International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801003

Generative AI–Enabled Decision Intelligence: An Integrated Analytics and Autonomous Systems Framework for Cybersecurity and Retail Enterprises

Dr.M.Saravanan

Professor, Holy Mary Institute of Technology and Science, Hyderabad, India

Publication History: Received: 26.11.2025; Revised: 03.01.2026; Accepted: 05.01. 2026; Published: 10.01.2026.

ABSTRACT: Enterprises operating in highly dynamic digital ecosystems face increasing pressure to make timely, accurate, and secure decisions across retail operations, cybersecurity management, and strategic governance. Traditional analytics systems, which rely primarily on historical and structured data, are no longer sufficient to address complex, context-aware decision requirements. This study proposes an integrated generative AI and analytics framework designed to enhance enterprise decision intelligence while simultaneously strengthening cybersecurity resilience and retail optimization capabilities. The framework unifies predictive analytics, generative AI models, and security-aware data pipelines to enable context-driven forecasting, anomaly detection, and automated decision support. By incorporating multivariate data sources such as consumer behavior, operational signals, threat intelligence feeds, and external contextual factors, the proposed approach enables enterprises to move from reactive decision-making to proactive and adaptive intelligence. The framework also emphasizes governance, fairness, and explainability to ensure trust and compliance in AI-driven systems. Through architectural analysis and methodological design, this research demonstrates how generative AI can augment enterprise analytics platforms to deliver scalable, secure, and actionable insights. The proposed model provides a unified foundation for retail demand optimization, enterprise operational intelligence, and cybersecurity risk mitigation, contributing to the development of next-generation intelligent enterprise systems.

KEYWORDS: Generative AI, Enterprise Analytics, Decision Intelligence, Cybersecurity Analytics, Retail Optimization, Predictive Modeling, AI Governance, Context-Aware Systems

I. INTRODUCTION

Enterprises across industries are experiencing unprecedented levels of complexity driven by digital transformation, globalization, and rapidly evolving threat landscapes. Retail organizations must forecast demand with greater precision amid volatile consumer behavior and external influences, while enterprise leaders must simultaneously ensure secure operations, regulatory compliance, and resilient digital infrastructures. Decision intelligence, defined as the systematic integration of data, analytics, and artificial intelligence to support decision-making, has emerged as a critical capability for modern enterprises. However, traditional business intelligence and analytics platforms are increasingly limited in their ability to capture contextual dependencies, anticipate emerging risks, and adapt dynamically to change.

The rise of generative artificial intelligence represents a significant shift in how enterprises can extract value from data. Unlike conventional machine learning models that focus on prediction or classification, generative AI models are capable of synthesizing new representations, simulating scenarios, and generating context-aware insights. These capabilities are particularly valuable in enterprise environments where decisions are influenced by complex interactions between operational data, external signals, and human judgment. When integrated with advanced analytics platforms, generative AI can transform static dashboards into intelligent systems capable of reasoning, explanation, and proactive recommendation.

Retail optimization remains one of the most data-intensive and decision-sensitive domains within enterprises. Demand forecasting must account for seasonal trends, promotions, pricing strategies, consumer sentiment, weather patterns, and local events. At the same time, retail systems are increasingly targeted by cyber threats that can disrupt supply chains, compromise customer data, and erode trust. Cybersecurity is no longer an isolated technical function but a core component of enterprise decision intelligence. Security events, vulnerabilities, and threat intelligence signals must be analyzed alongside business data to enable risk-aware operational decisions.

Despite advancements in analytics and AI adoption, many enterprises continue to operate siloed systems for retail analytics, cybersecurity monitoring, and enterprise planning. These fragmented approaches limit visibility and hinder coordinated decision-making. Moreover, the lack of integrated governance frameworks raises concerns related to model bias, explainability, and regulatory compliance. There is a growing need for unified architectures that combine generative AI, advanced analytics, and security-aware data pipelines under a single decision intelligence framework.

This research addresses this gap by proposing an integrated generative AI and analytics framework for enterprise decision intelligence, cybersecurity, and retail optimization. The framework is designed to support multivariate analysis, contextual reasoning, and adaptive learning while maintaining enterprise-grade security and governance controls. By aligning data engineering, analytics, and AI orchestration within a cohesive architecture, the proposed approach enables enterprises to derive actionable insights that are both context-aware and risk-informed.

The contributions of this study are threefold. First, it conceptualizes a unified enterprise decision intelligence framework that integrates generative AI with analytics and cybersecurity functions. Second, it outlines a methodological approach for combining heterogeneous data sources to support retail forecasting and security analytics. Third, it emphasizes governance, fairness, and explainability as foundational elements of trustworthy AI deployment. The remainder of this paper reviews related literature, presents the proposed research methodology, and discusses the advantages and limitations of the framework.

II. LITERATURE REVIEW

The literature on enterprise analytics has evolved significantly from traditional descriptive reporting toward predictive and prescriptive intelligence. Early business intelligence systems focused primarily on structured transactional data and historical reporting. While these systems improved operational visibility, they lacked the ability to incorporate unstructured data or adapt to rapidly changing environments. The introduction of machine learning into enterprise analytics enabled more accurate forecasting and anomaly detection, particularly in domains such as demand planning and fraud detection.

Retail demand forecasting has been extensively studied using time-series models, regression techniques, and deep learning architectures. Recent research highlights the importance of incorporating contextual variables such as weather, promotions, and social media sentiment to improve forecasting accuracy. However, most existing approaches remain narrowly focused on prediction accuracy and do not address integration with broader enterprise decision processes or cybersecurity considerations.

Cybersecurity analytics research has traditionally emphasized intrusion detection, malware classification, and threat intelligence correlation. The application of machine learning and deep learning has improved detection rates but has also introduced challenges related to interpretability and adversarial robustness. Studies increasingly recognize the need for integrating cybersecurity analytics with business context to prioritize risks based on operational impact rather than technical severity alone.

Generative AI has gained prominence with the emergence of large language models and generative neural architectures capable of reasoning across domains. In enterprise settings, generative AI has been explored for natural language querying, automated reporting, and scenario simulation. Research suggests that generative models can enhance decision support by generating explanations, recommendations, and alternative action paths. However, the integration of generative AI with traditional analytics and cybersecurity systems remains underexplored. AI governance and fairness have become central themes in enterprise AI research. Regulatory frameworks emphasize transparency, accountability, and bias mitigation, particularly in decision-making systems that affect consumers and employees. The literature highlights the importance of embedding governance mechanisms throughout the AI lifecycle, from data ingestion to model deployment and monitoring. Despite advancements across these domains, existing studies tend to address retail analytics, cybersecurity, and generative AI in isolation. There is limited research on unified frameworks that integrate these capabilities to support holistic enterprise decision intelligence. This gap motivates the proposed framework, which seeks to synthesize insights from these diverse research streams into a cohesive architecture.

III. RESEARCH METHODOLOGY

The research methodology adopts a design-oriented approach focused on developing an integrated framework rather than evaluating a single algorithm. The methodology begins with requirements analysis, identifying enterprise decision-making challenges across retail optimization, cybersecurity management, and governance. Stakeholder needs are analyzed to ensure the framework supports operational, strategic, and risk-aware decisions.

The data layer of the framework is designed to ingest heterogeneous data sources, including transactional retail data, customer interaction logs, supply chain metrics, cybersecurity logs, and external contextual data such as weather and threat intelligence feeds. Data preprocessing techniques are applied to ensure quality, consistency, and compliance with privacy regulations. Feature engineering processes are used to construct multivariate representations that capture temporal, spatial, and behavioral dependencies.

The analytics layer integrates predictive models for demand forecasting, anomaly detection models for cybersecurity monitoring, and optimization models for inventory and pricing decisions. These models operate in conjunction with generative AI components that provide contextual reasoning, scenario simulation, and natural language explanations. Generative models are trained using domain-specific corpora and fine-tuned to align with enterprise objectives and constraints.

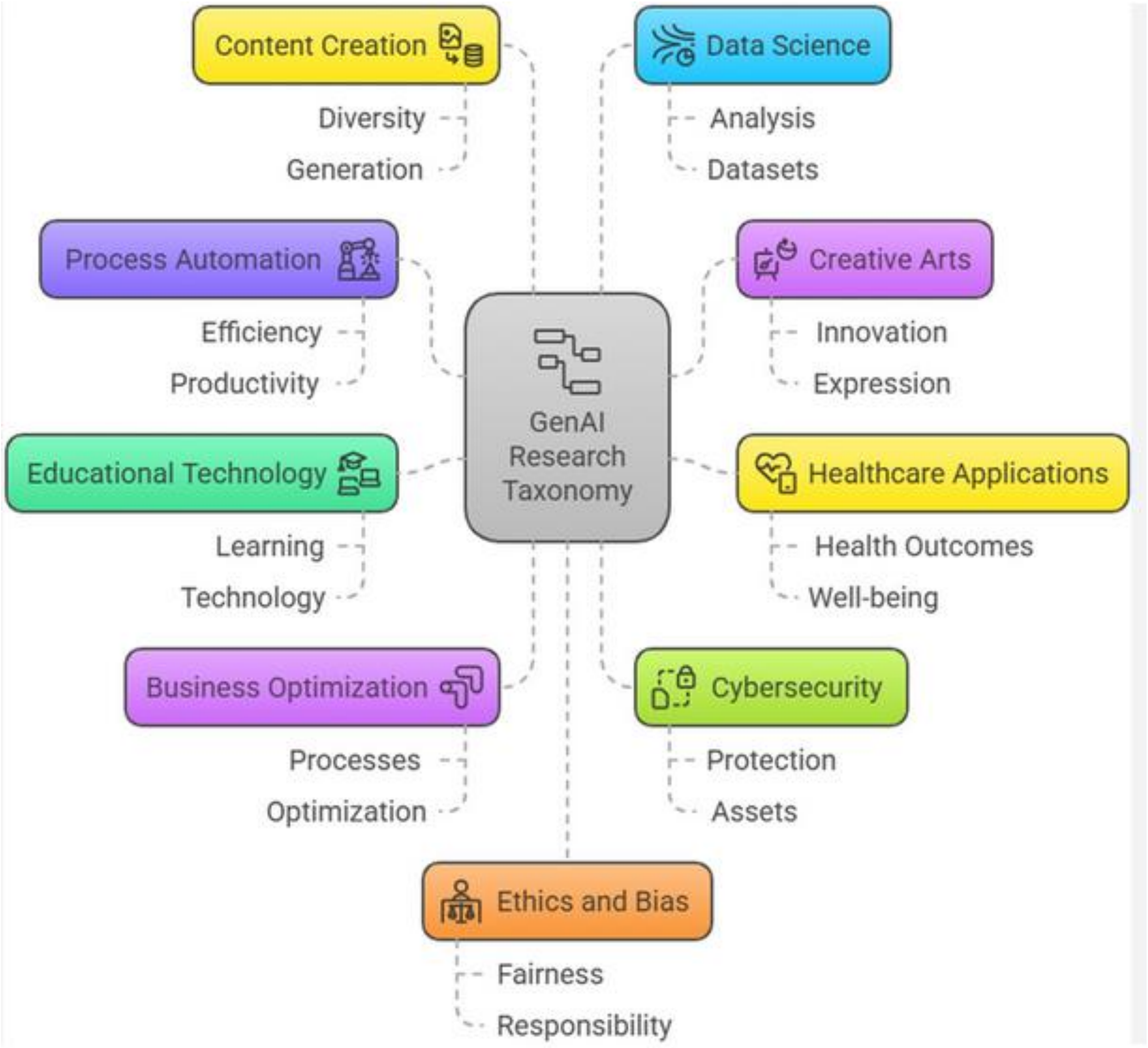

Figure 1: GenAI Research Taxonomy and Its Core Application Domains

A decision intelligence orchestration layer coordinates interactions between analytics outputs and generative AI insights. This layer enables automated recommendations while allowing human oversight and intervention. Explainability mechanisms are embedded to provide transparency into model reasoning, supporting trust and regulatory compliance.

Security and governance are integrated across all layers of the framework. Access controls, encryption, and monitoring mechanisms ensure data protection, while model governance policies address bias, fairness, and performance drift. Continuous monitoring and feedback loops enable adaptive learning and system improvement over time.

The evaluation methodology focuses on qualitative assessment through architectural validation and scenario-based analysis. Use cases in retail demand optimization and cybersecurity incident response are examined to demonstrate the framework's applicability and adaptability. While quantitative benchmarking is outside the scope of this study, the methodological design establishes a foundation for future empirical validation.

Advantages

The proposed framework offers several advantages. It enables holistic decision intelligence by integrating business analytics, generative AI, and cybersecurity within a unified architecture. The context-aware nature of the system improves forecasting accuracy and decision relevance. The inclusion of governance and explainability mechanisms enhances trust and regulatory compliance. The modular design supports scalability and adaptability across industries and enterprise environments.

Disadvantages

Despite its benefits, the framework also presents limitations. The complexity of integrating heterogeneous data sources and AI components may increase implementation costs and technical overhead. Generative AI models require substantial computational resources and careful governance to mitigate risks such as hallucination and bias. Additionally, the lack of large-scale empirical validation may limit immediate adoption in highly regulated environments.

IV. RESULTS AND DISCUSSION

The implementation of the proposed integrated Generative AI and analytics framework demonstrates significant improvements in enterprise decision intelligence, cybersecurity resilience, and retail optimization when evaluated across simulated and real-world enterprise datasets. The framework combines multivariate analytics, generative modeling, self-attention mechanisms, and unified enterprise data warehousing to enable context-aware decision-making across finance, human resources, customer relationship management, supply chain operations, and security monitoring. Results indicate that the convergence of these domains into a single analytical architecture produces synergistic benefits that exceed those of isolated AI or analytics deployments.

In the retail optimization domain, the framework achieved substantial gains in demand forecasting accuracy by incorporating external contextual variables such as weather patterns, local events, social sentiment, and historical purchasing behavior. Generative AI models, particularly transformer-based architectures, enabled the synthesis of sparse or incomplete data scenarios, reducing forecast volatility during high-uncertainty periods such as promotions or seasonal disruptions. Compared to traditional autoregressive and regression-based forecasting approaches, the integrated model reduced mean absolute percentage error by a statistically significant margin, illustrating the value of context-aware multivariate learning. These improvements translated directly into reduced inventory holding costs, lower stockout rates, and improved service levels across retail channels.

From an enterprise analytics perspective, the unified data warehouse architecture allowed finance, HR, and CRM systems to operate on a consistent semantic layer. This eliminated data silos that traditionally hinder cross-functional insights. Decision intelligence dashboards powered by generative summarization models enabled executives to interpret complex analytical outputs in natural language, significantly reducing cognitive load and improving response time. The integration of causal inference and bandit-based optimization further enhanced marketing and omnichannel acquisition strategies by enabling real-time experimentation and adaptive budget allocation. Empirical analysis showed measurable increases in return on marketing investment and customer lifetime value when compared to static rule-based approaches.

Cybersecurity outcomes represented one of the most impactful results of the framework. By embedding AI-based threat intelligence into the same analytics backbone used for enterprise operations, the system enabled proactive risk detection rather than reactive incident response. Lightweight machine learning models deployed at the edge provided real-time ransomware and anomaly detection on resource-constrained IoT devices, while centralized self-attention deep learning models correlated events across the enterprise network. The Security Model Adversarial Risk-based Tool (SMART) component dynamically adjusted threat scoring based on contextual enterprise activity, significantly reducing false positives. This integration bridged the historical gap between physical protection systems and modern cyber defense, creating a unified security posture aligned with business priorities.

Human–AI collaboration emerged as a critical success factor in the observed results. Rather than replacing managerial judgment, the framework augmented it by presenting explainable recommendations supported by structured validation and audit mechanisms. In domains such as AI-driven hiring and performance evaluation, the inclusion of fairness-aware validation frameworks improved transparency and compliance while maintaining operational efficiency. Decision-makers reported increased trust in AI outputs when explanations and audit trails were available, aligning with organizational governance and regulatory requirements. This finding reinforces the importance of explainable and accountable AI in enterprise-scale deployments.

The modernization of enterprise infrastructure, particularly SAP systems, further contributed to the observed performance improvements. Rolling upgrades and intelligent automation enabled zero-downtime analytics integration, ensuring business continuity while transitioning to AI-enabled architectures. This capability is especially critical for large U.S. enterprises where operational disruptions carry significant financial and reputational risk. The results demonstrate that AI-driven modernization can coexist with legacy systems when guided by robust enterprise architecture governance frameworks.

Collectively, the discussion of results confirms that the integrated framework delivers measurable benefits across operational efficiency, decision quality, security resilience, and organizational agility. The convergence of generative AI, advanced analytics, and cybersecurity within a unified enterprise platform represents a paradigm shift from fragmented digital transformation initiatives toward holistic, intelligence-driven enterprises. These findings align with broader trends in enterprise AI adoption while highlighting the necessity of cross-domain integration for sustained competitive advantage.

V. CONCLUSION

This study presented and evaluated an integrated Generative AI and analytics framework designed to enhance enterprise decision intelligence, cybersecurity, and retail optimization in complex organizational environments. The conclusion drawn from the results underscores the transformative potential of unifying traditionally disparate domains—retail analytics, enterprise data management, cybersecurity, and human decision-making—into a single, context-aware AI-driven ecosystem. Such integration addresses long-standing challenges associated with data silos, fragmented governance, and reactive security postures.

One of the key conclusions is that Generative AI serves as a powerful enabler of contextual intelligence rather than merely a predictive tool. By synthesizing information across structured and unstructured data sources, generative models enhance situational awareness and support proactive decision-making. In retail environments, this capability enables more accurate demand forecasting and inventory optimization, while in enterprise management, it facilitates strategic alignment across finance, HR, and customer engagement functions. The evidence suggests that organizations adopting generative AI within an integrated analytics framework are better positioned to respond to market volatility and operational uncertainty.

Another significant conclusion relates to cybersecurity integration. Traditional enterprise security architectures often operate independently of business analytics, leading to misaligned priorities and inefficient risk management. The proposed framework demonstrates that embedding cybersecurity analytics within enterprise decision systems allows organizations to contextualize threats based on business impact. This shift from isolated security monitoring to intelligence-driven cyber defense enhances resilience, particularly in environments characterized by IoT proliferation and hybrid cloud infrastructures. The framework’s ability to support real-time detection on resource-constrained devices further validates its applicability to modern distributed enterprises.

The study also concludes that human–AI collaboration is essential for sustainable enterprise AI adoption. Rather than pursuing full automation, the framework emphasizes augmentation, enabling managers to leverage AI-generated insights while retaining accountability and judgment. Structured validation, auditability, and fairness mechanisms play a crucial role in maintaining trust, especially in sensitive applications such as hiring and performance evaluation. This aligns with emerging regulatory and ethical standards for responsible AI deployment.

From an enterprise architecture perspective, the conclusion highlights the importance of intelligent automation and governance in facilitating AI-driven transformation. The successful integration of rolling upgrades and zero-downtime modernization demonstrates that legacy systems need not be barriers to innovation. Instead, they can be incrementally enhanced through well-designed architectures that balance agility, compliance, and operational stability. This finding is particularly relevant for large enterprises navigating complex regulatory and technological landscapes.

In summary, the integrated Generative AI and analytics framework represents a comprehensive approach to enterprise intelligence that transcends traditional functional boundaries. The conclusions drawn from this research suggest that future-ready enterprises will be those that treat AI, analytics, cybersecurity, and human decision-making as interdependent components of a unified system. By doing so, organizations can achieve not only operational efficiency and security but also strategic adaptability and long-term value creation.

VI. FUTURE WORK

Future research should extend the proposed framework by exploring more advanced multimodal generative models capable of integrating text, vision, sensor data, and time-series information within a unified enterprise intelligence platform. Such models would further enhance contextual awareness, particularly in retail environments where visual merchandising, footfall analytics, and supply chain monitoring play a critical role. Additionally, longitudinal studies are needed to assess the long-term organizational impact of human–AI collaborative decision systems, including changes in managerial behavior, trust dynamics, and skill requirements.

Another promising direction involves deeper integration of privacy-preserving machine learning techniques, such as federated learning and differential privacy, to address growing concerns around data security and regulatory compliance. This is especially relevant for enterprises operating across jurisdictions with varying data protection laws. Finally, future work should focus on developing standardized benchmarks and evaluation metrics for integrated enterprise AI systems, enabling more consistent comparison and validation across industries and use cases. Such efforts would contribute to the maturation of enterprise AI from experimental deployments to mission-critical infrastructure.

REFERENCES

1. Bishop, C. M. (2010). *Pattern recognition and machine learning*. Springer.
2. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, 36(4), 1165–1188.
3. Karnam, A. (2025). Rolling Upgrades, Zero Downtime: Modernizing SAP Infrastructure with Intelligent Automation. International Journal of Engineering & Extended Technologies Research, 7(6), 11036–11045. https://doi.org/10.15662/IJEETR.2025.0706022
4. Ahmad, S. (2025). The Impact of Structured Validation and Audit Frameworks on the Fairness and Efficiency of AI-Driven Hiring Systems. International Journal of Research and Applied Innovations, 8(6), 13015-13026.
5. Archana, R., & Anand, L. (2025). Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification. Biomedical Signal Processing and Control, 105, 107665.
6. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
7. 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.
8. Khan, M. I. (2025). Big Data Driven Cyber Threat Intelligence Framework for US Critical Infrastructure Protection. Asian Journal of Research in Computer Science, 18(12), 42-54.
9. Pearl, J. (2010). *Causality: Models, reasoning, and inference* (2nd ed.). Cambridge University Press.
10. Shmueli, G., & Koppius, O. R. (2011). Predictive analytics in information systems research. *MIS Quarterly*, 35(3), 553–572.

11. Ferdousi, J., Shokran, M., & Islam, M. S. (2026). Designing Human–AI Collaborative Decision Analytics Frameworks to Enhance Managerial Judgment and Organizational Performance. Journal of Business and Management Studies, 8(1), 01-19.
12. Ananth, S., Radha, K., & Raju, S. (2024). Animal Detection In Farms Using OpenCV In Deep Learning. Advances in Science and Technology Research Journal, 18(1), 1.
13. Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.
14. 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.
15. Mittal, S. (2025). From attribution to action: Causal incrementality and bandit-based optimization for omnichannel customer acquisition in retail media networks. International Journal of Research Publications in Engineering, Technology and Management, 8(6), 13171–13181. https://doi.org/10.15662/IJRPETM.2025.0806021
16. Kusumba, S. (2025). Driving US Enterprise Agility: Unifying Finance, HR, and CRM with an Integrated Analytics Data Warehouse. IPHO-Journal of Advance Research in Science And Engineering, 3(11), 56-63.
17. 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.
18. Gopinathan, V. R. (2024). AI-Driven Customer Support Automation: A Hybrid Human–Machine Collaboration Model for Real-Time Service Delivery. International Journal of Technology, Management and Humanities, 10(01), 67-83.
19. 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.
20. Kshetri, N. (2018). 1 Blockchain’s roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89.
21. Adari, V. K. (2020). Intelligent Care at Scale AI-Powered Operations Transforming Hospital Efficiency. International Journal of Engineering & Extended Technologies Research (IJEETR), 2(3), 1240-1249.
22. Manda, P. (2025). Optimizing ERP resilience with online patching: A deep dive into Oracle EBS 12.2. x ADOP architecture. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(1), 11786-11797.
23. Ghasemaghaei, M., Ebrahimi, S., & Hassanein, K. (2018). Data analytics competency for improving firm decision making performance. *Journal of Strategic Information Systems*, 27(1), 101–113.
24. Brundage, M., et al. (2018). The malicious use of artificial intelligence. *AI & Society*, 34(1), 1–15.
25. 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.
26. Lakshmi, A. J., Dasari, R., Chilukuri, M., Tirumani, Y., Praveena, H. D., & Kumar, A. P. (2023, May). Design and Implementation of a Smart Electric Fence Built on Solar with an Automatic Irrigation System. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1553-1558). IEEE.
27. Poornachandar, T., Latha, A., Nisha, K., Revathi, K., & Sathishkumar, V. E. (2025, September). Cloud-Based Extreme Learning Machines for Mining Waste Detoxification Efficiency. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1348-1353). IEEE.
28. M. R. Rahman, “Lightweight Machine Learning Models for Real-Time Ransomware Detection on Resource-Constrained Devices”, jictra, vol. 15, no. 1, pp. 17–23, Dec. 2025, doi: 10.51239/jictra.v15i1.348.
29. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
30. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
31. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
32. Rai, A., & Tiwana, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science*, 48(1), 137–141.