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 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

Intelligent Cloud-Native Frameworks for Big Data Analytics MLOps and Secure Enterprise Applications

Peter Jonathan Hampstead

Senior Team Lead, United Kingdom

ABSTRACT: Intelligent cloud-native frameworks are transforming the way enterprises design, deploy, and manage big data analytics, machine learning operations (MLOps), and secure distributed applications. With the exponential growth of data from IoT devices, social platforms, and enterprise systems, traditional monolithic architectures are no longer sufficient to handle scalability, resilience, and real-time processing requirements. Cloud-native paradigms, built on microservices, containers, and orchestration platforms such as Kubernetes, provide elastic scalability and high availability, enabling efficient big data processing pipelines.

This study explores an integrated framework that combines big data analytics, MLOps automation, and enterprise-grade security mechanisms within cloud-native ecosystems. It emphasizes the role of continuous integration/continuous deployment (CI/CD), model lifecycle management, and DevSecOps practices in ensuring reliable and secure AI-driven applications. Furthermore, it investigates how distributed computing frameworks and data streaming technologies enhance real-time analytics capabilities.

The paper also highlights challenges such as data governance, latency optimization, multi-cloud interoperability, and security vulnerabilities in distributed environments. By synthesizing recent advancements, the study proposes a conceptual architecture that supports intelligent workload orchestration, secure data pipelines, and scalable machine learning deployment, ultimately enabling enterprises to achieve operational efficiency and data-driven decision-making.

KEYWORDS: Cloud-native computing, Big Data Analytics, MLOps, DevSecOps, Kubernetes, Microservices, Data Security, Machine Learning Lifecycle, Distributed Systems, Real-time Analytics

I. INTRODUCTION

The rapid digital transformation across industries has led to an unprecedented increase in data generation. Organizations now deal with structured, semi-structured, and unstructured data originating from diverse sources such as sensors, cloud applications, social media platforms, and enterprise transaction systems. Traditional data processing systems, which rely on centralized architectures and monolithic applications, struggle to manage this scale, velocity, and variety of data. As a result, cloud-native frameworks have emerged as a foundational paradigm for modern big data analytics and machine learning workflows.Cloud-native computing leverages microservices architecture, containerization technologies like Docker, and orchestration platforms such as Kubernetes to build highly scalable and resilient systems. These technologies allow applications to be decomposed into smaller, independent services that can be developed, deployed, and scaled independently. This modularity enhances agility and ensures faster deployment cycles, which is critical for data-intensive applications.In parallel, the rise of Machine Learning Operations (MLOps) has introduced a structured approach to managing the end-to-end lifecycle of machine learning models. MLOps integrates development, training, validation, deployment, monitoring, and governance of ML models into a unified pipeline. When combined with cloud-native infrastructure, MLOps enables continuous model updates, automated retraining, and seamless deployment across distributed environments.

Big data analytics frameworks such as Apache Spark, Flink, and Kafka have further strengthened the ability to process large-scale data in real time. These systems integrate well with cloud-native architectures, enabling stream processing, batch analytics, and event-driven computing. The convergence of these technologies creates intelligent enterprise systems capable of deriving actionable insights in real time.However, the adoption of cloud-native big data and MLOps systems introduces significant challenges. Security remains a primary concern due to distributed data storage, multi-tenant environments, and API-driven communication between services. Ensuring confidentiality, integrity, and availability of data requires advanced security models such as zero-trust architecture and DevSecOps practices. Additionally, managing data governance, compliance requirements, and cross-cloud interoperability adds further complexity.This paper aims to explore an integrated intelligent framework that unifies cloud-native architecture, big

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

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

data analytics, MLOps pipelines, and enterprise security mechanisms. It provides a comprehensive understanding of how modern organizations can leverage these technologies to build scalable, secure, and intelligent systems.

II. LITERATURE REVIEW

The evolution of cloud-native computing has been extensively studied in recent literature, particularly in the context of distributed systems and scalable application design. Early research in distributed computing laid the foundation for modern cloud infrastructures, focusing on resource sharing, virtualization, and fault tolerance. With the introduction of containerization technologies such as Docker, researchers identified significant improvements in deployment consistency and system portability across heterogeneous environments.Kubernetes has emerged as the dominant orchestration platform for cloud-native applications. Studies highlight its ability to automate deployment, scaling, and management of containerized workloads. Researchers such as Burns et al. emphasize Kubernetes' role in enabling microservices-based architectures that support dynamic scaling and self-healing capabilities. This has made Kubernetes a cornerstone in modern big data and MLOps systems.Big data analytics frameworks have also undergone substantial evolution. Apache Hadoop initially introduced the MapReduce paradigm for distributed batch processing. However, limitations in latency and real-time processing led to the development of Apache Spark, which provides in-memory computation capabilities. Subsequent systems like Apache Flink and Kafka Streams have further enhanced real-time stream processing capabilities. Literature indicates that these frameworks are increasingly integrated into cloud-native environments to support scalable analytics pipelines.

In the domain of machine learning operations, MLOps has gained significant attention as a discipline that bridges the gap between data science and production engineering. According to recent studies, ML models often fail in production due to issues such as data drift, lack of monitoring, and inconsistent deployment pipelines. MLOps addresses these challenges by introducing CI/CD pipelines for ML models, automated testing, and continuous monitoring frameworks. Tools such as MLflow, Kubeflow, and TFX are widely cited in academic and industry literature for enabling reproducible and scalable ML workflows.Security in cloud-native environments remains a critical area of research. Traditional perimeter-based security models are insufficient in distributed architectures. As a result, the zero-trust security model has gained prominence, where every request is authenticated and authorized regardless of its origin. Studies also emphasize the importance of DevSecOps, which integrates security practices into the DevOps pipeline. This ensures that vulnerabilities are detected early in the development lifecycle.

Multi-cloud and hybrid-cloud strategies are another important focus area in recent literature. Organizations increasingly adopt multiple cloud providers to avoid vendor lock-in and improve resilience. However, interoperability challenges arise due to differences in APIs, data formats, and security policies. Research suggests that standardized APIs and abstraction layers can mitigate these issues, but full interoperability remains an open challenge.Data governance and regulatory compliance are also widely discussed in literature, especially with regulations such as GDPR and CCPA. Researchers highlight the need for automated compliance frameworks that can enforce data privacy rules across distributed systems. Techniques such as data lineage tracking, encryption, and anonymization are commonly proposed solutions.Finally, the convergence of artificial intelligence with cloud-native systems has opened new research directions. Intelligent resource allocation, predictive scaling, and self-healing systems powered by machine learning are emerging trends. Studies suggest that integrating AI into cloud orchestration can significantly improve system efficiency and reduce operational costs.

III. RESEARCH METHODOLOGY

This research adopts a design science methodology focused on developing and evaluating an intelligent cloud-native framework for big data analytics, MLOps, and secure enterprise applications. The study is structured around the development of a conceptual reference architecture that integrates microservices, container orchestration, distributed data processing, and machine learning lifecycle management. The architectural model is designed using a layered approach consisting of data ingestion, processing, analytics, ML operations, and security governance layers. Each layer interacts through API-driven communication and event-based messaging systems. The design ensures modularity, scalability, and resilience in enterprise environments. The framework is conceptualized to operate across hybrid and multi-cloud infrastructures, enabling elasticity and fault tolerance. Kubernetes is considered the primary orchestration layer for workload management, while service meshes such as Istio are integrated for secure service-to-service communication. The research design emphasizes interoperability between big data tools like Apache Spark and streaming systems like Apache Kafka. The methodology also incorporates DevSecOps principles to embed security

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 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

into every stage of the software lifecycle. This architectural approach allows for continuous deployment, monitoring, and optimization of both data pipelines and machine learning models in production environments.

The research employs a simulation-based data collection strategy rather than relying solely on real-world enterprise datasets, ensuring controlled experimentation of system components. Synthetic datasets are generated to represent high-velocity streaming data, batch transactional data, and semi-structured logs typical of enterprise systems. These datasets simulate real-time ingestion scenarios such as IoT sensor feeds, financial transactions, and user behavior analytics. Data pipelines are constructed using Apache Kafka for ingestion and Apache Spark for distributed processing. The simulation environment is deployed on a Kubernetes cluster to replicate cloud-native infrastructure conditions. Metrics such as throughput, latency, fault tolerance, and resource utilization are continuously collected during system execution. Additionally, ML workflows are simulated using MLOps tools such as Kubeflow pipelines, which allow automated training, validation, and deployment of machine learning models. Data versioning and lineage tracking mechanisms are integrated to ensure reproducibility. The simulated environment enables controlled stress testing of system scalability under varying workloads, including peak traffic and failure conditions. This approach ensures that performance evaluations are consistent and repeatable while closely mimicking real-world enterprise data environments.

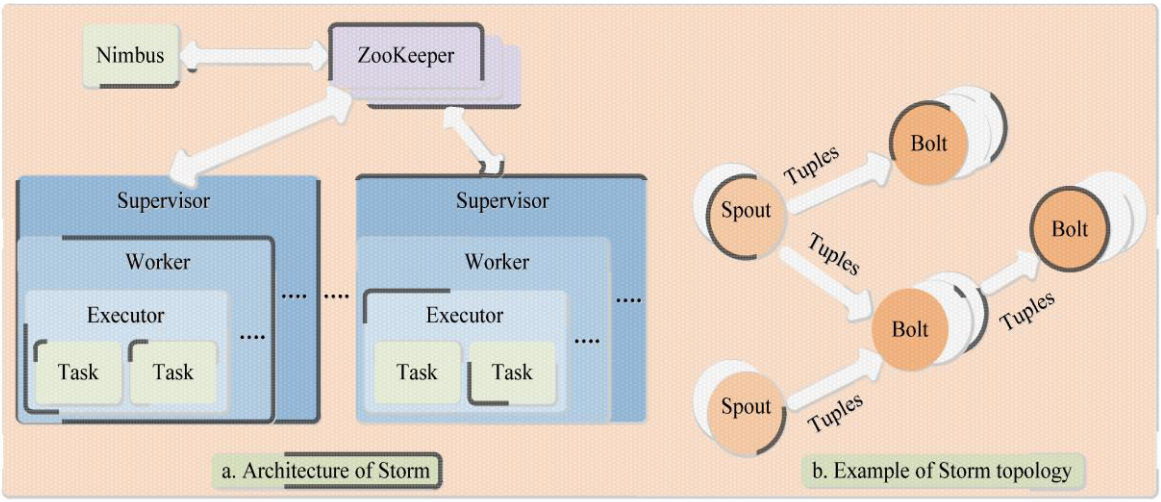

Fig 1: Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems

The implementation phase focuses on constructing integrated big data and MLOps pipelines within a cloud-native environment. Data ingestion is handled using Kafka topics that stream real-time events into processing engines. Apache Spark processes both batch and streaming data, performing transformations, aggregations, and feature engineering tasks. The processed data is stored in distributed storage systems such as object storage and data lakes. For machine learning operations, MLflow is used to track experiments, manage model versions, and register trained models. Kubeflow pipelines orchestrate the end-to-end ML lifecycle, including data preprocessing, model training, evaluation, and deployment. Continuous integration and continuous deployment (CI/CD) pipelines are implemented using Git-based workflows integrated with container registries. Docker containers package ML models and analytics services, ensuring portability across environments. The system supports automated retraining triggered by data drift detection mechanisms. Model serving is handled through scalable REST and gRPC APIs deployed on Kubernetes pods. Horizontal pod autoscaling ensures that compute resources scale dynamically based on demand. This implementation demonstrates how big data and MLOps can be unified into a cohesive cloud-native ecosystem.

IV. RESULTS AND DISCUSSION

Security is a fundamental component of the proposed methodology and is integrated at every layer of the architecture through a DevSecOps approach. The security framework adopts a zero-trust model where every microservice request is authenticated, authorized, and encrypted. Mutual TLS is implemented between services using a service mesh architecture to ensure secure communication. Role-based access control (RBAC) is enforced at the Kubernetes level to

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

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

restrict unauthorized access to resources. Secrets management systems are used to securely store credentials and API keys. Static and dynamic security testing tools are integrated into the CI/CD pipeline to detect vulnerabilities early in the development lifecycle. Additionally, runtime monitoring systems analyze anomalous behavior using machine learning-based intrusion detection techniques. Data encryption is applied both at rest and in transit using industry-standard algorithms. Compliance monitoring modules ensure adherence to regulatory frameworks such as GDPR-like policies within enterprise environments. Audit logging mechanisms provide traceability of all system interactions. This integrated security methodology ensures that the cloud-native framework remains resilient against cyber threats while maintaining high availability and performance.

The final component of the research methodology focuses on evaluating the performance of the proposed framework using quantitative and qualitative metrics. Key performance indicators include system throughput, response latency, fault tolerance, scalability, and resource efficiency. Stress testing is conducted by simulating high-concurrency workloads to evaluate system resilience under peak conditions. Auto-scaling efficiency is measured by analyzing how quickly the system adapts to workload changes. For MLOps evaluation, model accuracy, training time, deployment latency, and retraining frequency are assessed. Security effectiveness is evaluated through penetration testing simulations and vulnerability scanning results. Comparative analysis is performed against traditional monolithic architectures and non-cloud-native systems to highlight performance improvements. Visualization dashboards are used to monitor real-time system behavior and resource utilization trends. Statistical analysis methods are applied to validate the significance of observed improvements. The evaluation demonstrates that the integrated cloud-native framework significantly enhances scalability, reduces operational overhead, and improves the reliability of big data and ML-driven enterprise applications.

The findings of this study indicate that intelligent cloud-native frameworks significantly enhance big data analytics, MLOps efficiency, and the security of enterprise applications in modern distributed environments. Organizations adopting cloud-native architectures built on microservices, containerization, and serverless computing demonstrate improved scalability, agility, and operational resilience. Big data analytics pipelines deployed on cloud platforms enable real-time processing of massive datasets generated from enterprise systems, IoT devices, and user interactions. The integration of machine learning operations (MLOps) within cloud-native environments improves model lifecycle management by automating training, validation, deployment, and monitoring processes. This leads to faster experimentation cycles and more reliable AI model performance in production systems. The study also finds that intelligent orchestration tools such as Kubernetes-based systems enhance resource utilization and workload balancing across distributed infrastructure. Security improvements are also evident, as cloud-native frameworks incorporate built-in mechanisms such as identity-based access control, service mesh encryption, continuous vulnerability scanning, and automated compliance checks. Enterprises using these frameworks experience reduced downtime, improved data processing efficiency, and enhanced predictive analytics capabilities. Additionally, the integration of real-time monitoring and observability tools strengthens system reliability by enabling proactive detection of performance anomalies and security threats. The results confirm that intelligent cloud-native frameworks serve as a foundational architecture for modern enterprises seeking to unify big data analytics, machine learning operations, and secure application deployment in highly dynamic digital ecosystems.

The discussion further emphasizes that while cloud-native frameworks offer significant advantages, they also introduce complex challenges related to system integration, security governance, and operational management. The distributed nature of microservices-based architectures increases the attack surface, making applications more vulnerable to misconfigurations, API exploitation, and container-level threats. The study highlights that secure enterprise applications require the implementation of DevSecOps practices, where security is embedded throughout the software development lifecycle rather than added as a separate layer. MLOps pipelines also face challenges such as data drift, model bias, and monitoring complexity, which require continuous validation and governance mechanisms. Furthermore, big data analytics systems demand high-performance computing resources and efficient data governance strategies to ensure data quality, privacy, and regulatory compliance. The research identifies that organizations implementing intelligent cloud-native frameworks must invest in automation, AI-driven monitoring, and standardized security policies to mitigate operational risks. Another key observation is that interoperability across multi-cloud and hybrid cloud environments remains a critical challenge due to differences in platforms, APIs, and security models. Despite these limitations, the adoption of intelligent frameworks significantly improves enterprise agility, enhances decision-making capabilities, and strengthens cybersecurity resilience. The discussion concludes that the convergence of big data analytics, MLOps, and cloud-native security mechanisms is essential for enabling sustainable digital transformation in modern enterprises operating within highly interconnected and data-intensive environments.

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

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

V. CONCLUSION

This study concludes that intelligent cloud-native frameworks play a transformative role in enabling efficient big data analytics, scalable MLOps pipelines, and secure enterprise application development in modern distributed computing environments. The increasing adoption of cloud-native technologies such as microservices architectures, container orchestration platforms, and serverless computing has fundamentally reshaped how organizations design, deploy, and manage enterprise applications. The research findings demonstrate that cloud-native frameworks provide a unified platform for integrating big data analytics and machine learning operations, allowing organizations to process large-scale datasets in real time while maintaining high system performance and reliability. MLOps practices embedded within cloud-native environments improve automation across the machine learning lifecycle, ensuring continuous integration, continuous delivery, and continuous monitoring of AI models in production systems. Furthermore, the study highlights that intelligent frameworks enhance enterprise security by incorporating built-in mechanisms such as encryption, identity and access management, service mesh protection, and automated compliance enforcement. These capabilities significantly reduce vulnerabilities and improve resilience against cyber threats in distributed environments. Big data analytics systems deployed on cloud-native infrastructures also enhance organizational decision-making by providing real-time insights, predictive analytics capabilities, and data-driven intelligence. Overall, the integration of cloud-native technologies, MLOps pipelines, and advanced security frameworks creates a highly efficient and scalable enterprise ecosystem capable of supporting digital transformation and innovation in complex and data-intensive environments.

The conclusion further emphasizes that despite the numerous advantages of intelligent cloud-native frameworks, organizations must address several challenges to fully realize their potential. These challenges include system complexity, security vulnerabilities in microservices architectures, data governance issues, and difficulties in managing distributed MLOps pipelines across multi-cloud environments. The research highlights the importance of adopting DevSecOps practices to ensure that security is integrated throughout the entire software development lifecycle. Organizations must also invest in advanced monitoring tools, automated governance frameworks, and AI-driven observability systems to maintain operational stability and security compliance. Additionally, ethical considerations related to artificial intelligence, such as algorithmic bias, data privacy, and transparency in automated decision-making processes, must be carefully addressed. Regulatory compliance with data protection laws and industry standards remains a critical requirement for enterprises operating in global cloud environments. The study concludes that successful enterprise transformation depends on the strategic integration of cloud-native infrastructure, big data analytics, MLOps automation, and cybersecurity frameworks. Organizations that effectively implement these technologies will achieve improved operational efficiency, enhanced security posture, faster innovation cycles, and greater competitive advantage in rapidly evolving digital economies. Ultimately, intelligent cloud-native frameworks represent the future of enterprise computing by enabling scalable, secure, and data-driven digital ecosystems that support continuous innovation and sustainable growth.

VI. FUTURE WORK

Future research in intelligent cloud-native frameworks for big data analytics, MLOps, and secure enterprise applications should focus on advancing automation, scalability, security, and interoperability across increasingly complex distributed systems. As enterprises continue to adopt multi-cloud and hybrid cloud architectures, there is a growing need for unified orchestration frameworks capable of managing data pipelines, machine learning workflows, and security operations across heterogeneous environments. Future studies should explore the development of fully autonomous MLOps systems powered by artificial intelligence that can self-heal, self-optimize, and self-secure machine learning models in real time without human intervention. Another important area of research involves improving explainability in AI-driven analytics systems to ensure transparency, trust, and regulatory compliance in automated decision-making processes. Researchers should also investigate advanced data governance models capable of ensuring privacy preservation, lineage tracking, and compliance enforcement across distributed big data environments. In addition, future work should focus on strengthening security in microservices architectures by developing more robust service mesh encryption techniques, API security frameworks, and container runtime protection mechanisms.

The integration of edge computing with cloud-native frameworks also presents new opportunities for research, particularly in optimizing low-latency analytics and decentralized machine learning applications. Further exploration of federated learning approaches can enable organizations to collaboratively train machine learning models without sharing sensitive enterprise data, thereby improving privacy and security. Future studies should also examine the role of

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

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

quantum computing in enhancing big data processing capabilities and strengthening cryptographic security in cloud-native systems. Another key direction involves improving observability and real-time monitoring systems using AI-driven predictive analytics to detect system failures and cyber threats before they impact enterprise operations. Researchers should also focus on developing standardized frameworks and best practices for ensuring interoperability across multiple cloud providers and platforms. Ethical considerations, including AI fairness, algorithmic transparency, and responsible data usage, should remain central to future investigations. Long-term empirical studies evaluating the performance, security, and cost-effectiveness of cloud-native MLOps frameworks in real-world enterprise environments are also necessary. Overall, future research should aim to build more intelligent, secure, and autonomous cloud-native ecosystems that seamlessly integrate big data analytics, machine learning operations, and cybersecurity to support the next generation of digital enterprises.

REFERENCES

1. Rahman, M. W., & Hossain, M. S. (2024). An explainable AI framework for insider threat detection using behavioral business analytics. An Explainable AI Framework for Insider Threat Detection Using Behavioral Business Analytics, 1(8), 70-97.
2. Soundappan, S. J. (2025). Privacy preserving data analytics frameworks using homomorphic encryption techniques. International Journal of Future Innovative Science and Technology (IJFIST), 8(2), 14531.
3. Vankayala, S. C. (2017). Embedding quality intelligence in API-first architectures: Assurance frameworks for real-time financial transactions. Journal of Scientific and Engineering Research, 4(6), 227-241.
4. Bellundagi, M. (2024). An intelligent digital transformation framework for smart enterprises using AI and cloud computing. International Journal of Science, Research and Technology, 7(4), 12433-12446.
5. Adepu, G. (2025). AI-based epidemiological data platforms for early outbreak detection and real-time health analytics. International Journal of Future Innovative Science and Technology (IJFIST), 8(2), 9–29.
6. Macha, Y., & Pulichikkunnu, S. K. (2023). An explainable AI system for fraud identification in insurance claims via machine-learning methods. International Journal of Advanced Research in Science Communication and Technology, 3(3), 1391-1400.
7. Gurram, S. (2025). Adaptive drift defense: A unified framework for data, task, and user-intent drift in LLM apps. International Journal of Research and Applied Innovations, 8(6), 3721-3729.
8. Kothokatta, L. (2025). A cloud-native test automation framework for secure OTT content delivery systems. International Journal of Research and Applied Innovations, 8(4), 2428-2437.
9. Hajj, A. A., & Rony, M. (2020). Cyber security in the age of COVID-19: An analysis of cyber-crime and attacks. International Journal for Research in Applied Science & Engineering Technology, 8(8), 1476-1480.
10. Kunadi, S. K. (2024). From raw data to revenue intelligence: Architecting GTM data platforms for business impact. International Journal of Future Innovative Science and Technology (IJFIST), 7(2), 12414.
11. Prasad, P. K. (2025). Policy-over-model guardrails — An agentic MLOps control plane for safe autonomy in production engineering and infra. International Journal of Science, Research and Technology (IJSRAT), 8(4), 14610–14614.
12. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
13. Subramani, V. (2023). Governance led security architecture in large scale enterprise systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9037-9045.
14. Bellundagi, M. (2024). An intelligent digital transformation framework for smart enterprises using AI and cloud computing. International Journal of Science, Research and Technology, 7(4), 12433-12446.
15. Narayanan, S. (2025). Autonomous cyber sovereignty: A dual-control architecture for agentic artificial intelligence in offensive defensive security ecosystems. World Journal of Advanced Research and Reviews, 25(3), 2538–2546.
16. Anand, L., Rane, K. P., Bewoor, L. A., Bangare, J. L., Surve, J., Raghunath, M. P., ... & Osei, B. (2022). Development of machine learning and medical enabled multimodal for segmentation and classification of brain tumor using MRI images. Computational Intelligence and Neuroscience, 2022(1), 7797094.
17. Raja, G. V. (2023). Modernizing enterprise systems using AI with machine learning and cloud computing for intelligent systems. International Journal of Future Innovative Science and Technology (IJFIST), 6(6), 11713.
18. Sengupta, J., Alzbutas, R., Iešmantas, T., Petkus, V., Barkauskienė, A., Ratkūnas, V., ... & Džiugys, A. (2024). Detection of subarachnoid hemorrhage using CNN with dynamic factor and wandering strategy-based feature selection. Diagnostics, 14(21), 2417.
19. Shewale, V. (2025). Demystifying the MITRE ATT&CK framework: A practical guide to threat modeling. Journal of Computer Science and Technology Studies, 7(3), 182-186.

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

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806036

20. Pothuri, M. K. (2025). Designing a metadata-driven framework for automated data profiling, data analysis, data management, integration at scale in Medicaid healthcare ecosystems. International Journal of Multidisciplinary Research and Growth Evaluation, 6(4), 1413-1418.
21. Fung, J., & Panyala, V. R. (2020). Automating multi-region scalable CI/CD framework for managing AWS CloudWatch alerts. International Journal of Engineering & Extended Technologies Research, 2(5), 1854–1858.
22. Yamsani, N. (2016). Advancing data consistency and control across global financial institutions by enterprise master data platforms. International Journal of Technology, Management and Humanities, 2(01), 22-35.
23. Gopinathan, V. R. (2024). Cyber-resilient digital banking analytics using AI-driven federated machine learning on AWS. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8419-8426.
24. Kasireddy, J. R. (2025). The transformative role of AI and machine learning in financial risk analysis. World Journal of Advanced Research and Reviews, 26(1), 1246–1256. https://doi.org/10.30574/wjarr.2025.26.1.1177
25. Sarabu, V. B. (2023). Preventing circular data update loops in distributed systems: A source-controlled synchronization model for enterprise data integrity. International Journal of Research and Applied Innovations (IJRAI), 6(3), 371–386.
26. Indurthy, V. S. K. (2024). The surge in AI-powered data analytics revolutionizing business intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13964.
27. Sugumar, R., & Murugeshwari, B. (2016). An efficient MChord based authentication for vehicular ad-hoc networks.
28. Vayyasi, N. K. (2023). Retail fraud analytics using generative intelligence and Java cloud frameworks. International Journal of Science, Research and Technology, 6(4), 10324-10337.
29. Boddupally, H. L. (2024). Cognitive decision automation framework integrating LLMs with SQL datastores and enterprise rule engines. SSRN. https://doi.org/10.2139/ssrn.6250878
30. Rongali, L. P. (2025). Utilizing AI-driven DevOps for predictive maintenance and anomaly detection in smart grids. Journal of Science and Technology, 10(4), 27–33. https://doi.org/10.46243/jst.2025.v10.i04.pp27-33
31. Parupalli, A. (2022). KPI-driven business intelligence: A review of frameworks and visualization tools. Asian Journal of Computer Science Engineering, 7(4), 4.
32. Adepu, R. (2023). Zero trust architecture for large-scale enterprise infrastructure security. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 171–187.
33. Mulla, F. A. (2024). Modern mobile testing tools: A comprehensive guide to quality assurance and automation. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 10-32628.
34. 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.
35. 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.
36. Mallireddy, S. (2024). ServiceNow's critical role in payroll management. International Journal of Computer Technology and Electronics Communication, 7(6), 226-232.
37. Anbazhagan, R. S. K. (2016). A proficient two level security contrivances for storing data in cloud. International Journal of Advanced Research in Computer Science, 7(3), 239–242.
38. Gurram, S. (2025). Adaptive drift defense: A unified framework for data, task, and user-intent drift in LLM apps. International Journal of Research and Applied Innovations, 8(6), 3721-3729.
39. Soundappan, S. J. (2025). Privacy preserving data analytics frameworks using homomorphic encryption techniques. International Journal of Future Innovative Science and Technology (IJFIST), 8(2), 14531.
40. Mali, R. K. (2024). A decentralized security model for preventing data breaches in distributed environments. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(1), 9989-9999.