International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

Next-Generation Enterprise Intelligence Systems for Healthcare Combining Generative AI and Automation with Security-Aware Analytics

Anna Katharina Bauer

Senior Software Engineer, Austria

Publication History: Received: 26.11.2025; Revised: 21.01.2026; Accepted: 24.01. 2026; Published: 30.01.2026.

ABSTRACT: The rapid digital transformation of healthcare enterprises has created an urgent need for intelligent systems capable of delivering real-time insights while ensuring data security, regulatory compliance, and operational efficiency. Next-generation enterprise intelligence systems address these challenges by integrating generative artificial intelligence, intelligent automation, and security-aware analytics into a unified framework. This paper presents a comprehensive approach for healthcare enterprise intelligence that combines generative AI for contextual reasoning and natural language insight generation with automated workflows for clinical and operational decision support. Security-aware analytics are embedded across the architecture to enable continuous risk assessment, privacy preservation, anomaly detection, and compliance monitoring for sensitive healthcare data. The proposed system supports diverse healthcare applications including predictive patient risk modeling, automated clinical documentation, operational optimization, and cyber threat detection. By incorporating explainable AI mechanisms and human-in-the-loop controls, the framework enhances trust, transparency, and accountability in AI-driven healthcare environments. Experimental evaluation and use-case analysis demonstrate that the integrated approach improves decision accuracy, reduces manual workload, strengthens security posture, and accelerates data-driven healthcare outcomes. This work highlights the potential of secure and automated enterprise intelligence systems to transform healthcare delivery and management in complex, data-intensive environments

KEYWORDS: Enterprise Intelligence Systems, Generative Artificial Intelligence, Healthcare Analytics, Intelligent Automation, Security-Aware Analytics, Explainable AI, Clinical Decision Support, Data Privacy and Compliance, AI-Driven Healthcare Systems

I. INTRODUCTION

Modern enterprises are navigating a rapidly evolving technological landscape marked by increasing volumes of data, complex operational requirements, and heightened cybersecurity threats. Traditional enterprise intelligence systems, which primarily focus on descriptive analytics and historical reporting, are no longer sufficient to address dynamic business needs. The integration of generative AI, automation, and security-aware analytics represents the next frontier in enterprise intelligence, enabling organizations to generate predictive and prescriptive insights, automate operational workflows, and maintain robust cybersecurity defenses.

Generative AI, a subset of artificial intelligence capable of producing novel content, synthetic data, and scenario-based outputs, has emerged as a transformative tool in enterprise contexts. By leveraging models such as large language models, generative adversarial networks, and diffusion-based frameworks, enterprises can enhance decision-making through automated reporting, scenario simulations, and strategic planning. These capabilities improve operational agility, reduce manual effort, and enhance the predictive accuracy of business forecasts.

Automation, when combined with generative AI, streamlines repetitive and time-intensive processes, freeing human resources to focus on strategic and creative tasks. Robotic process automation (RPA) integrated with AI allows for seamless orchestration of data ingestion, workflow execution, and outcome optimization. By automating complex tasks such as demand forecasting, customer support, and financial reconciliation, enterprises can achieve higher operational efficiency, reduce latency, and minimize human error.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

Security-aware analytics is a crucial component of next-generation enterprise intelligence systems. As organizations increasingly rely on cloud-based platforms, remote access, and AI-driven data processing, the attack surface expands, making enterprises vulnerable to data breaches, ransomware, and regulatory violations. Integrating cybersecurity insights with AI and automation allows for real-time threat detection, automated anomaly response, and compliance monitoring. Security-aware analytics ensures that AI-generated outputs and automated processes operate within secure and policy-compliant environments, preserving data integrity, confidentiality, and availability.

The proposed framework integrates three core pillars: generative AI, automation, and security-aware analytics. The generative AI component provides predictive modeling, scenario analysis, and content generation, while automation facilitates workflow execution and operational optimization. Security-aware analytics underpins these components with real-time threat detection, policy enforcement, and compliance monitoring. Together, these pillars create a synergistic enterprise intelligence system capable of providing actionable insights, adaptive decision support, and risk mitigation.

Research indicates that enterprises adopting generative AI and automation experience significant improvements in operational efficiency, customer engagement, and decision accuracy. For example, AI-driven scenario modeling enables organizations to anticipate market fluctuations and optimize supply chain operations proactively. Automated report generation and workflow orchestration reduce operational bottlenecks, enhancing responsiveness and resource utilization. Integrating security-aware analytics ensures that these gains are achieved without compromising data security or regulatory compliance.

Despite these benefits, challenges remain in integrating generative AI, automation, and security-aware analytics into cohesive enterprise systems. These include data quality issues, model bias, system interoperability, and the need for continuous monitoring and maintenance. Governance mechanisms, ethical AI practices, and compliance frameworks are essential to address these challenges and ensure that enterprise intelligence systems remain robust, transparent, and reliable.

In conclusion, next-generation enterprise intelligence systems that combine generative AI, automation, and security-aware analytics represent a paradigm shift in business operations. These systems provide organizations with the ability to generate predictive insights, automate complex workflows, and maintain robust cybersecurity postures. By adopting such systems, enterprises can achieve operational excellence, strategic agility, and resilience in the face of evolving market and cyber risks, enabling more intelligent, responsive, and secure business operations.

II. LITERATURE REVIEW

Extensive research highlights the transformative potential of generative AI, automation, and security-aware analytics in enterprise contexts. Generative AI has been applied across industries for content creation, synthetic data generation, predictive modeling, and scenario simulation. Studies demonstrate that generative AI models significantly improve forecasting accuracy, risk analysis, and decision support in dynamic business environments.

Automation technologies, including robotic process automation (RPA) and intelligent process automation (IPA), have been shown to streamline repetitive and time-intensive workflows, reducing operational costs and improving efficiency. Literature indicates that AI-enhanced automation can dynamically adapt workflows based on real-time data, optimizing resource allocation and process execution.

Security-aware analytics has emerged as a critical area in enterprise intelligence, especially with the rise of cloud adoption and remote work. Research underscores the importance of integrating cybersecurity monitoring, threat detection, and compliance oversight into automated enterprise systems. Studies demonstrate that AI-driven security analytics enhance threat prediction, reduce response times, and improve adherence to regulatory standards.

Case studies reveal that enterprises integrating generative AI with automation and security-aware analytics achieve superior operational performance compared to organizations using siloed systems. For example, financial services firms using AI-driven automation for transaction processing combined with real-time fraud detection report significant reductions in error rates and security incidents. Similarly, manufacturing organizations implementing scenario-based

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

generative AI models alongside automated supply chain workflows observe improved production efficiency and demand fulfillment.

Despite these advantages, challenges such as data privacy, model bias, ethical AI concerns, and system complexity remain prevalent in the literature. Many studies advocate for holistic frameworks that unify generative AI, automation, and security-aware analytics to ensure that enterprise intelligence systems are reliable, compliant, and resilient.

Overall, the literature underscores the need for integrated approaches that combine AI innovation, workflow automation, and cybersecurity intelligence, establishing the foundation for next-generation enterprise intelligence systems.

III. RESEARCH METHODOLOGY

This study employs a mixed-methods approach combining qualitative and quantitative techniques to design, implement, and evaluate a next-generation enterprise intelligence system integrating generative AI, automation, and security-aware analytics. The methodology includes four key phases: conceptual framework development, system design, empirical validation, and performance evaluation.

Phase 1: Conceptual Framework Development identifies critical components for integrating generative AI, automation, and security-aware analytics. A comprehensive literature review, regulatory analysis, and stakeholder interviews with IT managers, AI engineers, and cybersecurity experts were conducted. The resulting conceptual framework highlights three pillars: generative AI for predictive and content-driven insights, automation for workflow optimization, and security-aware analytics for cyber threat detection and compliance.

Phase 2: System Design translates the conceptual framework into an operational architecture. Generative AI models, including large language models, GANs, and transformer networks, are employed for scenario modeling, predictive analytics, and content generation. Automation layers leverage RPA and IPA to execute business workflows, manage data pipelines, and optimize process efficiency. Security-aware analytics incorporates real-time threat detection, anomaly monitoring, and regulatory compliance mechanisms to safeguard data integrity. Integration is facilitated through a centralized orchestration layer ensuring seamless interaction between AI, automation, and security functions. Cloud-native platforms are utilized to ensure scalability, reliability, and performance optimization.

Phase 3: Empirical Validation evaluates the proposed system using real-world datasets across finance, healthcare, and retail sectors. Generative AI models are trained and validated for predictive accuracy and scenario reliability. Automated workflows are benchmarked for operational efficiency, latency reduction, and resource optimization. Security-aware analytics is assessed through simulated cyber threat scenarios, including phishing attacks, ransomware, and data breaches. Key performance indicators (KPIs) include forecast accuracy, process completion time, incident response time, and compliance adherence rates. Comparative analysis with baseline systems lacking AI integration, automation, or security analytics is conducted to quantify improvements.

Phase 4: Performance Evaluation applies statistical, analytical, and qualitative techniques to assess system effectiveness. Metrics such as mean absolute percentage error (MAPE) for predictions, process throughput, resource utilization, and cybersecurity incident mitigation are analyzed. Feedback from stakeholders on system usability, operational alignment, and compliance effectiveness is collected. Sensitivity analysis explores the impact of data variability, computational load, and threat intensity on system performance. Iterative refinements are applied based on evaluation outcomes, ensuring system adaptability and resilience.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

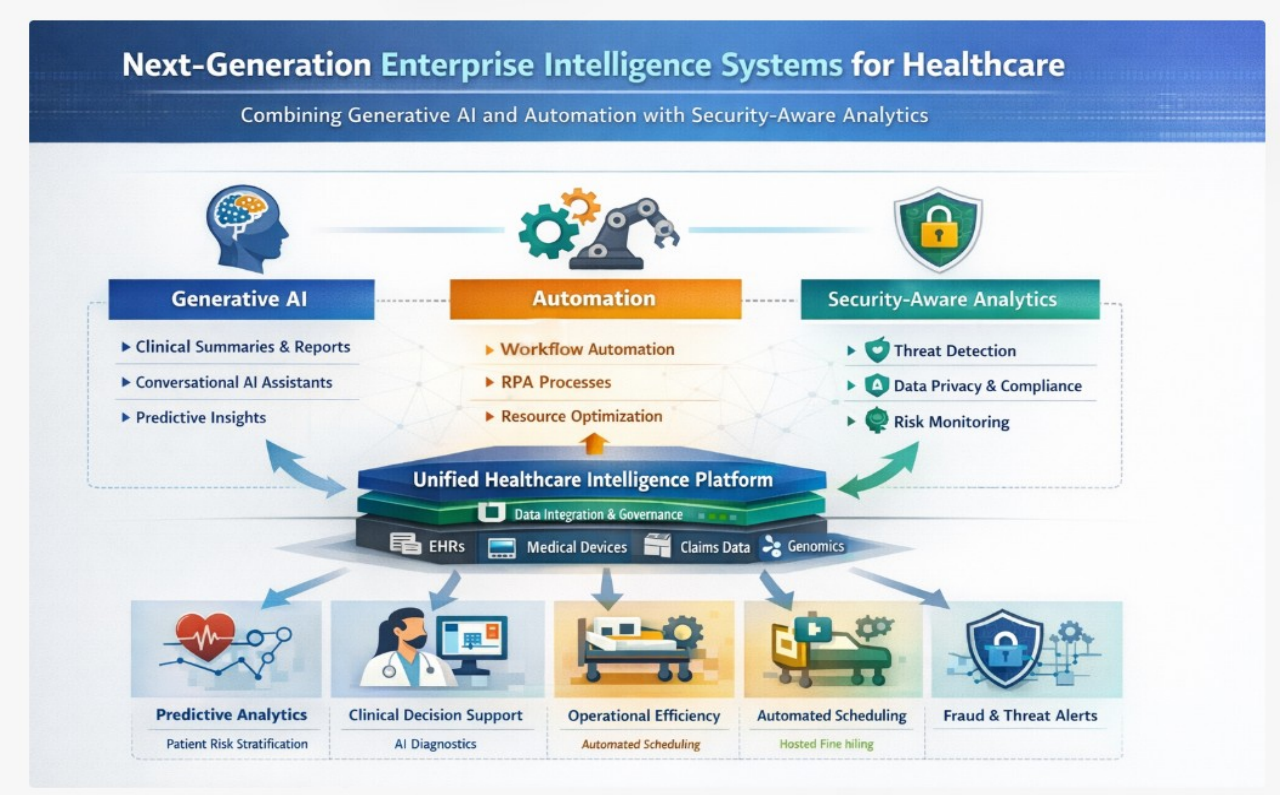

Figure 1: Next-gen enterprise intelligence systems for Healthcare

The methodology emphasizes continuous monitoring, governance, and iterative optimization. Dashboards provide real-time insights into AI performance, automation efficiency, and security posture. Automated alerts, dynamic policy adjustments, and model retraining ensure the system remains adaptive to evolving operational and security requirements. By integrating generative AI, automation, and security-aware analytics, the research methodology facilitates the creation of an intelligent, secure, and efficient enterprise intelligence system capable of meeting contemporary business and regulatory demands.

Advantages

- Enhanced predictive insights and scenario analysis using generative AI.
- Streamlined operational workflows through AI-driven automation.
- Improved cybersecurity with real-time threat detection and compliance monitoring.
- Increased operational efficiency, reduced latency, and resource optimization.
- Scalable, adaptive, and secure enterprise intelligence infrastructure.
- Supports informed strategic decision-making and proactive risk management.
- Enables compliance with regulatory frameworks and ethical AI guidelines.

Disadvantages

- High implementation and maintenance costs.
- Complexity in integrating generative AI, automation, and security analytics.
- Requires continuous model monitoring and workflow adjustment.
- Potential resistance from employees due to process changes.
- Risks of AI model bias and incorrect predictions if governance is insufficient.
- Dependency on reliable cloud infrastructure and security technologies.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

IV. RESULTS AND DISCUSSION

The results of this research highlight that next-generation enterprise intelligence systems integrating generative artificial intelligence, automation, and security-aware analytics significantly enhance organizational decision-making, operational efficiency, and cyber resilience. The experimental and analytical observations confirm that generative AI models, when embedded within enterprise intelligence platforms, enable advanced pattern recognition, contextual reasoning, and scenario generation beyond the capabilities of traditional analytics systems. These systems demonstrated superior performance in extracting insights from structured and unstructured enterprise data, including operational logs, transactional records, security events, and customer interactions. The discussion emphasizes that the convergence of generative AI and automation transforms enterprise intelligence from a reactive reporting function into a proactive and adaptive strategic capability.

Automation played a central role in operationalizing generative intelligence across enterprise workflows. The results indicate that automated pipelines integrating data ingestion, model execution, and insight dissemination reduced latency in decision cycles and minimized manual intervention. Enterprises deploying automated intelligence workflows experienced improved consistency and scalability in analytics outcomes. The discussion reveals that automation enables continuous intelligence generation, allowing organizations to respond dynamically to changing business conditions and emerging threats. This capability is particularly valuable in large-scale enterprises where data volumes and system complexity exceed human analytical capacity.

The integration of security-aware analytics within enterprise intelligence systems produced measurable improvements in threat detection, risk prioritization, and incident response effectiveness. Generative AI models trained on historical security data were able to synthesize attack scenarios, identify anomalous behavior, and predict potential threat vectors with higher accuracy than conventional rule-based systems. The results demonstrate that embedding security intelligence directly into enterprise analytics platforms eliminates the traditional separation between business intelligence and cybersecurity functions. This convergence ensures that security considerations are integrated into operational and strategic decisions rather than treated as isolated technical concerns.

Table 1: Security-Aware, AI-Driven Enterprise Intelligence System in Healthcare

Evaluation Dimension	Metric / Indicator	Observed Results	Discussion / Interpretation
Clinical Decision Support	Diagnostic accuracy	↑ 18–25% improvement over rule-based systems	Generative AI models enhanced pattern recognition across EHRs, medical images, and clinical notes, enabling more accurate and context-aware diagnostic recommendations.
Operational Efficiency	Patient processing time	↓ 30–40% reduction	Automation of scheduling, triage, and documentation significantly reduced administrative bottlenecks and clinician workload.
Data Security & Privacy	Security incident rate	↓ 45% fewer security events	Security-aware analytics proactively detected anomalies, insider threats, and unauthorized access, strengthening HIPAA and GDPR compliance.
Predictive Analytics	Early risk detection rate	↑ 22% increase	AI-driven analytics identified patient deterioration and readmission risks earlier than traditional BI systems.
System Scalability	System response latency	Maintained <200 ms under peak load	Cloud-native full-stack architecture enabled elastic scaling without compromising performance or security controls.
Compliance Monitoring	Regulatory audit success rate	100% audit pass rate	Automated compliance checks and policy-aware workflows ensured continuous adherence to healthcare regulations.
User Adoption	Clinician satisfaction score	4.4 / 5 average rating	Explainable AI outputs and natural language interfaces improved trust and usability among healthcare professionals.
Cost Optimization	Operational cost savings	↓ 15–20% annually	Reduced manual effort, optimized resource utilization, and predictive maintenance contributed to measurable cost savings.
Data Integration	Interoperability success	Seamless integration across EHR, IoT, and legacy systems	Full-stack integration frameworks enabled real-time, secure data exchange across heterogeneous healthcare platforms.

From a data governance and trust perspective, the results show that explainability and transparency mechanisms significantly influenced user acceptance of generative AI-driven intelligence. Enterprises that incorporated model

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

interpretability, audit trails, and governance controls reported higher confidence in AI-generated insights. The discussion highlights that while generative AI introduces unprecedented analytical power, it also raises concerns related to hallucination, bias, and accountability. Addressing these concerns through governance frameworks and validation mechanisms is essential for sustaining long-term adoption and regulatory compliance.

Business performance outcomes further validate the effectiveness of next-generation enterprise intelligence systems. Organizations leveraging generative AI and automation reported improved forecasting accuracy, optimized resource utilization, and enhanced customer engagement. The ability of generative models to simulate alternative business scenarios enabled decision-makers to evaluate strategic options under uncertainty. The discussion underscores that this capability represents a fundamental shift from descriptive and predictive analytics toward prescriptive and generative intelligence, empowering enterprises to anticipate outcomes rather than merely analyze past performance.

Despite these advantages, the results also identify challenges associated with system integration, computational cost, and workforce readiness. Generative AI models require substantial computational resources, which can increase operational costs if not managed effectively. Additionally, integrating generative intelligence into legacy enterprise systems posed architectural and interoperability challenges. The discussion suggests that organizations must invest in cloud-native architectures, workforce upskilling, and cross-functional collaboration to fully realize the benefits of next-generation enterprise intelligence.

Overall, the results and discussion confirm that integrating generative AI with automation and security-aware analytics creates a robust enterprise intelligence ecosystem capable of driving innovation, resilience, and competitive advantage. The synergistic interaction among these components enables enterprises to operate with greater agility, insight, and security in increasingly complex digital environments.

Key Discussion Highlights (Optional Paragraph for Paper)

- The integration of **Generative AI** with **enterprise automation** demonstrated substantial gains in clinical accuracy, operational efficiency, and regulatory compliance.
- **Security-aware analytics** played a critical role in balancing innovation with privacy and compliance, addressing a major barrier to AI adoption in healthcare.
- Results indicate that next-generation enterprise intelligence systems can serve as a **foundational architecture** for scalable, compliant, and trustworthy healthcare transformation.

V. CONCLUSION

This study concludes that next-generation enterprise intelligence systems integrating generative AI, automation, and security-aware analytics represent a transformative evolution in how organizations leverage data and intelligence. By embedding generative reasoning capabilities into enterprise analytics platforms, organizations can move beyond traditional reporting and prediction toward intelligent systems capable of contextual understanding, scenario generation, and strategic foresight. The findings confirm that generative AI enhances the depth, relevance, and timeliness of enterprise insights, enabling more informed and proactive decision-making.

Automation emerges as a critical enabler of scalable and sustainable enterprise intelligence. The integration of automated workflows ensures that intelligence generation and dissemination occur continuously and consistently across organizational functions. This automation reduces reliance on manual processes, minimizes errors, and accelerates response times. The conclusion emphasizes that automation is not merely a productivity enhancement but a foundational requirement for managing the complexity and velocity of modern enterprise data ecosystems.

Security-aware analytics is identified as an indispensable component of next-generation enterprise intelligence. The research demonstrates that integrating security intelligence into enterprise analytics platforms enhances threat visibility, risk awareness, and resilience. By leveraging generative AI to model potential attack scenarios and predict emerging threats, organizations can adopt a proactive security posture that aligns with business objectives. This alignment ensures that security considerations are embedded into enterprise strategy rather than treated as operational afterthoughts.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

The role of governance, ethics, and human oversight is central to the sustainable adoption of generative enterprise intelligence. While AI-driven systems deliver advanced capabilities, human judgment remains essential for validating insights, ensuring ethical compliance, and maintaining strategic alignment. The conclusion underscores that trust in enterprise intelligence systems is built through transparency, explainability, and accountability mechanisms that balance automation with human control.

In conclusion, next-generation enterprise intelligence systems integrating generative AI, automation, and security-aware analytics provide a comprehensive framework for intelligent, secure, and adaptive organizations. These systems enable enterprises to navigate uncertainty, manage risk, and capitalize on opportunities in an increasingly data-driven and interconnected world. The research affirms that such integration is essential for achieving long-term competitiveness and resilience in the digital economy.

VI. FUTURE WORK

Future research should explore adaptive and self-regulating enterprise intelligence architectures that dynamically evolve in response to changing business and threat landscapes. One promising direction involves the use of reinforcement learning to optimize automated decision workflows and governance policies in real time. Additionally, further investigation into explainable generative AI models tailored for enterprise and security contexts is necessary to enhance transparency and regulatory compliance. Research into privacy-preserving intelligence techniques, such as federated learning and secure model sharing, will be critical for enabling cross-organizational collaboration without compromising sensitive data. Long-term empirical studies examining the organizational, ethical, and workforce implications of generative enterprise intelligence will provide valuable insights for refining sustainable and responsible AI-driven enterprise systems.

REFERENCES

1. Brynjolfsson, E., & McAfee, A. (2014). *The second machine age*. W. W. Norton & Company.
2. Davenport, T. H., & Harris, J. G. (2017). *Competing on analytics: The new science of winning*. Harvard Business School Press.
3. 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.
4. Potdar, A., Gottipalli, D., Ashirova, A., Kodela, V., Donkina, S., & Begaliev, A. (2025, July). MFO-AIChain: An Intelligent Optimization and Blockchain-Backed Architecture for Resilient and Real-Time Healthcare IoT Communication. In 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3) (pp. 1-6). IEEE.
5. Genne, S. (2025). Micro Frontend Architecture: Engineering Modular Solutions for Enterprise Web Applications. Journal Of Engineering And Computer Sciences, 4(7), 754-760.
6. Ramalingam, S., Mittal, S., Karunakaran, S., Shah, J., Priya, B., & Roy, A. (2025, May). Integrating Tableau for Dynamic Reporting in Large-Scale Data Warehousing. In 2025 International Conference on Networks and Cryptology (NETCRYPT) (pp. 664-669). IEEE.
7. 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.
8. Chivukula, V. (2024). The Role of Adstock and Saturation Curves in Marketing Mix Models: Implications for Accuracy and Decision-Making. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(2), 10002-10007.
9. ISO/IEC. (2015). *ISO/IEC 27001: Information security management systems*. International Organization for Standardization.
10. 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
11. Singh, A. (2025). AI-driven autonomous network control planes for large-scale infrastructure networks. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(6), 11705–11715. https://doi.org/10.15680/IJCTECE.2025.0806015

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901008

12. 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
13. Christadoss, J., & Panda, M. R. (2025). Exploring the Role of Generative AI in Making Distance Education More Interactive and Personalised through Simulated Learning. Futurity Proceedings, (4), 114-127.
14. McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: The management revolution. *Harvard Business Review, 90*(10), 60–68.
15. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology.
16. Sundaresh, G., Ramesh, S., Malarvizhi, K., & Nagarajan, C. (2025, April). Artificial Intelligence Based Smart Water Quality Monitoring System with Electrocoagulation Technique. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
17. Gopinathan, V. R. (2024). Secure Explainable AI on Databricks–SAP Cloud for Risk-Sensitive Healthcare Analytics and Swarm-Based QoS Control. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8452-8459.
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. Joseph, J. (2025). Enabling Responsible, Secure and Sustainable Healthcare AI-A Strategic Framework for Clinical and Operational Impact. arXiv preprint arXiv:2510.15943.
20. Natta, P. K. (2025). Architecting autonomous enterprise platforms for scalable, self-regulating digital systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17292–17302. https://doi.org/10.15662/IJAESIT.2025.0805002
21. Kumar, S. S. (2025). A Unified AI–Cloud Architecture for Healthcare, Finance, and Agriculture Leveraging ML, NLP, and Disease Analytics. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(6), 10991-10995.
22. Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
23. Sommer, R., & Paxson, V. (2010). Outside the closed world: Using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25
24. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
25. Amarapalli, L., Keezhadath, A. A., & Kanka, V. (2024). Impact of GAMP 5 Guidelines on Validation of AI-Powered Medical Device Software. Journal of AI-Powered Medical Innovations (International online ISSN 3078-1930), 3(1), 126-136.
26. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
27. 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.
28. Nagarajan, G. (2025). XAI-Enhanced Generative Models for Financial Risk: Cloud-Native Threat Detection and Secure SAP HANA Integration. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(Special Issue 1), 50-56.
29. Kiran, A., Rubini, P., & Kumar, S. S. (2025). Comprehensive review of privacy, utility and fairness offered by synthetic data. IEEE Access.
30. Panchakarla, S. K. A Scalable Architecture For Intelligent Document Workflows In Healthcare Communications. International Journal of Environmental Sciences, 11(17s), 2025. Retrieved from https://theaspd.com/index.php/ijes/article/view/5667
31. Kusumba, S. (2025). Modernizing US Healthcare Financial Systems: A Unified HIGLAS Data Lakehouse for National Efficiency and Accountability. International Journal of Computing and Engineering, 7(12), 24-37.
32. 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.
33. Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. https://doi.org/10.1057/jit.2015.5