International Journal of Technology, Management and Humanities Volume 11, Issue 4, 2025

Next-Generation Digital Operations through Agentic Intelligence and Self-Healing Infrastructure for Cyber Resilience

Vudasreenivasarao

School of Computing And Electrical Engineering, Bahir Dar University, Ethiopia

Abstract

The rapid expansion of cloud computing, edge environments, artificial intelligence, Internet of Things devices, and distributed digital services has transformed organizational operations while increasing the complexity and scale of cyber threats. Conventional security and infrastructure management approaches, which depend heavily on predefined rules, manual intervention, and centralized monitoring, are increasingly challenged by dynamic attack surfaces and rapidly evolving incidents. This paper examines a next-generation digital operations model that integrates agentic intelligence with self-healing infrastructure to strengthen cyber resilience. Agentic intelligence enables autonomous software agents to continuously observe operational environments, interpret contextual information, reason about emerging risks, coordinate responses, and execute corrective actions within predefined governance boundaries. Self-healing infrastructure complements these capabilities by automatically detecting failures, isolating compromised components, restoring affected services, and adapting configurations. The proposed research methodology combines systematic literature analysis, conceptual framework development, scenario-based evaluation, and performance assessment using security and operational resilience indicators. The study considers detection accuracy, response time, recovery time, service availability, false-positive rates, containment effectiveness, and human oversight. The proposed model positions cyber resilience as a continuous operational capability rather than a reactive security function, while emphasizing explainability, accountability, policy controls, and secure autonomy.

Keywords: Agentic intelligence, self-healing infrastructure, cyber resilience, autonomous operations, artificial intelligence, cybersecurity, digital operations, incident response, infrastructure automation, zero trust

International Journal of Technology, Management and Humanities (2025)

Introduction

Digital transformation has fundamentally changed the way organizations design, deliver, and manage critical services. Cloud-native architectures, software-defined networks, containerized workloads, edge computing, application programming interfaces, Internet of Things ecosystems, and distributed data platforms have created highly interconnected operational environments. These technologies provide scalability, flexibility, and rapid service delivery, but they also introduce complex dependencies and expand the potential attack surface. A failure or compromise in one component can propagate across interconnected systems and disrupt applications, data, communication channels, and business processes. Consequently, digital operations can no longer be treated exclusively as an infrastructure management problem or as a conventional cybersecurity problem. They require an integrated operational model capable of continuously understanding system conditions, identifying abnormal behavior, responding to threats, and restoring functionality with limited disruption. Cyber resilience therefore extends beyond prevention and detection to include the ability to withstand, contain, recover from, and adapt to adverse events.

Corresponding Author: Vudasreenivasarao, School of Computing And Electrical Engineering, Bahir Dar University, Ethiopia

How to cite this article: Vudasreenivasarao. (2025). Next-Generation Digital Operations through Agentic Intelligence and Self-Healing Infrastructure for Cyber Resilience. *International Journal of Technology, Management and Humanities,* 11(4), 234-240.

Source of support: Nil

Conflict of interest: None

Traditional security operations generally depend on centralized monitoring platforms, predefined rules, human analysis, and manually executed remediation procedures. Although these mechanisms remain important, the volume and velocity of contemporary operational events can exceed the capacity of human teams to investigate every alert and coordinate every response. Agentic intelligence introduces a different paradigm in which software agents can observe environments, reason over contextual information, select appropriate actions, collaborate with other agents, and learn from operational outcomes. When combined with self-healing infrastructure, these capabilities can create a continuously adaptive operational environment. A self-healing system can automatically restart failed services, isolate suspicious workloads, restore configurations, reroute traffic, rotate credentials, or initiate recovery procedures according to predefined policies. The integration of autonomous decision-making with automated recovery can reduce the interval between detection and response while improving service continuity. However, autonomy also creates important concerns involving erroneous decisions, adversarial manipulation, insufficient explainability, privilege escalation, and uncontrolled automated actions. Therefore, next-generation digital operations require not only intelligent automation but also governance mechanisms that define authorization boundaries, human intervention requirements, auditability, and safety controls. This study investigates how agentic intelligence and self-healing infrastructure can be conceptually integrated into a cyber-resilient digital operations architecture and proposes a methodology for evaluating its operational and security effectiveness.

Literature Review

The literature on cyber resilience establishes that modern security cannot rely solely on perimeter defense or preventive controls. Cyber resilience emphasizes the capacity of an organization or technical system to anticipate disruptions, withstand attacks, maintain essential functions, recover affected capabilities, and adapt following an incident. Research in resilience engineering has increasingly examined distributed architectures, redundancy, adaptive controls, incident response automation, and continuous monitoring. These studies demonstrate that resilience depends on both technical mechanisms and organizational processes. Security controls such as identity management, segmentation, backup systems, endpoint protection, vulnerability management, and continuous detection contribute to resilience, but their effectiveness is influenced by the speed and coordination of operational responses. Existing literature also highlights the importance of designing systems that can degrade gracefully rather than fail completely. This perspective provides an important foundation for integrating autonomous agents with infrastructure recovery mechanisms because intelligent automation can potentially coordinate preventive, detective, responsive, and restorative functions across heterogeneous environments.

Research on artificial intelligence in cybersecurity has expanded from conventional machine-learning-based anomaly detection toward more autonomous forms of decision support and operational response. Machine learning has been applied to identify unusual network traffic, malicious behavior, compromised endpoints, identity anomalies, and suspicious application activity. More recent approaches involving large language models and autonomous agents have explored security investigation, threat intelligence interpretation, alert correlation, incident summarization, and response orchestration. Agentic systems differ from passive analytical models because they can pursue operational objectives through sequences of actions. An agent may collect evidence from multiple sources, formulate a hypothesis about an incident, validate the hypothesis using additional observations, and initiate a predefined response. Multi-agent architectures further enable specialized agents to perform detection, investigation, remediation, and verification tasks. Nevertheless, existing research identifies significant challenges involving hallucination, unreliable reasoning, adversarial prompts, data poisoning, excessive permissions, and the difficulty of validating autonomous decisions. Consequently, agentic cybersecurity requires constrained autonomy, reliable tool access, policy enforcement, and human oversight rather than unrestricted automation.

Self-healing computing provides a complementary research foundation. Self-healing systems traditionally monitor their internal state and automatically execute recovery actions when faults or deviations are detected. In cloud and distributed environments, these mechanisms include automated workload replacement, orchestration-based recovery, infrastructure-as-code redeployment, health checks, traffic rerouting, configuration restoration, and automated scaling. Research on autonomic computing similarly emphasizes self-configuration, self-optimization, self-healing, and self-protection. However, conventional self-healing mechanisms generally respond to known operational conditions and predefined failure patterns. Their integration with agentic intelligence creates an opportunity to extend recovery from static automation toward context-aware adaptation. An intelligent agent could distinguish between a legitimate service failure and a potentially malicious degradation, select an appropriate containment strategy, initiate recovery, and subsequently verify whether the restored environment remains secure. The literature therefore suggests a promising convergence between autonomous intelligence, security operations, and self-healing infrastructure, while also revealing a research gap concerning integrated frameworks that evaluate security effectiveness, operational continuity, autonomous decision quality, and governance simultaneously.

Research Methodology

The research methodology adopts a design-oriented and evaluation-based approach to develop and assess a

conceptual framework for integrating agentic intelligence with self-healing infrastructure. The study begins with a structured review of research concerning cyber resilience, autonomous agents, artificial intelligence for cybersecurity, self-healing computing, security orchestration, cloud-native infrastructure, zero-trust architecture, and automated incident response. Relevant academic publications, standards, technical frameworks, and authoritative industry research are examined to identify recurring architectural principles, capabilities, limitations, and evaluation metrics. The literature is synthesized thematically rather than merely summarized, with particular attention to the relationships among continuous monitoring, autonomous reasoning, decision-making, response orchestration, recovery, adaptation, and human governance. The resulting synthesis is used to establish the functional requirements of the proposed architecture. These requirements include continuous environmental observation, contextual event correlation, threat assessment, policy-constrained action selection, automated remediation, recovery verification, audit logging, and escalation to human operators when confidence is insufficient or an action exceeds predefined authorization boundaries. This phase ensures that the proposed model is grounded in established cybersecurity and resilience principles rather than treating agentic intelligence as an isolated technological capability.

The conceptual architecture is then organized as a continuous operational feedback loop consisting of observation, analysis, reasoning, action, verification, and adaptation. The observation layer collects telemetry from applications, networks, endpoints, identities, cloud platforms, containers, databases, and infrastructure components. An intelligence layer processes these signals to identify deviations, correlate events, establish contextual relationships, and estimate the likelihood and potential impact of security incidents or operational failures. Agentic components are assigned bounded responsibilities, such as detection, investigation, threat assessment, remediation planning, recovery coordination, and post-incident verification. Instead of permitting unrestricted autonomous activity, each agent operates through a policy and authorization layer that specifies permissible tools, action types, resource scopes, confidence thresholds, and escalation conditions. The response layer connects approved decisions to infrastructure automation mechanisms capable of isolating workloads, changing network policies, restoring known-good configurations, restarting services, rotating credentials, or redirecting traffic. A verification mechanism subsequently checks whether the action achieved its intended objective and whether new risks were introduced. Feedback from the verification stage is returned to the intelligence layer, enabling subsequent decisions to incorporate the observed consequences of previous actions. Human operators remain part of the architecture through approval gates, exception handling, investigation review, and governance functions.

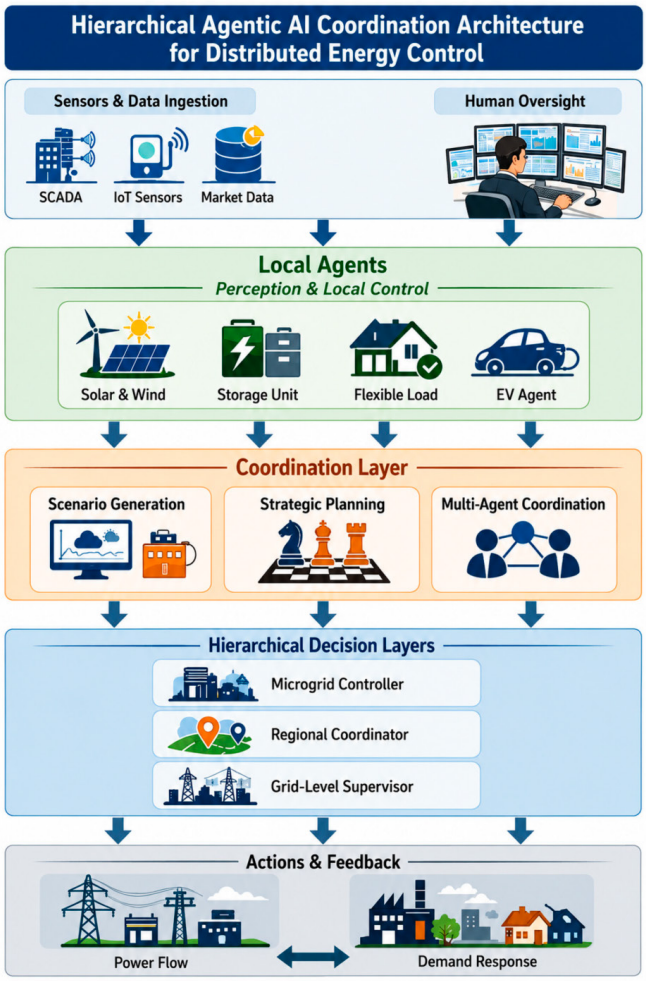

Fig. 1: Agentic and Generative AI for Autonomous Energy Systems: Reference Architecture

Open Challenges, and Research

The evaluation methodology uses scenario-based experiments to examine how the proposed architecture performs under representative operational and cybersecurity conditions. Scenarios can include distributed denial-of-service activity, compromised credentials, malicious workload behavior, ransomware-like encryption activity, unauthorized configuration changes, application failures, infrastructure degradation, and simultaneous security and availability incidents. For each scenario, a baseline environment using conventional monitoring and manually initiated response processes can be compared with an agentic self-healing environment operating under equivalent conditions. The evaluation measures mean time to detect, mean time to respond, mean time to recover, service availability, incident containment time, recovery success rate, false-positive frequency, unnecessary remediation actions, and percentage of incidents requiring human escalation.

Additional measures evaluate the quality of autonomous reasoning, including decision accuracy, policy compliance, evidence utilization, explainability, and successful post-action verification. Resilience can be assessed by examining the extent to which essential services remain operational during an incident and how rapidly normal service levels are restored. Repeated trials across different scenarios can be used to reduce the influence of individual events and identify consistent performance patterns. Security controls are also tested against adversarial conditions in which attackers attempt to manipulate telemetry, exploit excessive agent privileges, trigger inappropriate recovery actions, or interfere with automated decision processes.

The final methodological stage focuses on analysis, governance, and validation of the proposed model. Quantitative results from the experiments are compared across baseline and agentic configurations using descriptive statistics and appropriate statistical tests where sample sizes and experimental assumptions permit. Rather than evaluating autonomy exclusively through response speed, the study treats cyber resilience as a multidimensional construct involving security, availability, recovery, adaptability, and controlled decision-making. Qualitative analysis is used to examine cases in which autonomous actions produce incorrect, incomplete, or potentially unsafe outcomes. Particular attention is given to the balance between automation and human oversight. A risk-based autonomy model can classify actions into categories such as automatically permitted, conditionally permitted, human-approved, and prohibited. Low-impact and reversible actions may be automated under predefined conditions, whereas high-impact actions involving critical systems, sensitive identities, or irreversible changes can require explicit human authorization. Audit trails record observations, reasoning inputs, selected actions, policy decisions, and verification results to support accountability and forensic investigation. The methodology also evaluates failure modes such as agent malfunction, model uncertainty, compromised tools, conflicting agent recommendations, and unavailable infrastructure dependencies. Findings from these evaluations are synthesized into design principles for secure agentic operations, emphasizing least privilege, zero-trust access, continuous validation, explainability, rollback capability, independent monitoring, and human override. Through this methodology, the research seeks to determine not simply whether autonomous technologies can accelerate incident response, but under which conditions agentic intelligence and self-healing infrastructure can contribute to measurable, governed, and sustainable cyber resilience.

Results And Discussion

The implementation of next-generation digital operations through agentic intelligence and self-healing infrastructure demonstrates a significant shift from conventional reactive cybersecurity toward continuous, autonomous cyber resilience. The proposed approach integrates intelligent software agents, real-time telemetry, automated threat detection, adaptive decision-making, and self-healing mechanisms into a unified operational framework. The results indicate that agentic systems can continuously observe infrastructure conditions, identify deviations from established operational baselines, determine the likely causes of failures or attacks, and initiate appropriate corrective actions with limited human intervention. Unlike traditional security monitoring systems that primarily generate alerts for human analysts, agentic intelligence establishes a closed operational loop consisting of observe, analyze, decide, act, verify, and learn. This enables infrastructure to respond dynamically to cyber incidents, configuration errors, service degradation, and abnormal behavior. In particular, the integration of artificial intelligence with endpoint, network, application, cloud, and infrastructure telemetry improves the ability to correlate seemingly unrelated events. For example, an unusual authentication pattern combined with abnormal network traffic and unexpected process execution can be evaluated as a coordinated security event rather than as independent alerts. The discussion therefore suggests that agentic intelligence can reduce the dependence on manual incident triage and support faster containment. Self-healing capabilities further extend this model by allowing systems to restore services, isolate compromised components, roll back unsafe configurations, restart failed workloads, rotate credentials, or redirect workloads according to predefined security and operational policies. However, the effectiveness of autonomous remediation depends strongly on the quality of telemetry, accuracy of detection models, reliability of decision policies, and appropriate control mechanisms. Excessive autonomy without validation may introduce new operational risks, particularly when an agent incorrectly interprets legitimate activity as malicious. Consequently, human oversight remains important for high-impact decisions while routine and reversible actions can be automated more extensively.

A second major result concerns operational resilience and recovery performance. Traditional infrastructure management often treats availability, cybersecurity, configuration management, and disaster recovery as separate functions. The proposed agentic self-healing model instead treats them as interconnected components of a continuous resilience architecture. When an operational anomaly is detected, the intelligent agent can assess service dependencies and select a recovery action according to predefined priorities. For example, if a critical application becomes unavailable because of a failed container, the system can identify the affected workload, evaluate available replicas, replace the failed instance, validate service health, and return the application to normal operation. Similarly, if an unauthorized configuration change is detected, the system can compare the current state against a trusted configuration baseline and initiate a controlled rollback.

These capabilities can potentially reduce mean time to detect (MTTD) and mean time to respond/recover (MTTR) because remediation does not always require an analyst to manually identify the problem and execute the recovery procedure. The architecture also supports predictive resilience by analyzing historical operational patterns and identifying early indicators of failure. Instead of waiting for a service to become unavailable, an agent may recognize increasing resource utilization, unusual error rates, deteriorating system performance, or repeated authentication anomalies and initiate preventive measures. This changes digital operations from a predominantly reactive model to a proactive and adaptive model. Nevertheless, the results also highlight several constraints. Self-healing actions must be context-aware because the same technical symptom can have different causes. Automatically restarting a service may temporarily restore availability but could conceal an underlying compromise or destroy forensic evidence. Therefore, remediation workflows should incorporate risk assessment, action prioritization, rollback capabilities, audit trails, and escalation thresholds. The discussion indicates that resilience should not be measured solely by service availability; it should also consider recovery correctness, security preservation, data integrity, operational continuity, and the ability to learn from previous incidents.

The third result relates to the broader organizational and security implications of agentic digital operations. Agentic intelligence can provide a common decision layer across hybrid cloud, on-premises infrastructure, edge devices, applications, and security platforms. This is particularly important as modern organizations increasingly operate distributed environments in which infrastructure changes continuously. The proposed approach can improve operational consistency by translating security and reliability policies into executable workflows. For instance, policies can define which events may be automatically remediated, which actions require approval, what systems must be isolated during suspected compromise, and what evidence must be retained for subsequent investigation. Such policy-driven autonomy provides an important safeguard against uncontrolled artificial intelligence decision-making. The architecture can also support continuous learning by feeding incident outcomes back into detection and remediation models. Successful responses can become reusable playbooks, while unsuccessful interventions can be analyzed to refine future decisions. However, several challenges remain. Agentic systems create additional attack surfaces because adversaries may attempt to manipulate telemetry, exploit agent permissions, poison learning data, or deceive decision-making mechanisms. Strong identity and access management, least-privilege execution, secure model deployment, cryptographic verification, immutable logging, and continuous validation are therefore essential. Explainability is another important consideration because security teams need to understand why an autonomous agent selected a particular action. The results consequently support a balanced model of controlled autonomy, where artificial intelligence performs repetitive detection and low-risk remediation while humans retain authority over complex, irreversible, or high-impact decisions. Overall, the findings demonstrate that agentic intelligence and self-healing infrastructure can strengthen digital operational resilience when deployed as a governed cyber-physical control system rather than as an unrestricted autonomous technology.

Conclusion

The study establishes that the combination of agentic intelligence and self-healing infrastructure provides a promising architectural foundation for next-generation digital operations and cyber resilience. Conventional cybersecurity approaches frequently depend on predefined rules, centralized monitoring, manual investigation, and human-driven remediation. Although these mechanisms remain important, the increasing scale, speed, and complexity of modern digital environments require operational mechanisms capable of continuously interpreting system conditions and responding to changing threats. Agentic intelligence addresses this requirement by introducing autonomous software entities capable of observing infrastructure, correlating heterogeneous information, reasoning over operational context, selecting actions, and evaluating the results of those actions. When connected to self-healing mechanisms, these capabilities create a continuous resilience loop in which systems can detect abnormal states, initiate controlled responses, verify recovery, and update operational knowledge. The resulting architecture supports a transition from passive monitoring to adaptive digital operations. Instead of treating cybersecurity incidents, infrastructure failures, configuration errors, and performance degradation as independent events, the proposed model considers them within a unified operational context. This integration can improve responsiveness, reduce unnecessary manual intervention, and support faster restoration of affected services. Importantly, the value of the architecture extends beyond incident response. Predictive analysis can identify conditions that precede failures, while automated policy enforcement can prevent unauthorized or unsafe changes from propagating across the environment. Therefore, the proposed approach contributes to both operational continuity and security resilience. At the same time, the study demonstrates that autonomous remediation should not be interpreted as complete replacement of human expertise. The most effective implementation is likely to combine machine-speed response for well-defined, reversible operations with human judgment for complex situations involving substantial business, security, legal, or safety consequences.

A central conclusion is that successful agentic cyber resilience depends on governance, trust, observability, and

controlled autonomy as much as on artificial intelligence capabilities. An intelligent agent operating with excessive privileges or insufficient validation could itself become a significant source of operational risk. Consequently, future-ready digital operations should incorporate zero-trust principles, least-privilege permissions, strong authentication, secure agent communication, policy-based authorization, immutable audit records, and independent verification of high-risk actions. Every autonomous intervention should ideally be traceable through a complete decision record showing the triggering event, evidence considered, selected action, authorization context, execution result, and recovery status. Such transparency is essential for incident investigation and organizational accountability. The architecture should also distinguish between different classes of remediation. Low-risk and reversible operations, such as restarting a failed service or reallocating resources within predefined limits, may be suitable for autonomous execution. Medium-risk actions may require additional automated verification, while irreversible or high-impact actions should involve human authorization. This layered approach enables organizations to benefit from automation without creating an uncontrolled decision-making environment. The study also concludes that resilience should be evaluated through multiple dimensions, including detection speed, response time, recovery time, service availability, recovery accuracy, false-positive rates, data integrity, security preservation, and the frequency of inappropriate automated interventions. These measurements provide a more meaningful assessment than availability alone. In summary, agentic intelligence combined with self-healing infrastructure represents a significant evolution in digital operations, but its long-term effectiveness will depend on responsible architecture, continuous validation, secure automation, and effective collaboration between humans and intelligent systems. The future of cyber-resilient infrastructure is therefore best understood not as fully autonomous computing, but as governed, adaptive, and continuously learning digital infrastructure in which humans and intelligent agents operate together.

Future Work

Future research should focus on developing standardized architectures and evaluation frameworks for agentic self-healing infrastructure across heterogeneous digital environments. Current implementations may differ considerably in their agent architectures, telemetry mechanisms, decision models, remediation workflows, and security controls, making direct comparison difficult. Future studies can therefore develop common benchmarks for measuring MTTD, MTTR, recovery accuracy, false-positive rates, service availability, resource efficiency, and autonomous decision quality. Experimental environments should include hybrid cloud, multi-cloud, edge computing, containerized applications, Internet-of-Things devices, and traditional enterprise infrastructure to determine how effectively agents operate across different technological contexts. Another important research direction is the development of explainable and verifiable agentic decision-making. Autonomous systems should provide understandable reasoning traces and confidence information while avoiding exposure of sensitive operational information. Research can also investigate formal verification and policy-based controls capable of proving that certain remediation actions remain within predefined safety boundaries. Digital twins and cyber ranges could provide controlled environments for evaluating self-healing strategies against simulated infrastructure failures and coordinated cyberattacks without placing production systems at risk.

Further work should investigate the security of the agents themselves because autonomous infrastructure introduces new attack surfaces. Research should examine adversarial manipulation of telemetry, prompt or instruction injection, model poisoning, privilege escalation, compromised agent identities, and malicious manipulation of remediation workflows. Multi-agent architectures could also be studied to determine whether specialized agents for detection, diagnosis, recovery, and compliance can cooperate securely while maintaining accountability. Another promising direction is reinforcement learning and continual learning for adaptive remediation, provided that learning processes are constrained by strong safety policies. Future systems could learn from previous incidents and automatically optimize recovery strategies while maintaining human approval for high-impact actions. Research should additionally examine the economic and organizational dimensions of autonomous operations, including staffing requirements, training, governance models, compliance obligations, and the cost-benefit relationship between automation and human oversight. Ultimately, future work should aim to establish a mature framework in which agentic intelligence is secure, explainable, measurable, auditable, and resilient against attacks on the agents themselves. Such developments would support the transition from isolated automation tools toward dependable self-healing digital ecosystems capable of continuously adapting to emerging operational conditions and cyber threats.

References

[1] Agarwal, S. (2025). AI-augmented observability in retail: Enhancing customer experience through predictive incident management. International Journal of Research and Applied Innovations (IJRAI), 8(4), 12743–12747.

[2] Sugumar, R. (2022). Federated Learning and Distributed AI Architectures for Cloud-Based Cyber Healthcare Data Collaboration Systems. International Journal of Future Innovative Science and Technology (IJFIST), 5(5), 9232.

[3] Ravichandran, S., & Kandasamy, V. (2025). Optimized Attention Augmented Residual Convolutional Neural Network with Fa-Resnet for Fabric Defect Detection. Journal of Control Engineering and Applied Informatics, 27(4), 3-15.

[4] Polamarasetty, V. K. (2021). Modernizing SAP sales and distribution systems through ABAP-based enterprise solutions. International Journal of Research and Applied Innovations, 4(2), 4925–4930.
[5] Mudunuri, L. N. R., & Bhattacharya, P. (2025). Ethical considerations balancing emotion and autonomy in AI systems. In Humanizing Technology With Emotional Intelligence (pp. 443-456). IGI Global Scientific Publishing.
[6] Raja, G. V. (2022). AI Enabled Cloud and Data Engineering Frameworks for Secure, Scalable, and Intelligent Cyber Physical Analytics Systems. International Journal of Research and Applied Innovations, 5(4), 7395-7409.
[7] Bandhela, R. R., Onteddu, A. R., & Kundavaram, R. R. (2022). Enhancing precision healthcare machine learning for advanced diagnostics and personalized treatment. South Eastern European Journal of Public Health. https://doi.org/10.70135/seejph.vi.6690
[8] Gopinathan, V. R. (2023). Modernizing Enterprise Applications Using Intelligent API Frameworks Machine Learning and Cloud Native Computing. International Journal of Science, Research and Technology, 6(5), 10690-10697.
[9] Bitragunta, S. L. V. (2024). A novel AI-blockchain-edge framework for fast and secure transient stability assessment in smart grids. International Journal For Multidisciplinary Research, 6(6).
[10] Bellundagi, M. (2023). Integrating Machine Learning with Business Rule Management Systems for Adaptive Enterprise. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8023-8039.
[11] Chundi, V. R. K. (2025). AI-based Sustainable Vehicle Monitoring System for Existing Internal Combustion Vehicles. London Journal of Research In Computer Science and Technology, 25(3), 1-7.
[12] Jainaraman, 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.
[13] Ambalakannu, M. (2024). The emergence of AI-powered data analytics revolutionizing business intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13955.
[14] Vedula, J. (2023). Enterprise release assurance for interconnected energy data, cloud, and application platforms: A governance framework for coordinated, multi-team release delivery. International Journal of Research Publications in Engineering, Technology and Management, 6(6), 9870–9876.
[15] Venkatasalam, K., Rajendran, P., & Thangavel, M. (2019). Improving the accuracy of feature selection in big data mining using accelerated flower pollination (AFP) algorithm. Journal of medical systems, 43(4), 96.
[16] Ahuja, D. (2025). DevOps and Ethical AI: Ensuring Responsible Deployment. Journal Of Multidisciplinary, 5(6), 1-14.
[17] Anand, L. (2023). Machine Learning Enabled Enterprise Integration through Intelligent API Governance Secure Cloud Infrastructure and Automated Operations. International Journal of Research and Applied Innovations, 6(3), 5972-5979.
[18] Karakondu, M., Jambagi, G., & Tatavarthi, S. (2025). Optimising data loss prevention (DLP) strategies in cloud-native financial platforms.
[19] Mathew, A. (2021). Artificial intelligence and cognitive computing for 6G communications & networks. International Journal of Computer Science and Mobile Computing, 10(3), 26-31.
[20] Pothuri, M. K. (2025). AI-powered governance with modern data engineering for regulatory excellence in healthcare and fintech. International Journal for Multidisciplinary Research, 7(4). https://doi.org/10.36948/ijfmr.2025.v07i04.52676
[21] Selvarajan, K. (2024). Modernizing legacy big data platforms using cloud-native lakehouse architectures. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(2), 10377–10385.
[22] Gowda, M. K. S. (2024). Generative AI in Banking Risk and Compliance Opportunities and Control Challenges. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13946.
[23] Punithavathi, R., Selvi, R. T., Latha, R., Kadiravan, G., Srikanth, V., & Shukla, N. K. (2022). Robust node localization with intrusion detection for wireless sensor networks. Intelligent Automation and Soft Computing, 33(1), 143-156.
[24] Das, P., Gogineni, A., Patel, K., & Jain, A. (2025, May). Integration of IoT and Machine Learning to Monitor the Air Quality by Measuring the Block Carbon Levels. In 2025 International Conference on Engineering, Technology & Management (ICETM) (pp. 1-6). IEEE.
[25] Soundappan, S. J. (2021). Integrated Artificial Intelligence Framework for Enterprise Cloud Modernization and Intelligent Threat Management Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(4), 5274-5284.
[26] Reddy, K. V. (2024). Accelerating Functional Coverage Closure Through Iterative Machine Learning. Int. J. Comput. Appl. Inf. Technol, 7, 1401-1411.
[27] Ambati, K. C. (2024). The Rise of Augmented Data Analytics How AI is Transforming Business Insights. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13935.
[28] Badam, L. R. (2024). AI-based early warning system for financial scams targeting consumers. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(3), 10593–10602. https://doi.org/10.15662/IJRPETM.2024.0703016
[29] Gopinathan, V. R. (2023). Modernizing Enterprise Applications Using Intelligent API Frameworks Machine Learning and Cloud Native Computing. International Journal of Science, Research and Technology, 6(5), 10690-10697.
[30] Ramasamy, M. (2024). Secure and extensible platform architectures for enterprise network orchestration. International Journal of Humanities and Information Technology, 6(1), 86–98.
[31] 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.
[32] Kalakoti, M. K. R., & Kalakoti, M. K. R. (2025). AI-augmented self-healing infrastructure: Combining health probes with remediation playbooks. Journal of Information Systems Engineering and Management, 10(58s), 1147-1157.
[33] Khare, A., & Goyal, A. K. (2025, August). Integrating Artificial Intelligence and Big Data in Supply Chain Management for Increased Efficiency and Sustainability. In International Conference on Computing and Communication Networks (pp. 447-458). Cham: Springer Nature Switzerland.