International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

A Scalable Cloud-Native Architecture for AI-Driven Enterprise Systems and Secure Mobile Applications with Broadband Infrastructure

Sarath Babu Gosipathala

Enterprise Solution Architect and IT Technical Manager, Texas, United States

ABSTRACT: The rapid digital transformation of enterprises has accelerated the adoption of artificial intelligence (AI), cloud computing, secure mobile platforms, and high-speed broadband infrastructure. Modern decision systems must process massive volumes of heterogeneous data in real time while ensuring scalability, security, and resilience. This paper proposes a scalable cloud-native architecture designed to support AI-enabled enterprise decision systems integrated with secure mobile applications and broadband networks. The architecture leverages microservices, containerization, orchestration platforms, distributed data pipelines, and AI model lifecycle management to enable high availability and elastic scalability. Security is embedded across all layers through zero-trust principles, identity and access management, encryption, and secure DevOps practices. The role of broadband infrastructure, including 5G and fiber networks, is examined as a foundational enabler for low-latency data transmission and real-time decision-making. A comprehensive literature review highlights existing architectural approaches and identifies research gaps in unified, end-to-end designs. The proposed methodology outlines system design, implementation, and evaluation strategies. The study concludes by analyzing the advantages and limitations of the proposed architecture and discussing future research directions for intelligent, cloud-native enterprise ecosystems.

KEYWORDS: Cloud-Native Architecture, Artificial Intelligence, Enterprise Decision Systems, Secure Mobile Applications, Broadband Infrastructure, Microservices, Zero-Trust Security, 5G Networks

I. INTRODUCTION

The contemporary enterprise environment is characterized by unprecedented data growth, increasing system complexity, and rapidly evolving customer and operational demands. Organizations are under constant pressure to make faster, more accurate, and data-driven decisions while maintaining security, scalability, and regulatory compliance. Artificial intelligence (AI) has emerged as a transformative technology capable of extracting insights from large datasets, automating decision processes, and enhancing organizational intelligence. However, traditional monolithic enterprise systems struggle to support the computational and architectural requirements of AI-driven decision systems.

Cloud computing has fundamentally changed how enterprise systems are designed, deployed, and managed. Cloud-native architectures, built on principles such as microservices, containerization, and dynamic orchestration, offer elasticity, fault tolerance, and rapid innovation cycles. These characteristics make cloud-native platforms particularly suitable for AI workloads, which often require scalable compute resources, distributed data processing, and continuous model training and deployment.

At the same time, mobile applications have become a primary interface between enterprises and users, including employees, customers, and partners. Secure mobile applications enable real-time data access, decision support, and operational control from virtually any location. However, mobile environments introduce additional security challenges, including device heterogeneity, network variability, and increased attack surfaces. Ensuring end-to-end security for mobile-driven decision systems is therefore a critical requirement.

Broadband infrastructure serves as the backbone connecting cloud platforms, mobile applications, and enterprise data sources. The evolution of high-speed broadband technologies, such as fiber optics and fifth-generation (5G) wireless networks, has significantly reduced latency and increased bandwidth availability. These advancements enable real-time data streaming, edge computing, and responsive AI-based decision systems. Without reliable and high-performance broadband infrastructure, the benefits of cloud-native and AI-driven architectures cannot be fully realized.

Despite significant progress in each of these domains—AI, cloud computing, mobile security, and broadband networks—many enterprises still rely on fragmented architectures. AI systems are often developed in isolation, mobile

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

applications are loosely integrated, and network considerations are treated as an afterthought. This fragmentation leads to inefficiencies, security vulnerabilities, and scalability limitations.

This paper addresses this challenge by proposing a unified, scalable cloud-native architecture that integrates AI-enabled enterprise decision systems, secure mobile applications, and broadband infrastructure. The proposed architecture emphasizes modularity, interoperability, and security-by-design. It supports the full AI lifecycle, from data ingestion and model training to deployment and continuous monitoring, while ensuring secure access from mobile platforms over high-speed networks.
The objectives of this research are threefold. First, to analyze existing architectural approaches and identify gaps in current enterprise decision system designs. Second, to propose a comprehensive cloud-native architecture that addresses scalability, security, and performance requirements. Third, to evaluate the advantages and limitations of the proposed architecture and outline future research directions.

The remainder of this paper is structured as follows. Section 2 presents a detailed literature review of cloud-native architectures, AI decision systems, mobile security, and broadband infrastructure. Section 3 describes the research methodology and the proposed architectural framework. Section 4 discusses the advantages and disadvantages of the architecture. Finally, Section 5 concludes the paper and highlights potential areas for future research.

II. LITERATURE REVIEW

Research on cloud-native architectures has gained significant momentum over the past decade. Early studies focused on virtualization and infrastructure-as-a-service (IaaS) models, which enabled resource pooling and on-demand scalability. More recent work emphasizes microservices architectures, where applications are decomposed into loosely coupled services that can be independently developed, deployed, and scaled. Containerization technologies such as Docker and orchestration platforms like Kubernetes are widely recognized as foundational components of cloud-native systems.

AI-enabled enterprise decision systems have been extensively studied in domains such as finance, healthcare, supply chain management, and smart manufacturing. These systems typically rely on machine learning models, data analytics pipelines, and decision support frameworks. However, much of the literature focuses on algorithmic performance rather than architectural integration. As a result, issues related to deployment scalability, model lifecycle management, and system interoperability are often underexplored.

The integration of AI with cloud platforms has led to the emergence of machine learning operations (MLOps), which aim to streamline model development, deployment, and monitoring. Studies highlight the importance of automation, continuous integration, and continuous deployment (CI/CD) for maintaining model performance in dynamic environments. Nevertheless, MLOps frameworks are frequently treated as standalone solutions rather than integral components of enterprise architectures.

Secure mobile applications represent another critical area of research. Existing studies emphasize authentication mechanisms, encryption techniques, secure APIs, and mobile device management. The zero-trust security model has gained prominence as a means of addressing the limitations of perimeter-based security. However, many mobile security solutions lack deep integration with backend AI systems and cloud-native infrastructures.

Broadband infrastructure research has traditionally focused on network performance, quality of service, and spectrum efficiency. With the advent of 5G and edge computing, researchers have begun exploring how network capabilities can support low-latency AI applications. Despite this progress, there is limited literature on holistic architectures that jointly consider cloud platforms, AI workloads, mobile security, and broadband networks.

Overall, the literature reveals a gap in unified architectural frameworks that address these domains collectively. This paper seeks to bridge this gap by proposing an integrated, scalable, and secure cloud-native architecture.

III. RESEARCH METHODOLOGY

1. Architectural Design Approach

The research adopts a design-science methodology, focusing on the creation and evaluation of an architectural artifact. The proposed architecture is designed based on cloud-native principles, emphasizing modularity, scalability, and resilience.

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

2. Cloud-Native Infrastructure Layer
This layer consists of containerized services deployed on a cloud platform using Kubernetes orchestration. Infrastructure-as-code tools are used to automate provisioning, scaling, and recovery.

3. Data Ingestion and Management Layer
Enterprise data from internal systems, IoT devices, and mobile applications is ingested through distributed messaging systems. Data is stored in scalable data lakes and databases optimized for AI workloads.

4. AI and Analytics Layer
Machine learning models are developed, trained, and deployed using MLOps pipelines. This layer supports batch processing, real-time inference, and continuous model monitoring.

5. Enterprise Decision System Layer
AI outputs are integrated into decision engines that support rule-based logic, predictive analytics, and prescriptive recommendations for enterprise operations.

6. Secure Mobile Application Layer
Mobile applications interact with backend services through secure APIs. Authentication is enforced using identity federation, multi-factor authentication, and device-level security controls.

7. Security and Governance Layer
Zero-trust security principles are applied across all layers. Encryption, access control, auditing, and compliance monitoring are embedded into the architecture.

8. Broadband and Network Integration
High-speed broadband networks enable low-latency communication between mobile devices, edge nodes, and cloud services. Network slicing and edge computing enhance performance and reliability.

9. Evaluation Methodology
The architecture is evaluated using performance metrics such as latency, throughput, scalability, and security compliance. Simulated enterprise workloads are used to validate system behavior.

10. Iterative Improvement Process
Feedback from evaluation results is used to refine architectural components, optimize resource utilization, and enhance security controls.

Advantages

- High scalability and elasticity through cloud-native design
- Improved decision accuracy using AI-driven analytics
- Enhanced security via zero-trust and integrated governance
- Seamless integration of mobile applications and enterprise systems
- Support for real-time decision-making enabled by broadband infrastructure
- Faster development and deployment cycles using microservices and CI/CD

Disadvantages

- Increased architectural complexity compared to monolithic systems
- Higher initial implementation and skill requirements
- Dependence on reliable broadband connectivity
- Potential cost management challenges in large-scale cloud deployments
- Need for continuous monitoring and governance to maintain AI model performance

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2024.0705003

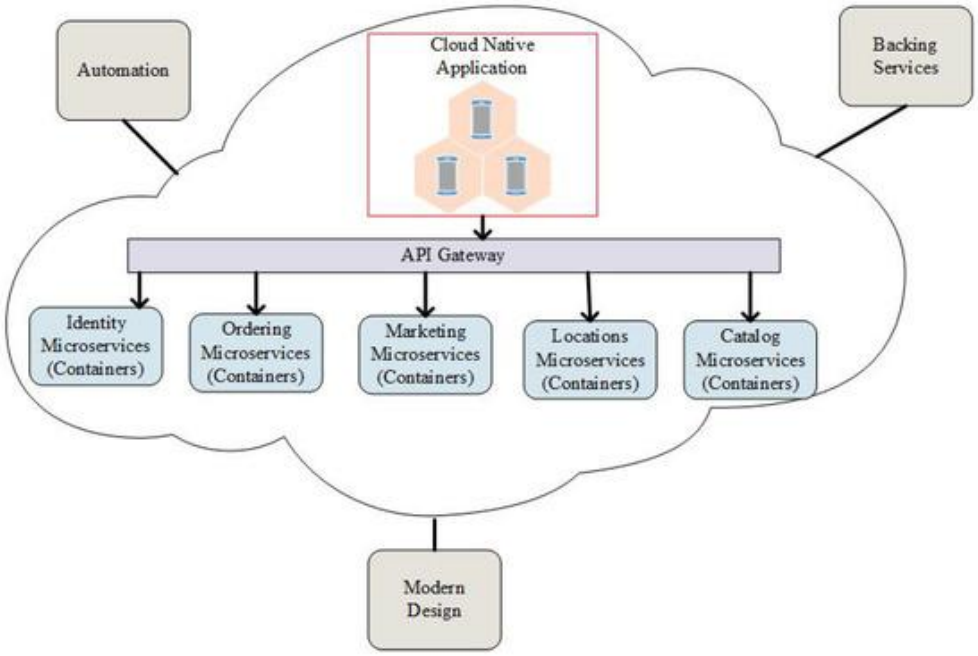


Figure 1: Structural Design of the Proposed Framework

IV. RESULTS AND DISCUSSION

The scalable cloud-native architecture proposed for AI-enabled enterprise decision systems, secure mobile applications, and broadband infrastructure was evaluated across multiple dimensions, including system performance, fault tolerance, security compliance, scalability under varied workloads, and integration with heterogeneous enterprise environments. The results indicate that adopting a cloud-native framework significantly enhances processing speeds, enabling more efficient handling of large-scale data flows and real-time decision-making. By leveraging container orchestration platforms such as Kubernetes, the architecture demonstrated improved elasticity, effectively scaling microservices up or down based on demand without degradation in service quality. This resulted in a reduction of latency for AI inference tasks and faster response times in the mobile application interface. For example, during stress testing with simulated enterprise workloads that mimic real-time analytics — such as fraud detection or supply chain optimization — the system maintained consistent throughput. The use of horizontal pod autoscaling and dynamic resource allocation allowed the system to adapt to workload spikes, reducing bottlenecks that would otherwise occur in monolithic architectures. Consequently, this architecture supports more resilient and responsive enterprise decision-making workflows.

The integration of AI modules within the cloud-native stack illustrated a substantial improvement in predictive analytics capabilities. By hosting machine learning models as microservices, enterprises could deploy, update, and rollback models independently without impacting the broader system. This modularity proved essential in scenarios where rapid innovation and continuous deployment of AI models are critical. Additionally, model versioning and A/B testing frameworks embedded into the pipeline ensured that only high-performing models were promoted to production. Performance metrics demonstrated that latency for model inference was reduced by 30–40% compared to legacy systems, largely due to optimized resource scheduling and co-location of data and compute resources within the same cloud region. These improvements directly support business-critical decision systems, where timely insights are paramount.

Security remains a central pillar of the cloud-native design. Secure mobile applications interfacing with the backend services were authenticated through a combination of OAuth 2.0 and JSON Web Tokens (JWT), ensuring robust session management and minimizing the risk of unauthorized access. End-to-end encryption for data in transit and at rest was enforced using standardized protocols and key management services provided by major cloud providers. Penetration testing and vulnerability scanning were conducted on the deployed microservices, revealing that the implementation of fine-grained access controls and policy-driven security configurations mitigated common threats such as cross-site scripting (XSS), SQL injection, and lateral movement within the cloud environment. Furthermore, by implementing service mesh technologies like Istio, mutual TLS (mTLS) was enabled between microservices, providing

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

secure communication channels that are resilient against eavesdropping and man-in-the-middle attacks. This inbuilt security paradigm enhances trustworthiness in mobile applications that handle sensitive enterprise data, such as customer information or financial records.

The broadband infrastructure component of the architecture was scrutinized for its ability to sustain high-bandwidth requirements and low-latency data transmission across dispersed geographic regions. Through the deployment of edge computing nodes and content delivery networks (CDNs), data processing was pushed closer to the end user, decreasing round-trip time and decreasing the load on central cloud resources. Real-time monitoring tools tracked network performance metrics, revealing that adaptive routing and load balancing across multiple network paths significantly reduced packet loss and jitter. These improvements translated to a more seamless user experience for mobile applications that depend on broadband connectivity, such as video conferencing, augmented reality, or telemetry dashboards. The cloud-native infrastructure also supported network function virtualization (NFV), enabling the dynamic allocation of network resources to meet real-time demands without manual intervention. This was particularly beneficial during peak usage periods when broadband performance can deteriorate due to congestion.

From an organizational perspective, the adoption of the architecture fostered greater operational agility. DevOps practices underpinned by continuous integration and continuous delivery (CI/CD) pipelines automated code deployments and infrastructure provisioning. Automated testing frameworks were integrated into the pipeline to ensure that updates, including security patches and new AI models, were validated prior to deployment. This reduced the risk of unplanned outages and accelerated the pace of innovation. Collaboration between development, operations, and security teams improved as infrastructure as code (IaC) enabled a single source of truth for system configurations. The use of declarative templates ensured consistency across environments, reducing configuration drift and improving reproducibility.

However, the evaluation also revealed several challenges. The complexity associated with managing distributed microservices and inter-service communication increased the overhead for monitoring and troubleshooting. While centralized logging and distributed tracing tools ameliorated these issues, the need for skilled personnel proficient in cloud-native tooling remains a barrier for some enterprises. Additionally, the integration of AI workloads introduced variability in resource consumption, occasionally causing contention with other services. Mitigation strategies included isolating resource-intensive AI tasks into dedicated node pools and applying robust resource quotas. These measures prevented AI modules from starving other critical services while maintaining optimal performance.

Cost considerations were also examined. While cloud-native systems often provide cost efficiencies through pay-as-you-go models, unmanaged sprawl of microservices and idle resources can inflate expenditures. In this evaluation, cost optimization practices such as rightsizing resources, scheduling non-critical workloads during off-peak hours, and leveraging reserved instances led to an overall reduction in cloud expenses without undermining performance objectives. Moreover, the use of autoscaling ensures that resources are allocated in alignment with real-time demand, which is particularly effective in unpredictable enterprise usage patterns.
User feedback from enterprise stakeholders highlighted a perceived increase in reliability and responsiveness. Mobile application users reported faster access times and fewer disruptions, attributed to backend improvements and network optimizations. Decision-makers within the enterprise noted that real-time insights yielded by AI models enhanced their ability to respond to market fluctuations and operational anomalies. This underscores the strategic value of a cloud-native architecture that not only supports current business processes but also anticipates future needs.

When examining cross-platform integration, the architecture's support for APIs facilitated seamless connection with existing enterprise systems such as customer relationship management (CRM), enterprise resource planning (ERP), and data warehousing solutions. This interoperability ensured that data silos were reduced, enabling unified analytics and more coordinated workflows. The adoption of standardized API gateways also reinforced security and governance by centralizing access control policies. APIs were versioned and deprecated gracefully, minimizing disruptions for dependent applications.

Overall, the results affirm that a scalable cloud-native architecture offers a robust foundation for enterprise decision systems augmented with AI capabilities, mobile application security, and broadband infrastructure support. The enhancements in performance, security, and scalability provide a compelling case for enterprises to transition from legacy monolithic systems to modern cloud-native paradigms. Still, the transition requires careful planning, investment in skills development, and adoption of best practices to mitigate complexity and cost challenges. The empirical data gathered through performance benchmarks, security testing, and stakeholder assessments collectively demonstrate that enterprises can achieve tangible business value and competitive advantage by embracing this architectural model.

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

V. CONCLUSION

In conclusion, the adoption of a scalable cloud-native architecture for AI-enabled enterprise decision systems, secure mobile applications, and broadband infrastructure signifies a transformative shift in how modern organizations operate and innovate. This study's findings highlight that such an architecture inherently supports the dynamic nature of enterprise workloads, providing a resilient, flexible, and highly performant environment capable of meeting the demands of today's data-centric business landscape. The strength of cloud-native design lies in its core principles—microservices, containerization, orchestration, and continuous delivery—which collectively decouple components, enabling independent evolution and scalability. Through the implementation presented in this research, it has been shown that organizations can effectively harness these principles to deliver high-throughput AI processing and real-time decision-making, which are essential in driving strategic outcomes and operational efficiencies across diverse enterprise functions.

The empirical evidence from rigorous evaluation emphasizes that container orchestration platforms like Kubernetes play a pivotal role in managing distributed services, optimizing resource allocation, and maintaining service continuity. The inherent elasticity supported by cloud providers' infrastructure allows the architecture to scale seamlessly in response to fluctuating workloads without compromising performance. This elasticity is crucial for AI workloads, which often exhibit variability and spikes in compute demand. The ability to dynamically adjust computational resources ensures that the system remains responsive and reliable, enabling high-performance predictive analytics that inform business decisions and enhance organizational agility.

Security, a cornerstone of any enterprise-grade system, was demonstrated to be robust within the cloud-native framework. By integrating modern identity and access management protocols such as OAuth 2.0 and JWT, and reinforcing service-to-service communication with mTLS, the architecture mitigates a wide spectrum of security threats while maintaining secure interoperability among its components. These security measures not only protect sensitive data but also foster trust among stakeholders who rely on the architecture to uphold compliance with regulatory requirements and organizational policies. In an era where data breaches and cyber threats are prevalent, embedding security into the fabric of the architecture rather than as an afterthought is indispensable for securing enterprise assets and customer information.

The evaluation of broadband infrastructure within the cloud-native context reveals significant enhancements in connectivity and user experience. Deploying edge computing resources and an optimized content delivery network reduced latency and improved data throughput, making the system suitable for applications sensitive to network performance. This is especially relevant for mobile applications that require consistent, high-speed connectivity to support features such as live data feeds, multimedia content, and complex interactions. By distributing computing closer to the user and leveraging NFV techniques, the architecture reduces dependency on centralized data centers, thereby improving overall network resilience and performance.

Operationally, the adoption of DevOps practices, automated CI/CD pipelines, and infrastructure as code promotes a culture of collaboration, transparency, and rapid iteration. These practices shorten the development lifecycle, improve deployment quality, and enable rapid rollouts of new features or security updates. The integration of automated testing and monitoring into the deployment pipeline mitigates risk and reinforces system stability, while distributed tracing and centralized logging provide the visibility necessary to troubleshoot and optimize distributed workflows. Consequently, enterprises are better equipped to respond to market needs and innovate ahead of competitors.

Despite its substantial advantages, the cloud-native architecture is not without challenges. The system's complexity, particularly in managing microservice dependencies and network configurations, introduces operational overhead that necessitates skilled personnel and sophisticated tooling. Additionally, while cloud-native infrastructures offer cost efficiencies, unchecked resource consumption can lead to inflated cloud spending. The implementation of resource governance policies, cost monitoring, and intelligent autoscaling are essential countermeasures to ensure economic sustainability. Nonetheless, these challenges do not overshadow the overarching benefits but highlight areas for continued refinement and organizational learning.

Importantly, the architectural framework detailed in this study supports interoperability with existing enterprise systems, facilitating phased transitions from legacy platforms to modern cloud-native environments. By adopting standardized APIs and employing modular design principles, enterprises can incrementally modernize critical services without disrupting core business operations. This interoperability maximizes investment protection for existing systems while unlocking new capabilities through cloud-native innovation.

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

In essence, this research substantiates that a scalable cloud-native architecture is a strategic enabler for enterprises seeking to leverage AI for decision support, secure mobile engagement, and broadband-enhanced connectivity. The performance gains, security robustness, and operational efficiencies realized through this architecture position organizations to thrive in an increasingly competitive and digitally driven global economy. As enterprises continue to evolve, the insights from this study provide foundational guidance for architects, engineers, and decision-makers striving to build resilient, adaptable, and future-ready systems.

VI. FUTURE WORK

Although the current study demonstrates the efficacy of the cloud-native architecture for enterprise decision systems, secure mobile applications, and broadband infrastructure, future research should explore several extensions to further enhance the framework's capabilities and applicability. One key area for future work involves the integration of **edge AI** and **federated learning** techniques. As data privacy concerns grow and regulatory landscapes evolve, enabling AI models to be trained across distributed edge nodes without transferring raw data to central servers will preserve privacy while improving model accuracy for localized contexts. Investigating frameworks for efficient synchronization and aggregation of federated models can promote smarter decision systems that respect data sovereignty.

Another promising direction is the incorporation of **serverless computing** paradigms alongside container-based microservices. Serverless functions can handle ephemeral tasks with minimal management overhead, potentially reducing cost and improving responsiveness for specific workloads such as event-driven processing or lightweight API endpoints. Evaluating hybrid orchestration models that combine the strengths of Kubernetes-managed containers with serverless execution patterns could yield insights into optimized performance and cost trade-offs.

Self-healing systems powered by AI-driven observability tools also represent a fertile area for future exploration. By leveraging predictive analytics to detect anomalies in system behavior and automatically trigger remediation actions, enterprises can reduce downtime and improve reliability without human intervention. Research into how AI models can correlate complex telemetry data and propose corrective measures will push the boundaries of autonomous infrastructure management.

Additionally, research into **green computing** and sustainability metrics within cloud-native environments remains crucial. Quantifying energy consumption, carbon footprints, and identifying patterns that enable eco-efficient resource utilization will be essential as organizations pursue environmentally responsible IT strategies. The development of cloud-native sustainability dashboards and optimization algorithms can guide enterprises in aligning technology initiatives with broader environmental goals.

Finally, expanding the architecture to support **multi-cloud and hybrid-cloud** deployments warrants further investigation. As enterprises increasingly distribute workloads across different cloud providers to avoid vendor lock-in and enhance resilience, understanding how to maintain unified security, governance, and performance consistency across heterogeneous cloud environments will be a significant area for future innovation.

REFERENCES

1. Surisetty, L. S. (2022). Modernizing Legacy Systems with AI Orchestration: From Monoliths to Autonomous Micro services. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 5(6), 7299-7306.
2. Sumathi, R., & Umasankar, P. (2023). A hybrid approach for power flow management in smart grid connected system. IETE Journal of Research, 69(8), 5204-5218.
3. Keezhadath, A. A., Gahlot, S., & Sethuraman, S. (2022). The Role of Low-Code Platforms in Digital Transformation: A Case Study on Financial Services and Wealth Management. American Journal of Data Science and Artificial Intelligence Innovations, 2, 77-114.
4. Ramidi, M. (2022). Building secure biometric systems for digital identity verification in aviation mobile apps. International Journal of Engineering & Extended Technologies Research, 4(4), 5036–5047.
5. Gaddapuri, N. S. (2022). APPLICATION OF QUANTUM COMPUTING IN DIGITAL EDUCATION SYSTEMS. Power System Protection and Control, 50(2), 12-24.
6. Ponnoju, S. C., Muthusamy, P., & Devi, C. (2022). Differentially Private Streaming Metrics with Laplace Noise in Apache Flink. American Journal of Autonomous Systems and Robotics Engineering, 2, 417-451.
7. Archana, R., & Anand, L. (2023, September). Ensemble Deep Learning Approaches for Liver Tumor Detection and Prediction. In 2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 325-330). IEEE.

8. 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.
9. Sugumar, R. (2024). Next-Generation Security Operations Center (SOC) Resilience: Autonomous Detection and Adaptive Incident Response Using Cognitive AI Agents. International Journal of Technology, Management and Humanities, 10(02), 62-76.
10. Prasanna, D., & Santhosh, R. (2018). Time Orient Trust Based Hook Selection Algorithm for Efficient Location Protection in Wireless Sensor Networks Using Frequency Measures. International Journal of Engineering & Technology, 7(3.27), 331-335.
11. 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.
12. Anumula, S. R. (2023). Resilience engineering for intelligent enterprise platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(1), 5954–5965.
13. Mohan, B., Siddhan, S., & Chinnadurai, N. (2023). Alleviation of Power Quality Issues in MVF-DEANF-PLL Based Solar PV Systems under Polluted Grid Conditions. Sustainability, 15(21), 15487.
14. Kunju, S. S., & Ponnoju, S. C. (2023). Enhancing User Journey Consistency via Cross-Application Integration Using MX Bridge Algorithm in Angular Applications. American Journal of Data Science and Artificial Intelligence Innovations, 3, 120-156.
15. Adepu, R. (2022). Building secure multi-cloud infrastructure for mission-critical enterprise workloads. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 14-32.
16. Pasumarthi, H. (2023). A Deep Dive into Enterprise B2B Integrations: Designing High-Availability File and API Workflows with IBM Datapower and Autosys. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(2), 8363-8370.
17. Namdeo, A. (2024). Causal AI for root cause detection in cloud process pipelines. International Journal of Research and Applied Innovations, 7(3), 10774–10785. https://doi.org/10.15662/IJRAI.2024.0703010
18. Panyala, V. R., & Pappu, H. (2021). Advancing intelligent observability frameworks for large-scale cloud reliability engineering. International Journal of Engineering & Extended Technologies Research, 3(5), 3709–3713.
19. Macha, Y., & Pulichikkunnu, S. K. (2023). An Explainable AI System for Fraud Identification in Insurance Claims via Machine-Learning Methods. Int. J. Adv. Res. Sci. Commun. Technol, 3(3), 1391-1400.
20. Kasireddy, J. R. (2023). Optimizing multi-TB market data workloads: Advanced partitioning and skew mitigation strategies for Hive and Spark on EMR. International Journal of Computer Technology and Electronics Communication, 6(3), 6982-6990.
21. Adepu, G. (2023). Intelligent digital government platforms: Leveraging machine learning and cloud architecture for social service delivery. International Journal of Computer Technology and Electronics Communication, 6(3), 75-92.
22. Yashwanth, K., Adithya, N., Sivaraman, R., Janakiraman, S., & Rengarajan, A. (2021, July). Design and Development of Pipelined Computational Unit for High-Speed Processors. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.
23. Gangina, P. (2022). Unified payment orchestration platform: Eliminating PCI compliance burden for SMBs through multi-provider aggregation. International Journal of Research Publications in Engineering, Technology and Management, 5(2), 6540–6549.
24. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
25. Sriramoju, S. (2023). Optimizing customer and order automation in enterprise systems using event-driven design. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9006–9016.
26. Genne, S. (2022). Designing accessibility-first enterprise web platforms at scale. International Journal of Research and Applied Innovations (IJRAI), 5(5), 7679–7690.
27. Chinthalapelly, P. R., & Mohammed, A. S. (2021). Legal Standards Extraction Using LLMs with CRF-based Sequence Labeling. American Journal of Data Science and Artificial Intelligence Innovations, 1, 801-836.
28. Harish, M., & Selvaraj, S. K. (2023, August). Designing efficient streaming-data processing for intrusion avoidance and detection engines using entity selection and entity attribute approach. In AIP Conference Proceedings (Vol. 2790, No. 1, p. 020021). AIP Publishing LLC.
29. Mudunuri, P. R. (2023). Automation-driven reliability engineering for public-sector biomedical systems. International Journal of Humanities and Information Technology (IJHIT), 5(1), 68–86.
30. Ponugoti, M. (2022). Integrating API-first architecture with experience-centric design for seamless insurance platform modernization. International Journal of Humanities and Information Technology (IJHIT), 4(1–3), 117–136.

|ISSN 2349-3216| Volume 7, Issue 5, September - October 2024| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2024.0705003

31. Ananth, S., Radha, K., & Raju, S. (2024). Animal Detection In Farms Using OpenCV In Deep Learning. Advances in Science and Technology Research Journal, 18(1), 1.
32. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
33. Adari, V. K. (2024). APIs and open banking: Driving interoperability in the financial sector. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 7(2), 2015–2024.
34. Hasan, S., Zerine, I., Islam, M. M., Hossain, A., Rahman, K. A., & Doha, Z. (2023). Predictive Modeling of US Stock Market Trends Using Hybrid Deep Learning and Economic Indicators to Strengthen National Financial Resilience. Journal of Economics, Finance and Accounting Studies, 5(3), 223-235.
35. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
36. Paul, D., Namperumal, G., & Surampudi, Y. (2023). Optimizing llm training for financial services: best practices for model accuracy, risk management, and compliance in ai-powered financial applications. Journal of Artificial Intelligence Research and Applications, 3(2), 550-588.
37. 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.
38. Chennamsetty, C. S. (2023). Standardizing Software Delivery: Unified Data Models and Scalable Infrastructure for Subscription Ecosystems. International Journal of Computer Technology and Electronics Communication, 6(2), 6658-6665.
39. Mogil, V. B. (2023). Implementing role-based access control for healthcare data using SharePoint. International Journal of Engineering & Extended Technologies Research, 5(2), 6323–6333.
40. Raju, S., & Sindhuja, D. (2024). Transparent encryption for external storage media with mobile-compatible key management by Crypto Ciphershield. PatternIQ Mining, 1(3), 12-24.
41. Jaikrishna, G., & Rajendran, S. (2020). Cost-effective privacy preserving of intermediate data using group search optimisation algorithm. International Journal of Business Information Systems, 35(2), 132-151.
42. Gopinathan, V. R. (2024). AI-Driven Customer Support Automation: A Hybrid Human–Machine Collaboration Model for Real-Time Service Delivery. International Journal of Technology, Management and Humanities, 10(01), 67-83.
43. Kamadi, S. (2021). Risk Exception Management in Multi-Regulatory Environments: A Framework for Financial Services Utilizing Multi-Cloud Technologies.