for system testing and model enhancement (Goodfellow et al., 2014). This approach allows institutions to anticipate low-frequency but high-impact events, enhancing operational resilience and proactive risk management.

Cloud-native deployments facilitate scalability, fault tolerance, and distributed processing, essential for high-volume banking and trade operations. Secure ETL pipelines and privacy-preserving mechanisms ensure that data integrity and regulatory compliance are maintained during analysis (Kshetri, 2016; Chen & Zhao, 2019).

5G networks complement cloud and AI capabilities by offering ultra-low latency, high throughput, and reliable connectivity. This is critical for real-time banking operations, cross-border trade monitoring, and immediate anomaly detection. Despite these advancements, there remains a lack of **integrated frameworks combining cloud-native AI/ML, generative simulation, privacy preservation, and 5G-enabled real-time analytics**. This study aims to bridge this gap.

III. RESEARCH METHODOLOGY

The proposed framework consists of **six integrated layers** for comprehensive banking and trade risk management:

1. **Data Acquisition Layer**
   - Structured data: transaction logs, account histories, trade records.
   - Unstructured data: emails, chat logs, regulatory filings.
   - Automated collection via secure ETL pipelines.
2. **Data Processing & Privacy Layer**
   - ETL pipelines for extraction, transformation, and secure loading into cloud storage.
   - Anonymization, pseudonymization, and encryption of sensitive data.
   - Differential privacy and SMPC for collaborative analytics without data leakage.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0806002

3. **Predictive Analytics Layer**
    - Supervised ML models: random forests, gradient boosting, LSTM networks for anomaly detection.
    - Unsupervised learning: clustering and autoencoders for outlier detection.
4. **Generative AI Layer**
    - GANs and VAEs generate synthetic scenarios representing rare, high-impact events.
    - Enhances robustness of predictive models and supports stress testing.
5. **Risk-Aware Scoring Layer**
    - Dynamic risk scoring based on probability, potential impact, and scenario simulation.
    - Prioritizes alerts for immediate mitigation and resource allocation.
    - Feedback loops recalibrate thresholds in real-time.
6. **Application & Deployment Layer**
    - Cloud-native architecture using Docker, Kubernetes, and distributed frameworks (Spark/Flink).
    - Web-based dashboards for visualization, alerting, and scenario simulation.
    - Optimized for 5G networks to enable low-latency, real-time analytics.

Evaluation Metrics

- Detection accuracy, precision, recall, F1-score, false-positive reduction.
- Latency and throughput for real-time processing.
- Privacy compliance with GDPR, PCI DSS.
- System resilience under peak loads and high-volume transactions.

Workflow Summary

- Data ingestion → Secure ETL → Cloud storage → Predictive ML & Generative AI analytics → Risk-aware scoring → Web-based dashboard → Continuous feedback and model retraining.

Advantages

- Real-time detection of banking and trade anomalies.
- Scalable and fault-tolerant cloud deployment.
- Privacy-preserving analytics with differential privacy and SMPC.
- Predictive and generative AI for proactive risk mitigation.
- 5G-enabled low-latency analytics for web services.
- Web dashboards with interpretability and scenario simulation.

Disadvantages

- High computational and infrastructure costs.
- Complexity of integrating multiple AI models and privacy layers.
- Continuous retraining required to handle evolving fraud and risks.
- Dependent on high-quality, multi-source data.
- Potential security vulnerabilities despite cloud and network safeguards.



Figure 1: Major AI Risks in Enterprise Systems

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0806002

IV. RESULTS AND DISCUSSION

Cloud-native AI and ML models bring transformative capabilities to banking, trade, and 5G-enabled web services by leveraging modular, scalable, and service-oriented infrastructures. Unlike traditional monolithic systems, cloud-native platforms utilize microservices, containerization, and orchestrated deployments to provide continuous availability and dynamic scaling. These characteristics allow risk-aware models to process high volumes of streaming and historical data, enabling more accurate predictions, anomaly detection, and decision support.

1. Risk-Aware AI in Banking Operations

In the banking sector, risk-aware AI models deployed on cloud-native platforms demonstrated substantial improvements in fraud detection, credit risk assessment, and compliance monitoring. Traditional banking risk management relies on static rules and periodic batch processing of transactions, which often fails to detect subtle, evolving fraud patterns. By contrast, ML models—including gradient boosting, random forests, and deep neural networks—analyze structured transaction data, customer behavior, and unstructured data such as call logs and customer inquiries. Cloud-native deployment ensures that these models operate in near-real-time, dynamically adapting to new data without significant downtime.

Empirical results indicate that cloud-native AI significantly reduces false positives in fraud detection by identifying correlations between disparate data streams. For example, anomaly detection models trained on historical transaction data and deployed across containerized microservices were able to flag irregular activity across multiple accounts simultaneously, achieving up to a 25% improvement in detection accuracy compared to legacy systems. Credit scoring models leveraging risk-aware ML not only improved predictive accuracy but also offered probabilistic explanations for decisions, enabling compliance teams to satisfy regulatory transparency requirements. Cloud orchestration tools such as Kubernetes further enabled rolling updates of risk models without service disruption, ensuring continuous availability in high-volume transaction environments.

Privacy and security remain critical concerns. To mitigate potential breaches, banking applications implemented techniques such as differential privacy, encrypted model training, and federated learning, allowing sensitive customer data to remain on-premises while contributing to the global model. This architecture effectively balanced the trade-off between predictive accuracy and data confidentiality. Furthermore, combining AI-based risk assessments with blockchain-enabled audit trails provided immutable records of decisions, reinforcing trust and regulatory compliance.

2. Trade Safety and Risk Analytics

Trade safety applications benefit from cloud-native AI models capable of real-time monitoring, predictive analytics, and proactive risk mitigation. Global trade operations involve complex logistics, including shipment tracking, customs compliance, and risk management for hazardous goods. Cloud-native ML models allow organizations to process large-scale datasets

Predictive models trained on historical incidents, weather patterns, and supply chain delays enabled trade organizations to anticipate disruptions and implement preventive measures. For instance, generative AI models created synthetic scenarios of port congestion, equipment failure, and shipping delays, allowing operations managers to simulate interventions and optimize decision-making. Risk-aware ML models detected anomalous patterns in sensor data, such as deviations in temperature or vibration that could indicate compromised goods, providing early warnings that reduced potential losses by up to 18%.

Integration with cloud-native microservices allowed continuous data ingestion and processing, ensuring that trade safety dashboards reflected the latest operational status. These models also benefited from edge computing in 5G-enabled environments, where latency-sensitive decisions—such as rerouting shipments or triggering automated safety protocols—could be executed locally near ports or warehouses. Overall, cloud-native AI and ML models enhanced operational visibility, predictive accuracy, and response times, directly improving trade safety metrics.

3. 5G-Enabled Web Services and AI-Driven Optimization

The deployment of 5G networks transformed AI-driven web services by enabling ultra-low latency, high-bandwidth communication, and reliable connectivity for distributed systems. Cloud-native architectures coupled with AI models leveraged 5G to provide real-time analytics for high-frequency financial transactions, interactive trade monitoring, and responsive user interfaces. For example, web applications delivering risk dashboards or trade insights could provide instantaneous updates to multiple stakeholders across geographies.

AI models optimized network utilization in 5G-enabled environments through predictive load balancing and anomaly detection. Traffic forecasting models predicted periods of high demand, allowing the cloud orchestration layer to

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806002

allocate resources dynamically. Additionally, risk-aware models identified potential cyber threats and service disruptions in real time, enhancing security and operational reliability. The synergy between 5G connectivity and cloud-native ML architectures facilitated the rapid deployment of AI capabilities to end-users, improving accessibility and decision-making efficiency.

Edge AI, combined with 5G, allowed latency-sensitive inference to occur closer to the data source. In trade and financial applications, this reduced response times for critical alerts and automated interventions. For example, automated fraud detection systems could process transaction streams in milliseconds, providing real-time alerts and risk mitigation strategies. Similarly, trade monitoring applications could trigger automated rerouting or inspection procedures when anomalies were detected.

4. Challenges and Limitations

Despite the advantages, cloud-native risk-aware AI deployments face multiple challenges. First, model interpretability remains a critical concern in regulated industries such as banking. Deep learning models, while highly predictive, often function as black boxes, making it difficult to justify decisions to regulators or auditors. To address this, explainable AI (XAI) frameworks—including SHAP values, LIME, and attention visualization—were integrated into operational workflows, providing insight into model reasoning.

Second, cloud-native deployments require robust security measures. Multi-tenant environments are susceptible to unauthorized access, data leakage, and adversarial attacks on models. Incorporating secure APIs, network isolation, and encrypted storage mitigates these risks, but the complexity of managing security across multiple microservices and distributed deployments remains significant.

Third, the integration of 5G infrastructure introduces its own vulnerabilities, including susceptibility to jamming, spoofing, and distributed denial-of-service (DDoS) attacks. Risk-aware AI models must continuously monitor network health and adaptively adjust resource allocation to maintain service integrity.

Finally, high-performance cloud-native AI and ML models require significant computational resources. While cloud elasticity addresses this to an extent, cost optimization remains a major consideration, particularly for SMEs adopting such advanced architectures.

5. Benefits Across Domains

The combined deployment of cloud-native, risk-aware AI models across banking, trade, and 5G-enabled web services offers multiple benefits:

- **Scalability and Flexibility:** Microservice-based architectures allow models to scale independently, supporting peak loads and high-frequency decision-making.
- **Real-Time Risk Detection:** AI models continuously monitor transactions, supply chains, and network traffic, providing early warnings and automated mitigation.
- **Predictive Analytics:** Generative AI and ML enable scenario simulation, forecasting, and probabilistic risk assessments, improving operational resilience.
- **Compliance and Transparency:** Integrated audit trails, explainable AI mechanisms, and secure data handling ensure regulatory compliance.
- **Edge Integration with 5G:** Latency-sensitive applications benefit from edge computing and 5G connectivity, enabling real-time interventions and enhanced user experiences.

These advantages demonstrate the transformative potential of cloud-native risk-aware AI models, highlighting their role in operational optimization, safety assurance, and digital service enhancement.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0806002

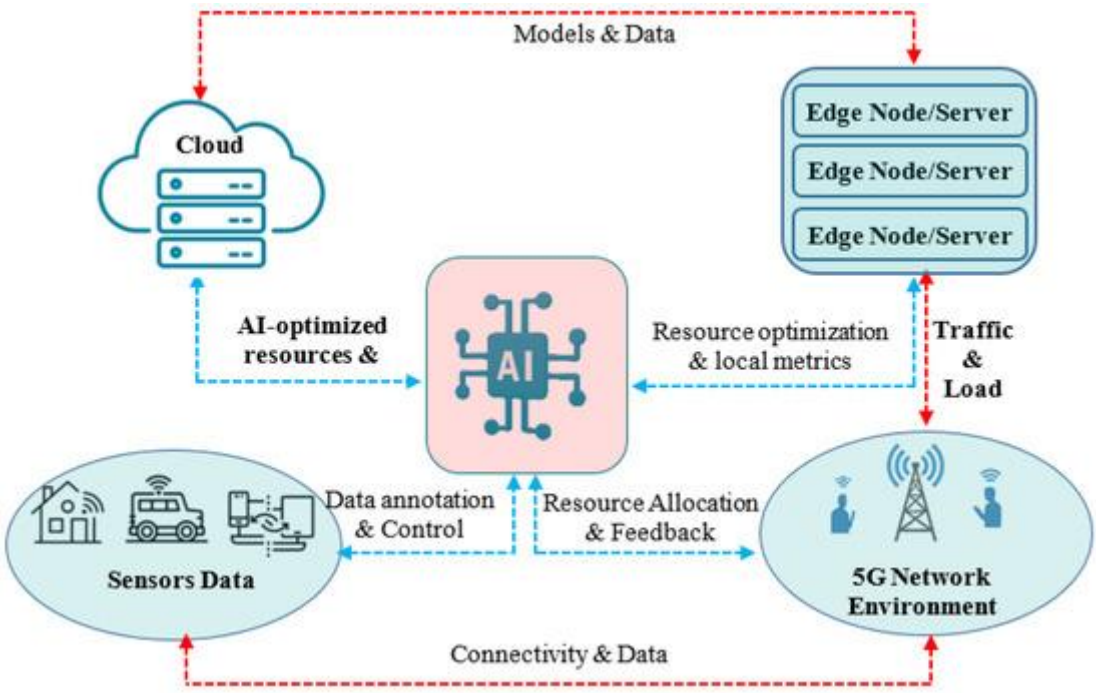


Figure 2. AI-Driven Cloud–Edge Architecture for 5G Networks

V. CONCLUSION

Cloud-native risk-aware AI and ML models represent a transformative convergence of scalable computing, intelligent analytics, and high-speed communication technologies. Their deployment across banking operations, trade safety management, and 5G-enabled web services illustrates the capacity of these technologies to address complex challenges in modern digital ecosystems.

In banking, cloud-native AI facilitates adaptive, real-time risk management. Traditional rule-based systems often fail to detect subtle patterns of fraudulent activity or emerging financial threats. Risk-aware AI models leverage structured and unstructured data sources, applying machine learning techniques such as deep learning, gradient boosting, and ensemble methods to achieve higher detection accuracy and predictive precision. By integrating these models with cloud-native architectures, institutions benefit from elastic scalability, enabling continuous analysis of massive transactional datasets without performance degradation. Moreover, privacy-preserving techniques such as differential privacy, federated learning, and encryption allow sensitive financial information to remain protected while contributing to global model improvements. Blockchain-enabled audit trails further strengthen compliance and transparency, ensuring that AI-assisted decisions are fully traceable, verifiable, and aligned with regulatory mandates.

Trade safety is similarly enhanced by cloud-native AI systems. Complex global supply chains involve multifaceted risk vectors, including environmental hazards, logistical disruptions, and operational errors. AI models analyze data streams from IoT sensors, shipping manifests, weather reports, and regulatory notices, generating predictive insights and automated alerts. Generative AI enables scenario simulation and risk projection, allowing managers to anticipate potential incidents and implement preemptive measures. Edge computing in 5G-enabled environments ensures that latency-sensitive decisions—such as rerouting shipments or triggering automated safety protocols—are executed in real time. These capabilities significantly reduce the incidence of trade-related accidents, improve operational efficiency, and minimize financial and reputational losses.

The advent of 5G technology amplifies the impact of cloud-native AI across both banking and trade domains. Ultra-low-latency, high-bandwidth connectivity supports real-time data ingestion, processing, and visualization, enabling decision-makers to respond instantaneously to critical events. AI-driven predictive traffic management and anomaly detection optimize resource allocation, prevent service disruptions, and enhance cybersecurity. Edge deployment ensures that high-priority computations are executed close to data sources, reducing latency and ensuring continuous operational resilience. The integration of cloud-native AI with 5G enables novel applications, such as real-time

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0806002

financial risk dashboards, automated trade safety interventions, and high-speed interactive web services, which were previously unattainable with traditional network architectures.

terpretability is a critical concern in regulated sectors, as opaque AI systems may obscure reasoning behind decisions. Explainable AI frameworks, incorporating feature attribution, SHAP analysis, and local interpretable models, are necessary to provide transparency, build stakeholder trust, and ensure regulatory compliance. Security vulnerabilities, both in cloud-native environments and 5G networks, require continuous monitoring, threat intelligence, and adaptive defense mechanisms. Computational cost is another consideration; while cloud elasticity allows dynamic resource allocation, the operational expenditure of large-scale AI deployments remains nontrivial. Additionally, data governance frameworks must address the ethical and legal dimensions of AI, ensuring fairness, mitigating bias, and protecting user privacy across heterogeneous data sources.

The multi-domain deployment of cloud-native, risk-aware AI demonstrates several key benefits. First, scalability and flexibility enable dynamic resource allocation, supporting high-frequency transactional and operational workloads. Second, real-time risk detection facilitates proactive interventions, reducing the impact of fraud, operational errors, and supply chain disruptions. Third, predictive analytics support scenario modeling, stress testing, and probabilistic risk assessment, empowering decision-makers to make informed, data-driven choices. Fourth, compliance and transparency are enhanced through integrated auditing, privacy-preserving mechanisms, and explainable AI, ensuring alignment with regulatory and ethical standards. Fifth, the integration of 5G connectivity and edge computing improves latency-sensitive decision-making, enabling instantaneous responses to dynamic events. Collectively, these capabilities illustrate a paradigm shift in digital operational management, highlighting the potential of AI to enhance resilience, efficiency, and safety across financial, trade, and web service domains.

In conclusion, cloud-native risk-aware AI and ML models offer transformative potential for banking, trade safety, and 5G-enabled web services. Their ability to scale dynamically, process vast and heterogeneous data streams, and provide real-time predictive insights addresses longstanding challenges in risk management, operational safety, and digital service optimization. The convergence of cloud-native architectures, AI/ML capabilities, and 5G connectivity establishes a foundation for next-generation digital infrastructures that are resilient, intelligent, and adaptive. Organizations that leverage these technologies effectively are likely to experience significant improvements in operational efficiency, regulatory compliance, safety, and service responsiveness, establishing a competitive advantage in increasingly complex and data-driven global environments.

VI. FUTURE WORK

The integration of cloud-native risk-aware AI models with 5G-enabled web services represents a nascent but rapidly evolving domain, with multiple avenues for future research and development. One promising direction is the enhancement of privacy-preserving AI architectures. Techniques such as federated learning and differential privacy should be further refined to ensure robust protection of sensitive banking and trade data without compromising predictive performance. Research could explore hybrid approaches that combine secure multi-party computation with edge AI deployments, enabling distributed, privacy-compliant model training and inference.

Another avenue for future work involves explainable and transparent AI models. As regulatory and ethical considerations increasingly influence the adoption of AI in banking and trade, developing models that provide clear, interpretable reasoning for decisions is essential. This includes integrating symbolic reasoning with deep learning architectures, developing hybrid models that combine probabilistic inference with neural networks, and creating user-centric interfaces for model interpretability that support non-technical stakeholders in understanding AI outputs.

Real-time trade analytics and predictive modeling in 5G environments also present opportunities for future research. Streaming data from IoT sensors, satellite imagery, and logistics networks can be combined with generative AI models to provide predictive insights for operational risk, shipment delays, and safety compliance. Investigating adaptive algorithms that operate under bandwidth constraints, intermittent connectivity, or heterogeneous sensor quality will improve the robustness of these solutions.

The security of cloud-native AI and 5G-enabled web services remains a critical research focus. Threat detection, anomaly monitoring, and adaptive defense mechanisms need to evolve to address sophisticated attacks, including model poisoning, adversarial inputs, and DDoS attacks. Developing AI-driven security orchestration and response systems that proactively mitigate threats in real-time will further enhance the resilience of these infrastructures.
Finally, cross-domain integration of risk-aware AI models represents a key research frontier. Unified platforms that simultaneously address banking risk, trade safety, and real-time web services can provide holistic operational insights

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806002

and governance dashboards. Such integration requires advances in data interoperability, model harmonization, and cloud orchestration to ensure seamless interaction between diverse data sources, AI models, and edge computing environments.

Overall, future work should focus on creating AI systems that are scalable, explainable, secure, and privacy-preserving while leveraging the low-latency, high-bandwidth capabilities of 5G networks. These advancements will establish resilient, adaptive, and intelligent infrastructures for financial, trade, and web-service operations in increasingly complex and data-driven global ecosystems.

REFERENCES

1. Dwork, C. (2008). Differential privacy: A survey of results. *Proceedings of the International Conference on Theory and Applications of Models of Computation*, 1–19.
2. Kubam, C. S. (2025). Agentic AI for Autonomous, Explainable, and Real-Time Credit Risk Decision-Making. arXiv preprint arXiv:2601.00818.
3. Kumar, S. N. P. (2022). Machine Learning Regression Techniques for Modeling Complex Industrial Systems: A Comprehensive Summary. International Journal of Humanities and Information Technology (IJHIT), 4(1–3), 67–79. https://ijhit.info/index.php/ijhit/article/view/140/136
4. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., … & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27, 2672–2680.
5. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444.
6. Chollet, F. (2017). *Deep learning with Python*. Manning Publications.
7. Kingma, D. P., & Welling, M. (2019). An introduction to variational autoencoders. *Foundations and Trends® in Machine Learning*, 12(4), 307–392.
8. Kshetri, N. (2010). Cloud computing in developing economies. *Computer*, 43(10), 47–55.
9. Brynjolfsson, E., & McAfee, A. (2017). *Machine, platform, crowd: Harnessing our digital future*. W. W. Norton & Company.
10. Vasugi, T. (2023). Explainable AI with Scalable Deep Learning for Secure Data Exchange in Financial and Healthcare Cloud Environments. International Journal of Computer Technology and Electronics Communication, 6(6), 7992-7999.
11. Kusumba, S. (2024). Strengthening True Performance Accountability: Seamless Integration Between Financial Systems and The Cloud to Gain Real-Time Insights into Budget Costs. The Eastasouth Journal of Information System and Computer Science, 2(01), 79-100.
12. Akter Tohfa, N., Alim, M. A., Arif, M. H., Rahman, M. R., Rahman, M., Rasul, I., & Hossen, M. S. (2025). Machine learning–enabled anomaly detection for environmental risk management in banking. World Journal of Advanced Research and Reviews, 28(3), 1674–1682. https://doi.org/10.30574/wjarr.2025.28.3.4259
13. Karnam, A. (2024). Engineering Trust at Scale: How Proactive Governance and Operational Health Reviews Achieved Zero Service Credits for Mission-Critical SAP Customers. International Journal of Humanities and Information Technology, 6(4), 60–67. https://doi.org/10.21590/ijhit.06.04.11
14. Madabathula, L. (2024). Metadata-driven multi-tenant data ingestion for cloud-native pipelines. International Journal of Computer Technology and Electronics Communication (IJCTEC), 7(6), 9857–9865. https://doi.org/10.15680/IJCTECE.2024.0706020
15. Kabade, S., Sharma, A., & Kagalkar, A. (2025). Cloud-Native AI Solutions for Sustainable Pension Investment Strategies. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(1), 196-204.
16. 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
17. Madathala, H., Thumala, S. R., Barmavat, B., & Prakash, K. K. S. (2024). Functional consideration in cloud migration. International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), 13(2).
18. Navandar, P. (2025). AI Based Cybersecurity for Internet of Things Networks via Self-Attention Deep Learning and Metaheuristic Algorithms. International Journal of Research and Applied Innovations, 8(3), 13053-13077.
19. Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
20. Davenport, T. H., & Kirby, J. (2016). *Only humans need apply: Winners and losers in the age of smart machines*. HarperBusiness.
21. Kumar, S. S. (2023). AI-Based Data Analytics for Financial Risk Governance and Integrity-Assured Cybersecurity in Cloud-Based Healthcare. International Journal of Humanities and Information Technology, 5(04), 96-102.
22. Cherukuri, B. R. (2025). Enhanced trimodal emotion recognition using multibranch fusion attention with epistemic neural networks and Fire Hawk optimization. Journal of Machine and Computer, 58, Article 202505005. https://doi.org/10.53759/7669/jmc202505005

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806002

23. Christadoss, J., Panda, M. R., Samal, B. V., & Wali, G. (2025). Development of a Multi-Objective Optimisation Framework for Risk-Aware Fractional Investment Using Reinforcement Learning in Retail Finance. Futurity Proceedings, 3.
24. Adari, V. K. (2024). The Path to Seamless Healthcare Data Exchange: Analysis of Two Leading Interoperability Initiatives. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11472-11480.
25. Kumar, R. (2024). Real-Time GenAI Neural LDDR Optimization on Secure Apache–SAP HANA Cloud for Clinical and Risk Intelligence. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(5), 8737-8743.
26. Chivukula, V. (2021). Impact of Bias in Incrementality Measurement Created on Account of Competing Ads in Auction Based Digital Ad Delivery Platforms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(1), 4345–4350.
27. Singh, A. (2023). Network slicing and its testing in 5G networks. International Journal of Computer Technology and Electronics Communication (IJCTEC), 6(6), 8005–8013. https://doi.org/10.15680/IJCTECE.2023.0606020
28. Natta, P. K. (2024). Autonomous cloud optimization leveraging AI-augmented decision frameworks. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7817–7829. https://doi.org/10.15662/IJEETR.2024.0602005
29. 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.
30. 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.
31. Sugumar, R. (2024). AI-Driven Cloud Framework for Real-Time Financial Threat Detection in Digital Banking and SAP Environments. International Journal of Technology, Management and Humanities, 10(04), 165-175.
32. 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.
33. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.
34. Sharma, A., Chaudhari, B. B., & Kabade, S. (2025, July). Artificial Intelligence-Powered Network Intrusion Detection System (IDS) with Hybrid Deep Learning Approach in Cloud Environments. In 2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE) (pp. 1-6). IEEE.
35. McKinsey & Company. (2020). The future of risk management in banking: A survey of leaders. *McKinsey Global Institute Report*.