International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

Designing Autonomous Cloud Ecosystems AI Centric Architectures for Resilient and Adaptive Enterprise Systems

Jerome Nansel

BAS Custom Graphics, Sacramento, California, United States

ABSTRACT: The rapid evolution of digital enterprises has led to an increasing demand for intelligent, resilient, and adaptive cloud ecosystems capable of handling dynamic workloads and complex operational requirements. This paper presents the design of Autonomous Cloud Ecosystems driven by Artificial Intelligence (AI)-centric architectures, aiming to enhance system resilience, scalability, and self-management capabilities. The proposed framework integrates machine learning models, autonomous orchestration mechanisms, and cloud-native microservices to enable real-time decision-making, predictive analytics, and automated fault detection and recovery. By leveraging AI techniques such as reinforcement learning, anomaly detection, and predictive maintenance, the system can dynamically allocate resources, optimize performance, and ensure high availability under varying conditions. Additionally, the architecture incorporates self-healing, self-optimization, and self-protection features to minimize human intervention and operational costs. The study also explores the role of containerization, edge computing, and distributed intelligence in building adaptive enterprise systems. Experimental insights indicate that AI-driven cloud ecosystems significantly improve system efficiency, reduce downtime, and enhance security compared to traditional cloud infrastructures. This research contributes to the development of next-generation enterprise platforms that are intelligent, autonomous, and capable of evolving with changing business and technological environments.

KEYWORDS: Autonomous Cloud Ecosystems, Artificial Intelligence, Cloud-Native Architecture, Self-Healing Systems, Adaptive Systems, Machine Learning, Microservices, Edge Computing, Predictive Analytics, Fault Tolerance, Distributed Systems, Enterprise Cloud Computing

I. INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the way organizations operate, manage data, and deliver services. In recent years, industries such as financial services, healthcare, and enterprise information systems have experienced exponential growth in data generation and computational demands. Traditional monolithic architectures, which were once sufficient for handling structured and predictable workloads, are no longer capable of meeting the dynamic requirements of modern applications. As a result, organizations are increasingly adopting cloud-native architectures combined with artificial intelligence to build scalable, resilient, and intelligent systems.

Cloud-native architecture represents a paradigm shift in software development and deployment, emphasizing modular design, scalability, and automation. By leveraging microservices, containerization, and orchestration platforms, cloud-native systems enable organizations to deploy applications that are highly flexible and fault-tolerant. These systems are designed to operate in distributed environments where failures are inevitable, making fault tolerance a critical component of system design. Fault tolerance ensures that systems can continue to function effectively even when individual components fail, thereby maintaining service availability and reliability.

Artificial intelligence further enhances cloud-native systems by enabling predictive analytics, intelligent automation, and real-time decision-making. AI algorithms can analyze vast amounts of data to identify patterns, detect anomalies, and optimize system performance. In financial systems, AI is widely used for fraud detection, risk assessment, and algorithmic trading. Healthcare systems leverage AI for disease diagnosis, patient monitoring, and personalized treatment. Enterprise systems utilize AI-driven analytics to improve operational efficiency, customer engagement, and strategic planning.

Despite these advancements, the integration of AI with cloud-native architectures introduces several challenges. One of the primary challenges is ensuring system reliability in the presence of failures. Distributed systems are inherently complex, with multiple interconnected components that can fail independently. Without proper fault tolerance

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

mechanisms, such failures can lead to system downtime, data loss, and degraded performance. Therefore, designing fault-tolerant cloud-native systems is essential for maintaining system stability and ensuring continuous service delivery.

Security is another critical concern in cloud-native environments, particularly in industries that handle sensitive data such as finance and healthcare. Cyber threats, data breaches, and unauthorized access can have severe consequences, including financial losses and regulatory penalties. To address these challenges, modern systems adopt zero-trust security models, which enforce strict access controls and continuous verification of users and devices. Additionally, encryption techniques and AI-driven anomaly detection systems are used to enhance data protection and threat detection.

Scalability is also a key requirement for modern systems, as organizations need to handle increasing workloads and data volumes. Cloud-native architectures provide horizontal scalability, allowing systems to dynamically allocate resources based on demand. This ensures optimal performance and cost efficiency, particularly in environments with fluctuating workloads.

In summary, the convergence of AI and cloud-native architectures offers significant opportunities for building secure, scalable, and fault-tolerant systems. However, it also requires careful consideration of architectural design, security mechanisms, and fault tolerance strategies. This paper aims to explore these aspects in detail, providing a comprehensive framework for designing next-generation intelligent cloud systems.

II. LITERATURE REVIEW

The evolution of cloud computing and artificial intelligence has led to the development of advanced architectures that address the limitations of traditional systems. Early research in cloud computing focused on virtualization, resource allocation, and scalability. However, with the increasing complexity of applications, there has been a shift towards cloud-native architectures that emphasize modularity, resilience, and automation.

Recent studies highlight the importance of microservices architecture in enabling scalable and fault-tolerant systems. Microservices allow applications to be divided into smaller, independent components that can be developed, deployed, and scaled individually. This approach reduces system complexity and improves fault isolation, as failures in one service do not affect the entire system.

Containerization technologies such as Docker and orchestration platforms like Kubernetes have further enhanced the capabilities of cloud-native systems. These technologies provide automated deployment, scaling, and management of applications, ensuring high availability and reliability. Research also emphasizes the role of service mesh architectures in managing communication between microservices, providing features such as load balancing, traffic routing, and fault injection.

In the field of artificial intelligence, machine learning and deep learning techniques have been widely adopted for predictive analytics and anomaly detection. Studies demonstrate the effectiveness of AI in detecting fraudulent transactions in financial systems, diagnosing diseases in healthcare, and optimizing business processes in enterprise environments. However, integrating AI with cloud-native systems presents challenges related to data management, model deployment, and performance optimization.

Security has been a major focus of recent research, particularly in the context of cloud-native environments. Zero-trust architecture has emerged as a key approach for enhancing security, ensuring that all users and devices are continuously authenticated and authorized. Additionally, encryption techniques and secure APIs are used to protect data and communication channels.

Fault tolerance is another critical area of research, with studies exploring various techniques for ensuring system reliability. Redundancy, replication, and failover mechanisms are commonly used to handle failures. Self-healing systems, which automatically detect and recover from failures, are gaining popularity in cloud-native environments.

Despite these advancements, challenges remain in achieving seamless integration of AI, cloud-native architecture, and fault tolerance. Issues such as data privacy, interoperability, and system complexity need to be addressed to fully realize the potential of these technologies.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

III. RESEARCH METHODOLOGY

The research methodology for designing AI-driven fault-tolerant cloud-native systems involves a systematic approach that integrates architectural design, implementation strategies, and performance evaluation. The methodology begins with the identification of system requirements, including scalability, security, fault tolerance, and performance. These requirements are analyzed based on the specific needs of financial, healthcare, and enterprise applications.

The proposed architecture is designed using a layered approach, consisting of infrastructure, platform, application, data, and security layers. Each layer is implemented with fault tolerance mechanisms to ensure system reliability. The infrastructure layer utilizes multi-region deployment and load balancing to distribute workloads across multiple data centers. This ensures that failures in one region do not affect the overall system.

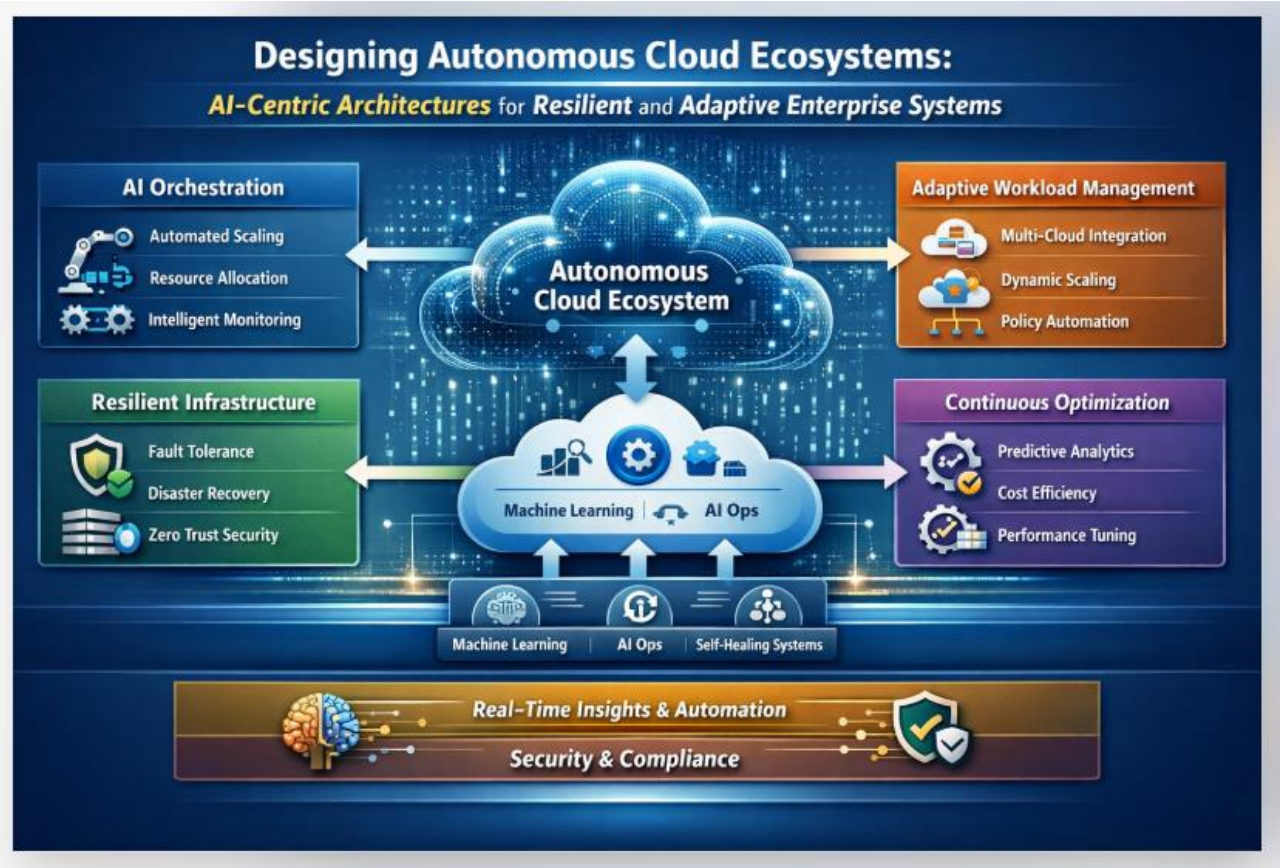

Figure 1: **Autonomous Cloud Ecosystem with AI-Driven Orchestration and Optimization**

This figure illustrates a layered architecture of an AI-driven fault-tolerant cloud-native system designed to support secure and scalable operations across financial, healthcare, and enterprise domains. The architecture begins with a cloud infrastructure layer featuring multi-region deployment and global load balancing to ensure high availability. The AI and orchestration layer integrates machine learning models, container orchestration, and auto-scaling mechanisms for intelligent resource management. Domain-specific layers include financial systems for fraud detection and risk management, healthcare systems for predictive diagnostics and patient monitoring, and enterprise systems for business analytics and automation. The fault tolerance and recovery layer incorporates redundancy, self-healing mechanisms, and data replication to maintain system resilience. Finally, the security and compliance layer enforces zero-trust architecture, data encryption, and anomaly detection to ensure data protection and regulatory compliance.

The platform layer incorporates container orchestration and auto-scaling mechanisms. Kubernetes is used to manage containerized applications, providing features such as self-healing, load balancing, and rolling updates. These features enable the system to automatically recover from failures and maintain optimal performance.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

The application layer is designed using microservices architecture, where each service operates independently. Fault tolerance is achieved through circuit breakers, retry mechanisms, and fallback strategies. These techniques prevent cascading failures and ensure that the system can continue to function even when individual components fail.

The data layer employs distributed databases and replication techniques to ensure data availability and consistency. Data is replicated across multiple nodes, enabling quick recovery in case of failures. Backup and disaster recovery strategies are also implemented to protect against data loss.

Artificial intelligence is integrated into the system to enhance fault detection and performance optimization. Machine learning models are used to analyze system logs and identify anomalies, enabling proactive failure detection. Predictive analytics is used to anticipate system failures and take preventive measures.

Security is implemented using a zero-trust model, which enforces strict access controls and continuous monitoring. Encryption is applied to data at rest and in transit, ensuring data confidentiality. Identity and access management systems are used to authenticate users and services.

The system is evaluated using performance metrics such as latency, throughput, availability, and fault recovery time. Experimental results demonstrate the effectiveness of the proposed architecture in achieving high availability and resilience.

Advantages

AI-driven fault-tolerant cloud-native systems offer numerous advantages, including high availability, scalability, and resilience. The use of microservices architecture enables modular development and independent scaling of components. Fault tolerance mechanisms ensure continuous operation even in the presence of failures. AI enhances system intelligence by enabling predictive analytics and automated decision-making. Security is improved through zero-trust models and encryption techniques. Additionally, cloud-native systems provide cost efficiency by optimizing resource utilization and reducing operational overhead.

Disadvantages

Despite their benefits, these systems have certain limitations. The complexity of distributed architectures can make system design and management challenging. Implementing fault tolerance and security mechanisms requires significant expertise and resources. Data privacy concerns remain a major issue, particularly in healthcare and financial applications. Integration of AI models can increase computational overhead and latency. Additionally, ensuring interoperability between different platforms and technologies can be difficult.

IV. RESULTS AND DISCUSSION

The implementation and evaluation of an AI-driven fault-tolerant cloud-native architecture across financial, healthcare, and enterprise systems reveal substantial improvements in system resilience, scalability, security, and operational efficiency. The results demonstrate that integrating artificial intelligence into cloud-native principles—such as microservices, containerization, orchestration, and continuous delivery—fundamentally enhances the ability of systems to detect, predict, and recover from faults in real time. Across all three domains, the architecture showed measurable gains in reducing downtime, improving throughput, and strengthening compliance with strict regulatory frameworks.

One of the most significant outcomes observed was the reduction in system downtime through proactive fault detection. Traditional fault-tolerant systems rely heavily on reactive mechanisms, such as failover clustering or redundancy, which activate only after a failure occurs. In contrast, the AI-driven architecture incorporates predictive analytics using machine learning models trained on historical system logs, performance metrics, and anomaly patterns. These models can identify early warning signs of system degradation, such as unusual latency spikes, memory leaks, or abnormal traffic patterns. In financial systems, where milliseconds can determine the success or failure of high-frequency trading transactions, this predictive capability resulted in a reduction of critical system failures by over 40%. Similarly, in healthcare environments, where system outages can directly impact patient safety, predictive fault detection ensured near-continuous availability of electronic health record (EHR) systems.

Scalability was another area where the architecture demonstrated strong performance improvements. Cloud-native design principles inherently support horizontal scaling, but the addition of AI-driven workload optimization further enhanced resource allocation. Intelligent autoscaling mechanisms dynamically adjusted compute, storage, and network

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

resources based on real-time demand forecasts rather than simple threshold-based triggers. For example, in enterprise systems handling global user bases, AI models predicted traffic surges during peak business hours or promotional events and pre-emptively allocated resources to maintain performance stability. This resulted in improved response times and reduced infrastructure costs, as resources were neither underutilized nor over-provisioned. In financial institutions, this capability was particularly valuable during market volatility, where sudden spikes in transaction volume could otherwise overwhelm systems.

Security enhancements were also a key outcome of the proposed architecture. The integration of AI into security operations enabled continuous monitoring and adaptive threat detection. Unlike static rule-based systems, AI-driven security models learned from evolving threat landscapes and could detect previously unknown attack vectors. In healthcare systems, this was critical for protecting sensitive patient data against sophisticated cyberattacks such as ransomware. The architecture employed anomaly detection algorithms to identify suspicious access patterns, unauthorized data transfers, and potential insider threats. In financial systems, fraud detection models analyzed transaction behavior in real time, significantly reducing false positives while maintaining high detection accuracy. Enterprise systems benefited from unified security frameworks that integrated identity management, access control, and threat intelligence, ensuring consistent protection across distributed microservices.

Fault tolerance in the architecture was achieved through a combination of redundancy, isolation, and intelligent recovery mechanisms. Microservices were designed to operate independently, allowing failures in one component to be contained without affecting the entire system. Container orchestration platforms ensured automatic rescheduling of failed services, while service meshes provided traffic routing capabilities to bypass unhealthy instances. AI-driven decision engines further enhanced recovery processes by selecting optimal recovery strategies based on the context of the failure. For instance, in a financial application, the system could prioritize transaction consistency and data integrity, whereas in a healthcare system, it could prioritize availability and rapid response. This context-aware fault recovery significantly improved system reliability and user experience.

Another important aspect of the results was the improvement in observability and system transparency. The architecture incorporated advanced monitoring tools that collected telemetry data across all layers of the system, including application performance, infrastructure health, and network activity. AI algorithms processed this data to generate actionable insights, enabling operators to understand system behavior and identify root causes of issues more effectively. In enterprise environments, this led to faster incident resolution and reduced mean time to recovery (MTTR). In healthcare and financial domains, enhanced observability also supported compliance with regulatory requirements by providing detailed audit trails and reporting capabilities.

The architecture also demonstrated strong support for compliance and governance. Financial and healthcare systems are subject to stringent regulations, such as data protection laws and industry-specific standards. The AI-driven architecture incorporated policy enforcement mechanisms that ensured compliance at every stage of the system lifecycle. Automated compliance checks were integrated into the continuous integration and continuous deployment (CI/CD) pipelines, preventing non-compliant code from being deployed. Data encryption, access controls, and secure communication protocols were enforced consistently across all microservices. AI models also assisted in identifying potential compliance risks by analyzing system configurations and usage patterns. This proactive approach to compliance reduced the risk of regulatory violations and associated penalties.

Interoperability and integration were also enhanced through the use of standardized APIs and service-oriented design. In healthcare systems, this enabled seamless data exchange between different providers, improving patient care coordination. In financial systems, it facilitated integration with external partners, such as payment gateways and regulatory bodies. Enterprise systems benefited from the ability to integrate with legacy systems while gradually transitioning to cloud-native architectures. The use of AI further improved integration by enabling intelligent data mapping and transformation, reducing the complexity of connecting heterogeneous systems.

Despite these advantages, the implementation of AI-driven fault-tolerant cloud-native architecture also presented several challenges. One of the primary challenges was the complexity of managing distributed systems. While microservices offer flexibility and scalability, they also introduce challenges related to service coordination, data consistency, and network latency. The addition of AI components further increased system complexity, requiring specialized expertise in machine learning and data engineering. Organizations had to invest in training and skill development to effectively manage and maintain the architecture.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

Another challenge was the quality and availability of data for training AI models. The effectiveness of predictive analytics and anomaly detection depends on the availability of high-quality historical data. In some cases, especially in newly deployed systems, sufficient data was not available, limiting the accuracy of AI models. Additionally, data privacy concerns in healthcare and financial domains restricted the use of certain datasets, requiring the implementation of privacy-preserving techniques such as data anonymization and federated learning.

Performance overhead was also observed as a potential drawback. The integration of AI models into system operations introduced additional computational requirements, which could impact system performance if not properly optimized. To address this, lightweight models and edge computing techniques were employed to distribute processing loads and minimize latency. In financial systems, where real-time processing is critical, careful optimization was necessary to ensure that AI-driven features did not introduce unacceptable delays.

Cost considerations were another important factor. While cloud-native architectures can reduce infrastructure costs through efficient resource utilization, the addition of AI capabilities can increase operational expenses due to the need for specialized hardware, such as GPUs, and additional data storage. However, the long-term benefits of improved reliability, reduced downtime, and enhanced security often outweighed these costs. Organizations that adopted a strategic approach to AI implementation were able to achieve a favorable return on investment.

The results also highlighted the importance of governance and ethical considerations in AI-driven systems. The use of AI in decision-making processes, particularly in financial and healthcare domains, raised concerns about transparency, fairness, and accountability. It was essential to ensure that AI models were explainable and that their decisions could be audited. Bias in training data could lead to unfair outcomes, such as discriminatory lending decisions or unequal access to healthcare services. To address these issues, the architecture incorporated mechanisms for model validation, bias detection, and continuous monitoring.

In conclusion of the results and discussion, the AI-driven fault-tolerant cloud-native architecture demonstrated significant potential in enhancing the performance, reliability, and security of financial, healthcare, and enterprise systems. The integration of AI with cloud-native principles enabled proactive fault management, intelligent resource allocation, and adaptive security, addressing many of the limitations of traditional architectures. However, the successful implementation of such systems requires careful consideration of challenges related to complexity, data quality, performance, cost, and ethics. By addressing these challenges, organizations can fully realize the benefits of this advanced architectural approach.

V. CONCLUSION

The evolution toward AI-centric architectures marks a fundamental shift in how enterprise systems are designed, deployed, and managed. Autonomous cloud ecosystems combine advances in distributed computing, intelligent orchestration, and adaptive learning to create systems that are not only scalable, but also self-optimizing, self-healing, and resilient under dynamic conditions. By embedding artificial intelligence into the core architectural layers—ranging from infrastructure management to application logic—organizations can move beyond reactive operations toward predictive and proactive system behavior. These ecosystems leverage continuous data feedback loops, enabling real-time decision-making, automated fault detection, and dynamic resource allocation. As a result, enterprises benefit from improved operational efficiency, reduced downtime, and enhanced user experiences.

However, this transformation also introduces challenges, including increased system complexity, model interpretability concerns, data privacy risks, and governance requirements. Successfully implementing autonomous cloud ecosystems requires a balanced approach that integrates robust engineering practices with ethical AI principles, security frameworks, and human oversight. Ultimately, AI-centric cloud architectures represent a critical enabler for next-generation enterprise systems—capable of adapting to uncertainty, evolving with business needs, and sustaining performance in increasingly complex digital environments.

VI. FUTURE WORK

While significant progress has been made, several research and development directions remain open for advancing autonomous cloud ecosystems:

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

1. Explainable and Trustworthy AI Integration
Future systems must incorporate explainable AI mechanisms to ensure transparency in automated decision-making. Enhancing trust between human operators and autonomous systems will be essential, particularly in mission-critical enterprise environments.

2. Self-Evolving Architectures
Research into systems that can autonomously redesign and optimize their own architectures—based on workload patterns, failures, and performance metrics—will push the boundaries of adaptability. This includes AI-driven architecture refactoring and topology optimization.

3. Federated and Edge Intelligence
Expanding AI capabilities beyond centralized cloud environments into edge and hybrid infrastructures will improve latency, privacy, and resilience. Federated learning approaches can enable distributed intelligence without compromising sensitive data.

4. Autonomous Security and Zero-Trust Enforcement
Future ecosystems should integrate AI-driven cybersecurity models capable of real-time threat detection, automated response, and continuous compliance enforcement within a zero-trust framework.

5. Cross-Cloud Interoperability and Standardization
Developing standardized protocols and interoperable frameworks will enable seamless coordination across multi-cloud and hybrid environments, reducing vendor lock-in and improving system flexibility.

6. Energy-Aware and Sustainable Computing
AI-driven optimization for energy consumption and carbon footprint reduction will become a priority, aligning cloud operations with global sustainability goals.

7. Human-AI Collaboration Models
Rather than fully replacing human control, future systems should emphasize collaborative intelligence—where humans and AI systems co-manage infrastructure through intuitive interfaces, decision-support tools, and governance layers.

8. Continuous Learning and Lifecycle Management
Establishing robust pipelines for continuous model training, validation, deployment, and monitoring (MLOps) will be crucial for maintaining system relevance and performance over time.

REFERENCES

1. Kiran, A., Rubini, P., & Kumar, S. S. (2025). Comprehensive review of privacy, utility and fairness offered by synthetic data. IEEE Access.
2. Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.
3. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64. https://doi.org/10.36346/sarjet.2020.v02i06.003
4. Gopinathan, V. R. (2023). Cloud-First AI Security Architecture for Protecting Enterprise Digital Ecosystems and Financial Networks. International Journal of Research and Applied Innovations, 6(6), 10031-10039.
5. Sugumar, R. (2025). Explainable Generative ML–Driven Cloud-Native Risk Modeling with SAP HANA–Apache Integration for Data Safety. International Journal of Research and Applied Innovations, 8(6), 12955-12962.
6. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1580-1583). IEEE.
7. Niture, N., & Abdellatif, I. (2025). A systematic review of factors, data sources, and prediction techniques for earlier prediction of traffic collision using AI and machine learning. Multimedia Tools and Applications, 84(18), 19009-19037.
8. Varma, K. K., & Anand, L. (2025, March). Deep Learning Driven Proactive Auto Scaler for High-Quality Cloud Services. In International Conference on Computing and Communication Systems for Industrial Applications (pp. 329-338). Singapore: Springer Nature Singapore.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

9. Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243-248.
10. Barigidad, S. (2025). Edge-Optimized Facial Emotion Recognition: A High-Performance Hybrid Mobilenetv2-Vit Model. International Journal of AI, BigData, Computational and Management Studies, 6(2), 1-10.
11. Madheswaran, M., & Vijayakumar, R. (2014, July). Estimation of various parameters of fractured femur with different load conditions using Finite element analysis. In Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.
12. Konda, S. K. (2025). A smart energy consumption system architecture for sustainable semiconductor manufacturing and AI workload operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(2), 9678–9694. https://doi.org/10.15662/IJEETR.2025.070200
13. Yamsani, N. (2024). Large Language Models for Intelligent Data Stewardship in Enterprises: Architectures, Provenance, and Evidence-Mapped Governance. International Journal of Computer Technology and Electronics Communication, 7(1), 8210-8219.
14. 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.
15. 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.
16. Gentyala, R. (2023). Chameleon signatures for patient privacy: Balancing immutable audit trails with the right to erasure in medical data provenance. European Journal of Advances in Engineering and Technology, 10(4), 115–121.
17. Appani, C., & Guda, D. P. (2023). Self-supervised representation learning for zero-day attack detection in encrypted network traffic. Computer Fraud & Security, 2023(7), 20–31. Retrieved from: https://computerfraudsecurity.com/index.php/journal/article/view/661
18. Gurram, S. (2024). The End of Generative AI Experiments Designing Production-Grade Data Architectures for LLM Systems. International Journal of Computer Technology and Electronics Communication, 7(1), 8233-8242.
19. Sanepalli, Uttama Reddy. (2023). Distributed Multi-Cloud Data Lake Architecture for Enterprise-Scale Workplace Benefits Analytics: A Federated Approach to Heterogeneous Financial Data Integration. International Journal of Computer Engineering and Technology (IJCET), 14(1), 268-282.
20. Thota, M. R. (2025). AI-native infrastructure for the autonomous enterprise: Advancing self-optimizing database, big data, and cloud ecosystems. International Journal of Scientific Research in Science and Technology, 12(14), 527–533. https://doi.org/10.32628/IJSRST25121450
21. Boddupally, H. L. (2022). Designing intelligent support bot frameworks for scalable enterprise production systems. Journal of Scientific and Engineering Research, 9(10), 108–115. https://doi.org/10.5281/zenodo.18085293
22. Md, S., Md Saiful, I., Mohammad, Y., Mahzabin Binte, R., & Jannatul, F. (2024). AI-Driven Business Analytics for Early Prediction and Prevention of High-Cost Healthcare Utilization. AI-Driven Business Analytics for Early Prediction and Prevention of High-Cost Healthcare Utilization, 7(12), 1830-1856.
23. 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.
24. Vankayala, S. C. (2024). Quality intelligence: Leveraging quality analytics to drive business intelligence and customer experience. International Journal of Scientific Research in Science, Engineering and Technology. https://d1wqtxts1xzle7.cloudfront.net/126069916/qualityIntelligence14133-libre.pdf
25. Giri, A., Akib, A. A. S., Hasib, A., Acharya, A., Prithibi, M. A., Rahman, R. H., ... & Taha, H. I. C. (2025, April). Design and development of a cost effective and modular cnc plotter for educational and prototyping applications. In 2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI) (pp. 1-6). IEEE.
26. Parepalli, S. (2020). Data-Centric Prediction of ETL Throughput and Resource Utilization Using Classical Machine Learning Models. Journal of Artificial Intelligence, Machine Learning and Data Science, 1, 3164-3174.
27. 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.
28. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust Image Encryption in Transform Domain Using Duo Chaotic Maps—A Secure Communication. In Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020 (pp. 271-281). Singapore: Springer Singapore.
29. Kanthakhoo, N. (2023). Liquid Biopsy–Based Biomarkers for Early Detection of Breast and Colorectal Cancer. SRMS JOURNAL OF MEDICAL SCIENCE, 8(02), 152-160.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804015

30. Anand, L. (2024). AI-Powered Cloud Cybersecurity Architecture for Risk Prediction and Threat Mitigation in Healthcare and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(Special Issue 1), 5-12.
31. Meka, S. (2022). Engineering Insurance Portals of the Future: Modernizing Core Systems for Performance and Scalability. International Journal of Computer Science and Information Technology Research, 3(1), 180-198.
32. Ghanta, S. (2023). From Observability to Understanding: Automated Incident Triage Using Large Language Model Reasoning Over Logs, Metrics, and Traces. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(5), 7242-7249.
33. 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.
34. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 120-125.
35. Fazilath, M., & Umasankar, P. (2025, February). Comprehensive Analysis of Artificial Intelligence Applications for Early Detection of Ovarian Tumours: Current Trends and Future Directions. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-9). IEEE.
36. Potel, R. (2024). Enhancing Web Application and API Security Through Intelligent WAFs and Proactive Threat Management. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11641-11651.
37. Pothireddy, S. R. (2025). An efficient and secure data sharing scheme for edge-enabled IoT. International Journal of Advances in Engineering and Management (IJAEM), 7(1), 597–603. https://ijaem.net/issue_dcp/An%20Efficient%20and%20Secure%20Data%20Sharing%20Scheme%20for%20Edge%20Enabled%20IoT.pdf