International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805028

Intelligent Multi Agent Artificial Intelligence Architecture for Secure Cloud Native Digital Transformation and Infrastructure Automation

José Merseguer

Senior Project Manager, Italy

ABSTRACT: Digital transformation across enterprises has accelerated the adoption of cloud native architectures artificial intelligence driven automation and secure infrastructure platforms. However managing complex distributed environments requires intelligent autonomous systems capable of monitoring optimizing and protecting digital ecosystems. This paper proposes an Intelligent Multi Agent Artificial Intelligence Architecture designed to support secure cloud native digital transformation and automated infrastructure management. The architecture integrates AI agents machine learning analytics cybersecurity intelligence and cloud orchestration frameworks to enable autonomous decision making predictive operations and resilient enterprise systems. The proposed framework utilizes distributed intelligent agents responsible for workload orchestration resource optimization threat detection compliance governance and operational automation. Each agent collaborates through a coordinated decision layer supported by data driven analytics and real time monitoring. The system is designed to integrate with container orchestration platforms microservices infrastructure and enterprise cloud platforms such as AWS Azure and hybrid cloud environments. The research highlights how multi agent AI architectures enhance scalability operational efficiency cybersecurity resilience and intelligent infrastructure management in modern enterprises. Experimental evaluation and conceptual modeling demonstrate that the proposed architecture significantly improves infrastructure reliability reduces operational overhead and strengthens cyber defense mechanisms. The findings contribute to the development of autonomous enterprise platforms capable of supporting next generation digital transformation initiatives across finance healthcare manufacturing and government sectors.

KEYWORDS: Multi Agent Artificial Intelligence, Cloud Native Architecture, Digital Transformation, Infrastructure Automation, Autonomous Enterprise Systems, Cybersecurity Intelligence, DevOps Automation, Intelligent Cloud Platforms.

I. INTRODUCTION

The rapid evolution of digital technologies has significantly transformed enterprise infrastructure and business operations. Organizations are increasingly adopting cloud native platforms microservices architectures and artificial intelligence driven automation to improve scalability efficiency and agility. Digital transformation initiatives are now central to enterprise competitiveness as industries seek to modernize legacy infrastructure and integrate advanced computing technologies into their operational frameworks. However managing large scale distributed systems introduces challenges related to infrastructure complexity security risks operational inefficiencies and resource optimization.

Cloud native environments often consist of distributed containers microservices orchestration platforms data pipelines and dynamic resource provisioning systems. While these technologies provide flexibility and scalability they also require sophisticated management strategies capable of handling continuous workload changes system vulnerabilities and performance monitoring requirements. Traditional manual infrastructure management approaches are no longer sufficient to maintain reliability security and operational efficiency in highly dynamic cloud ecosystems.

Artificial intelligence has emerged as a critical technology for enabling intelligent automation within enterprise platforms. Machine learning algorithms predictive analytics and intelligent monitoring systems allow organizations to analyze infrastructure behavior detect anomalies and optimize system performance. Despite these advancements many enterprise infrastructures still rely on centralized control mechanisms that lack autonomous decision making capabilities.

Multi agent artificial intelligence systems provide a promising approach for addressing these limitations. In a multi agent system multiple intelligent agents operate independently while collaborating to achieve shared objectives. Each agent performs specialized tasks such as monitoring security events optimizing workloads managing network resources or coordinating infrastructure updates. The distributed nature of multi agent systems enables scalable decision making resilience and adaptive behavior in complex digital environments.

This research proposes an Intelligent Multi Agent Artificial Intelligence Architecture designed to support secure cloud native digital transformation and automated infrastructure management. The architecture introduces specialized agents responsible for monitoring infrastructure performance analyzing security threats orchestrating cloud resources and maintaining compliance across enterprise systems. By integrating these agents with cloud orchestration frameworks and security intelligence systems the proposed model enables autonomous infrastructure operations.

The main objectives of this study are to design a scalable multi agent AI framework analyze its operational components and evaluate its potential impact on enterprise cloud ecosystems. The proposed architecture aims to enhance infrastructure automation improve cybersecurity resilience and support intelligent digital transformation initiatives across diverse enterprise sectors.

II. LITERATURE REVIEW

Recent research in artificial intelligence cloud computing and enterprise automation has highlighted the growing importance of intelligent systems capable of managing complex digital infrastructures. The integration of machine learning algorithms cloud native architectures and distributed computing platforms has enabled organizations to develop advanced operational models that improve efficiency and scalability.

Several studies have explored the role of artificial intelligence in cloud infrastructure management. AI driven monitoring platforms use predictive analytics to identify performance bottlenecks detect system anomalies and optimize resource allocation across distributed computing environments. These solutions rely on large scale data analytics to generate insights that support automated decision making and proactive infrastructure management.

Cloud native architectures have also been widely adopted as a foundation for modern digital transformation initiatives. Microservices containerization and orchestration platforms such as Kubernetes allow enterprises to deploy scalable and flexible applications. However these architectures introduce new operational challenges including service coordination security management and dynamic workload balancing. Researchers have emphasized the need for intelligent automation systems that can manage these complexities without extensive human intervention.

Multi agent systems have gained significant attention as a solution for distributed decision making in complex environments. In such systems autonomous agents collaborate to perform tasks that would otherwise require centralized control mechanisms. These agents can analyze local data communicate with other agents and coordinate actions to achieve global system objectives. Multi agent architectures have been applied in domains such as smart manufacturing robotics network management and cybersecurity.

Cybersecurity remains a critical concern in cloud based digital ecosystems. Modern enterprise infrastructures face a wide range of threats including ransomware attacks data breaches distributed denial of service attacks and insider threats. AI driven security platforms have been developed to detect abnormal network behavior identify potential vulnerabilities and respond to security incidents in real time. Integrating these capabilities into autonomous infrastructure management systems can significantly improve organizational resilience against cyber threats.

Despite these advancements many existing solutions focus on isolated components of infrastructure management rather than providing an integrated framework that combines artificial intelligence security automation and cloud orchestration. This research addresses this gap by proposing a comprehensive multi agent AI architecture capable of coordinating infrastructure operations security intelligence and digital transformation processes.

III. PROPOSED INTELLIGENT MULTI AGENT AI ARCHITECTURE

The proposed architecture introduces a distributed system of intelligent agents that collaborate to manage cloud native enterprise infrastructure. Each agent is responsible for a specific functional domain while sharing information with other agents through a centralized coordination framework. The architecture is designed to operate across hybrid cloud environments integrating data analytics security monitoring and infrastructure automation capabilities.

The architecture consists of several layers including the data collection layer agent intelligence layer decision orchestration layer cloud infrastructure layer and application service layer.

The data collection layer gathers operational information from enterprise infrastructure including system logs network telemetry application performance metrics and security alerts. These data streams provide the foundation for machine learning models and real time analytics processes.

The agent intelligence layer contains specialized AI agents responsible for performing different operational tasks. These include monitoring agents that track system health security agents that analyze threat patterns optimization agents that manage resource allocation and compliance agents that ensure regulatory adherence. Each agent applies machine learning models and rule based reasoning mechanisms to analyze data and generate actionable insights.

The decision orchestration layer coordinates interactions among the agents and ensures that their actions align with overall enterprise objectives. This layer uses reinforcement learning algorithms and collaborative decision models to determine the most effective infrastructure management strategies. The coordination framework enables agents to share knowledge adapt to changing environments and respond collectively to system events.

The cloud infrastructure layer includes container orchestration platforms microservices architectures virtual machines and distributed storage systems. The multi agent AI framework integrates with these technologies to automate resource provisioning manage workloads and maintain system reliability.

The application service layer supports enterprise business applications analytics platforms and user interfaces. By integrating intelligent infrastructure automation with application level services organizations can achieve seamless digital transformation while maintaining operational security and performance.

IV. METHODOLOGY

The research methodology involves designing the multi agent architecture developing conceptual models for agent interactions and evaluating the effectiveness of the proposed framework using simulation based analysis. The study focuses on three primary components including intelligent agent design data driven decision mechanisms and infrastructure automation workflows.

The intelligent agents are designed using machine learning algorithms capable of analyzing infrastructure data and generating operational recommendations. Each agent operates autonomously but communicates with other agents through a coordination protocol that ensures synchronized system behavior.

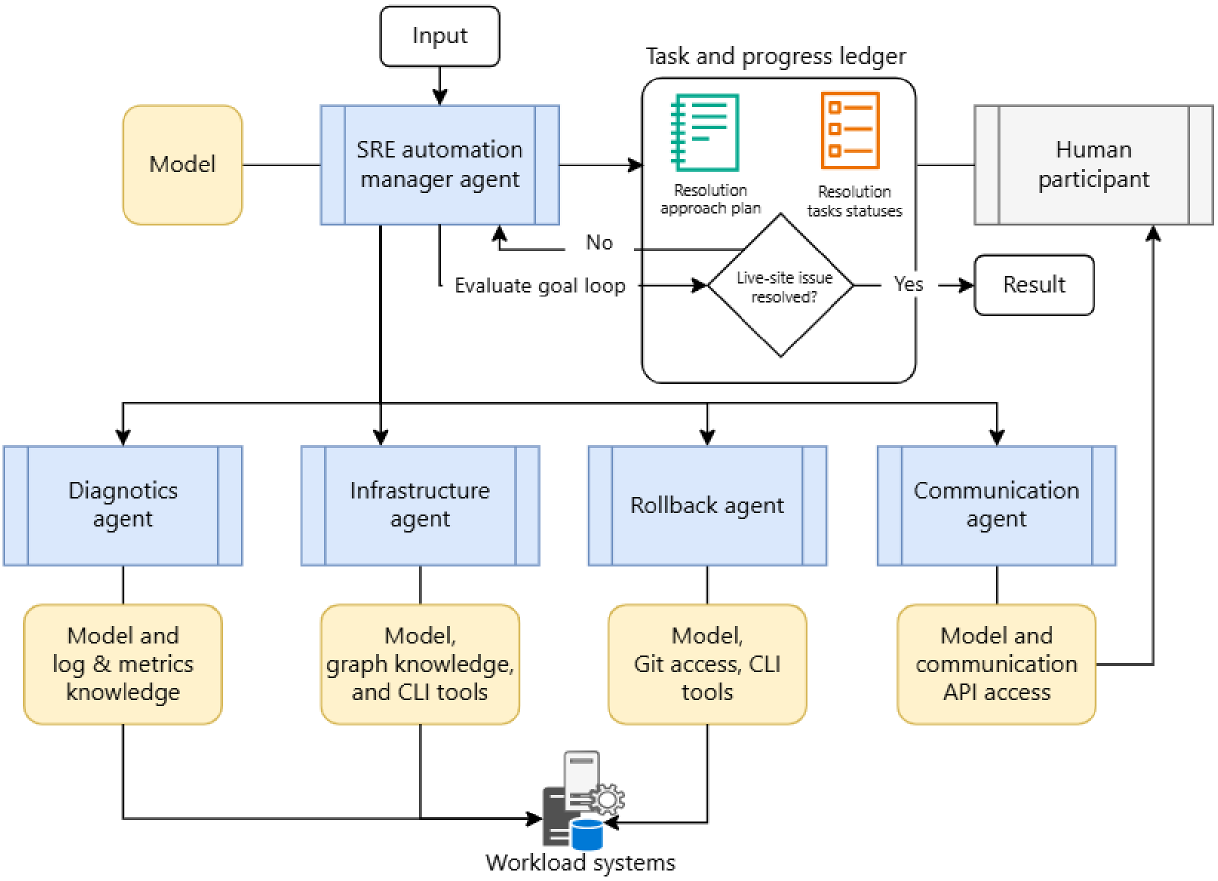
Input
Task and progress ledger
Model
SRE automation manager agent
Resolution approach plan
Resolution tasks statuses
Human participant
No
Evaluate goal loop
Live-site issue resolved?
Yes
Result
Diagnostics agent
Infrastructure agent
Rollback agent
Communication agent
Model and log & metrics knowledge
Model, graph knowledge, and CLI tools
Model, Git access, CLI tools
Model and communication API access
Workload systems

Figure 1: Multi-Agent SRE Automation Architecture for Intelligent Infrastructure Management

The figure illustrates a **Multi-Agent Site Reliability Engineering (SRE) Automation Architecture** designed to support intelligent infrastructure management and automated incident resolution in modern cloud-based systems. The architecture integrates multiple specialized agents coordinated by a central automation manager to detect, analyze, and resolve operational issues within enterprise workload environments.

At the top of the architecture, **input data** is provided to the **SRE automation manager agent**, which acts as the central control component of the system. This manager interacts with a **machine learning model** to analyze incoming operational signals and determine appropriate actions. The manager agent initiates a **goal evaluation loop**, continuously assessing system status and determining whether a detected issue has been successfully resolved.

The system maintains a **task and progress ledger**, which records the resolution approach plan and tracks the status of tasks executed by the agents. This ledger functions as a coordination and monitoring mechanism, ensuring transparency in automated decision processes. If a live-site issue remains unresolved, the automation manager continues coordinating additional agent actions until the issue is mitigated. Once resolved, the system produces a final result that may also be reviewed by a **human participant** for validation or oversight.

The architecture includes several **specialized operational agents**, each responsible for a specific infrastructure management function:

- **Diagnostics Agent:** Analyzes system logs, metrics, and monitoring data to detect anomalies and identify the root cause of infrastructure issues.
- **Infrastructure Agent:** Interacts with system infrastructure using knowledge graphs, operational models, and command-line interface (CLI) tools to manage configuration or deployment tasks.
- **Rollback Agent:** Executes corrective actions such as reverting system configurations or application versions using Git repositories and infrastructure management tools.
- **Communication Agent:** Handles communication with external systems and stakeholders through APIs, reporting interfaces, or alerting platforms.

These agents interact directly with the **workload systems**, which represent the operational cloud infrastructure hosting enterprise services and applications.

Overall, this architecture demonstrates how **collaborative AI agents can automate site reliability engineering tasks**, enabling rapid incident detection, automated remediation, infrastructure rollback, and continuous operational monitoring. The integration of AI-driven decision-making with human oversight ensures both efficiency and reliability in managing complex cloud-native environments.

Data driven decision making is implemented using predictive analytics models trained on infrastructure performance metrics and security logs. These models allow the agents to anticipate potential system failures identify security threats and optimize resource allocation strategies.

Infrastructure automation workflows are developed to demonstrate how agents interact with cloud orchestration platforms. For example the optimization agent can automatically adjust container resource allocations based on predicted workload demand while the security agent can initiate automated responses to detected vulnerabilities.

The evaluation process includes performance analysis security assessment and scalability testing. Simulation environments are used to measure how effectively the multi agent architecture improves infrastructure reliability reduces response times and enhances system resilience.

V. RESULTS AND DISCUSSION

The proposed architecture demonstrates significant improvements in infrastructure automation operational efficiency and cybersecurity resilience. Simulation results indicate that the multi agent framework can reduce infrastructure management latency by enabling autonomous decision making across distributed components. The integration of predictive analytics allows the system to identify performance issues before they impact enterprise operations. This proactive approach improves system reliability and reduces downtime in large scale cloud environments. The security agents play a critical role in detecting abnormal behavior patterns across enterprise networks. By analyzing real time telemetry data the agents can identify potential cyber threats and initiate automated response procedures. This capability enhances enterprise cybersecurity posture and reduces reliance on manual incident response processes. Another key advantage of the architecture is its scalability. As enterprise systems expand new agents can be deployed to manage additional infrastructure components without disrupting existing operations. This modular design supports continuous digital transformation and infrastructure modernization. The collaborative nature of the agents also improves decision accuracy. By sharing information and coordinating actions the agents develop a comprehensive understanding of system conditions enabling more effective operational strategies.

VI. CONCLUSION

This research presented an Intelligent Multi Agent Artificial Intelligence Architecture designed to support secure cloud native digital transformation and infrastructure automation. The proposed framework integrates distributed intelligent agents machine learning analytics cybersecurity intelligence and cloud orchestration technologies to create an autonomous enterprise infrastructure management system. The architecture enables proactive monitoring predictive optimization and automated security response across complex digital ecosystems. By distributing decision making among specialized agents the framework enhances scalability resilience and operational efficiency. The integration of

AI driven analytics with cloud native infrastructure platforms allows enterprises to manage dynamic workloads maintain security compliance and support continuous digital innovation. Future research can extend this work by implementing real world prototypes integrating advanced reinforcement learning models and exploring the application of multi agent AI systems in emerging domains such as smart cities industrial automation and autonomous digital enterprises.

REFERENCES

1. Kamadi, S. (2025). Machine learning and AI architecture: A comprehensive framework for production-grade intelligent systems. World Journal of Advanced Research and Reviews, 27(1), 2789–2799.
2. Ravi Kumar Ireddy. (2023). AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 9(2), 894-903.
3. Grandhe, K. (2025). Designing a Scalable Data Lake Architecture on AWS Using Glue and S3. International Journal of Artificial Intelligence Data Science and Machine Learning, 6(3), 60-63.
4. Jagadeesh, S., & Sugumar, R. (2017). Optimal knowledge extraction system based on GSA and AANN. International Journal of Control Theory and Applications, 10(12), 153–162.
5. Adari, V. K. (2024). Interoperability and Data Modernization: Building a Connected Banking Ecosystem. International Journal of Computer Engineering and Technology, 15(6), 653-662.
6. Parathraju, P., & Umasankar, P. (2025). Performance evaluation of ultrathin CdTe-based solar cells with dual absorbers via SCAPS-1D simulation. Scientific Reports, 15(1), 26428.
7. 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.
8. Vijayakumar, R., & Gireesh, G. (2013, July). Quantitative analysis and fracture detection of pelvic bone X-ray images. In 2013 Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
9. Panda, S. S. (2024). Delivering Scalable Cloud Services in China: Microsoft and 21Vianet Collaboration. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11325-11333.
10. Muthusamy, P., Muthirevula, G. R., & Mohammed, A. S. (2025). Zero-Touch Continuous Audit with Hybrid Symbolic-Neural Reasoning. Newark Journal of Human-Centric AI and Robotics Interaction, 5, 80-111.
11. Gaddapuri, N. S. (2025). Digital twin governance: IoT-driven real-time regulatory auditing in smart hospital architecture. International Journal of Computer Technology and Electronics Communication, 8(5), 11515–11524.
12. Surampudi, Y., Kondaveeti, D., & Pichaimani, T. (2023). A Comparative Study of Time Complexity in Big Data Engineering: Evaluating Efficiency of Sorting and Searching Algorithms in Large-Scale Data Systems. Journal of Science & Technology, 4(4), 127-165.
13. Ramidi, M. (2024). Securing Mobile App Development with Compliance Aware CI/CD Pipelines in Government. International Journal of Computer Technology and Electronics Communication, 7(3), 8824-8825.
14. Ramsugeerthi, A., Neela Madheswari, A., Umamaheswari, A., & Prassana, D. (2020). Location navigation assistance for educational institutions using augmented reality. Journal of Xidian University, 14(4), 1342–1347.
15. Gurajapu, A., Anumolu, S., Garimella, V., Chundi, V. M. S. R., & Gubbala, V. S. A. P. (2025). Ethical and Trustworthy Autonomous Agents in Network SecOps: Transparency, Auditing, and Human-in-the-Loop Overrides. Frontiers in Computer Science and Artificial Intelligence, 4(2), 63-66.
16. Vimal Raja, G. (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research, 12(2), 515-518.
17. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
18. Gowda, M. K. S. (2025). Driving Return on Risk-Weighted Assets Improvement via Audit, Analytics, and Advanced Modeling in Bank Portfolio Management. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(3), 12197-12206.
19. 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.

20. Ambati, K. C. (2024). Enterprise-wide procurement consolidation: Ivalua-SAP-EDW integration architecture for global supply chain excellence. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 7(4), 14309–14318.
21. Konda, S. K. (2024). Carbon-native DCIM architectures for AI data centers: Autonomous infrastructure control via smart grid intelligence. World Journal of Advanced Research and Reviews, 21(1), 3008–3318.
22. Suddala, V. R. A. K. (2025, November). FADL-DP and CNN-GRU Driven Cloud Framework for Secure Healthcare E-Commerce Platform. In 2025 5th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 991-996). IEEE.
23. S. Vishwarup et al. (2020). Automatic Person Count Indication System using IoT in a Hotel Infrastructure. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4).
24. Thota, S. (2023). Federated Learning Approaches for Privacy-Preserving Artificial Intelligence in Distributed Cloud Environments. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(3), 118-127.
25. 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.
26. Kalra, S., Faiz, A., Aggarwal, D., Vigenesh, M., Ramesh, P. N., & Elais, S. (2025, December). Optimizing CNNR-NNT Model for Effective Product Recommendation in E-Commerce. In 2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU) (pp. 1-7). IEEE.
27. Kumar, S. A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems, 19(11), 3841-3855.
28. Jothilingam, P. (2025). Towards autonomous commissioning: Integrating digital twins artificial intelligence and smart sensors for next-generation process control systems. Certified Journal of International Research, 5(1), 1-8.
29. Gopinathan, V. R. (2024). Cyber-Resilient Digital Banking Analytics Using AI-Driven Federated Machine Learning on AWS. International Journal of Engineering & Extended Technologies Research, 6(4), 8419-8426.
30. Gadige, C. D. (2025). The evolution of user interface development in Salesforce: From Visualforce to Lightning Web Components. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 8(5), 12883–12890.
31. Namdeo, A. (2022). Federated learning BI across multi-cloud data silos. The International Journal of Research Publications in Engineering, Technology and Management, 5(6), 7893–7903.
32. Pothuri, M. K. (2025). The role of data governance in achieving compliance and trust in healthcare and fintech. IJAIDR–Journal of Advances in Developmental Research, 16(2).
33. Shewale, V. (2025). The Ethics of Cybersecurity: Balancing Security and Privacy in the Digital Age. European Journal of Computer Science and Information Technology, 13(15), 11-20.
34. Sarabu, V. B. (2022). Hybrid on-premise to cloud data migration: A controlled one-way synchronization framework for enterprise-scale modernization. International Journal of Science, Research and Technology, 5(5), 19-33.
35. Viswanathan, V. (2024). Embedding ethical principles into generative AI workflows for project teams. ProQuest. https://www.proquest.com/openview/2f467f07557f45c3a732296d5b78ad70
36. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
37. Thumala, S. R., Madathala, H., & Sharma, S. (2025, March). Towards Sustainable Cloud Computing: Innovations in Energy-Efficient Resource Allocation. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1528-1533). IEEE.
38. Uttama Reddy Sanepalli. (2022). Adaptive Intelligence Framework for Retirement Portfolio Management: Self-Optimizing Infrastructure for Dynamic Asset Allocation and Risk Mitigation. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 8(6), 769-780.
39. Ravi Kumar Ireddy. (2023). AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 9(2), 894-903.
40. Karnam, A. (2023). SAP Beyond Uptime: Engineering Intelligent AMS with High Availability & DR through Pacemaker Automation. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9351–9361. https://doi.org/10.15662/IJRPETM.2023.060501
41. Anumula, S. R. (2025). Real-Time Scheduling Optimization Using Machine Learning in Pilot Trading and Tracking Systems. Journal Of Multidisciplinary, 5(7), 128-133.