Journal of Cyber-Physical Security and Robotics
Volume 01, Issue 1, 39-45, 2025

Research Article

Advanced Machine Learning and Cloud Data Engineering Architectures for Secure IoT and Enterprise Analytics Systems

P. Shanmugapriya

Associate Professor, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Deemed to be University, Kanchipuram, Tamilnadu, India

Abstract

AI-powered distributed computing and secure cloud transformation frameworks are redefining the architecture of modern intelligent enterprise applications. As organizations increasingly adopt data-intensive and latency-sensitive systems, traditional centralized computing models struggle to meet scalability, resilience, and security requirements. Distributed computing combined with cloud-native paradigms enables dynamic resource allocation, parallel processing, and fault-tolerant execution across geographically dispersed nodes. The integration of Artificial Intelligence (AI) further enhances these systems by enabling predictive scaling, anomaly detection, workload optimization, and intelligent orchestration of computing resources. However, this transformation introduces significant challenges in terms of data security, privacy preservation, multi-tenant isolation, and regulatory compliance. Secure cloud transformation frameworks address these challenges by embedding zero-trust architectures, cryptographic mechanisms, and policy-driven access controls into distributed environments. This paper explores the convergence of AI-driven orchestration and secure distributed cloud systems for intelligent enterprise applications. It highlights architectural models, enabling technologies, and operational frameworks that support scalability, efficiency, and security. The study also examines how enterprises can transition from legacy systems to intelligent cloud ecosystems while maintaining operational continuity and minimizing risk. Ultimately, the research emphasizes that the future of enterprise computing lies in adaptive, self-healing, and intelligence-augmented distributed cloud infrastructures capable of supporting next-generation digital transformation initiatives.

Keywords: AI-powered distributed computing, secure cloud transformation, intelligent enterprise applications, edge computing, cloud-native architecture, zero trust security, workload optimization, data privacy, microservices, orchestration frameworks

Introduction

The rapid evolution of enterprise computing has been significantly influenced by the convergence of distributed computing systems, cloud technologies, and artificial intelligence. Modern organizations are increasingly dependent on intelligent applications that require high availability, real-time responsiveness, and large-scale data processing capabilities. Traditional monolithic architectures are no longer sufficient to handle these demands, leading to a paradigm shift toward distributed and cloud-native ecosystems. These systems distribute computation across multiple nodes, often spanning hybrid and multi-cloud environments, enabling improved scalability, fault tolerance, and performance optimization.

Artificial Intelligence plays a transformative role in this ecosystem by enabling systems to become adaptive and self-managing. AI algorithms are used for predictive analytics, automated resource allocation, anomaly detection, and workload balancing. This intelligence layer allows cloud infrastructures to dynamically adjust to changing workloads and operational conditions without human intervention. As a result, enterprises can achieve higher efficiency and reduced operational costs while maintaining service quality.

However, the transition to distributed cloud environments introduces new complexities, particularly in terms of security and governance. Data is no longer confined to a single controlled environment but is distributed across multiple nodes, increasing the attack surface and

vulnerability exposure. Issues such as unauthorized access, data leakage, and compliance violations become more prominent. Therefore, secure cloud transformation frameworks are essential to ensure data integrity, confidentiality, and availability across distributed systems.

These frameworks typically incorporate zero-trust security models, identity-based access control, encryption mechanisms, and continuous monitoring systems. The zero-trust approach assumes that no entity—internal or external—should be trusted by default, thereby enforcing strict verification for every access request. Additionally, blockchain and distributed ledger technologies are increasingly being explored to enhance transparency and auditability in cloud environments.

Furthermore, edge computing has emerged as a complementary paradigm that brings computation closer to data sources, reducing latency and improving real-time decision-making capabilities. When integrated with AI-powered distributed systems, edge computing enables faster response times and efficient bandwidth utilization. In this context, intelligent enterprise applications are built upon a foundation of interconnected cloud services, distributed computing nodes, and AI-driven orchestration engines. These applications are capable of self-optimization, predictive scaling, and autonomous recovery from failures. The integration of these technologies represents a significant step toward fully autonomous digital enterprises.

Literature Review

Recent advancements in distributed computing and cloud technologies have significantly transformed the landscape of enterprise IT systems. Early research in distributed systems focused primarily on resource sharing and parallel computation, as seen in cluster and grid computing models. These systems laid the foundation for modern cloud computing by enabling computation across multiple interconnected nodes. However, they lacked the elasticity, automation, and intelligence required for today's dynamic enterprise workloads.With the emergence of cloud computing, platforms such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) introduced scalable and on-demand computing resources. According to foundational cloud research, virtualization technologies played a key role in enabling resource abstraction and multi-tenancy. Studies have shown that virtualization improves hardware utilization while reducing operational costs, making cloud computing a viable solution for enterprise-scale applications. Artificial Intelligence integration into cloud systems has been widely explored in recent literature. Machine learning models are increasingly used for predictive auto-scaling, where workloads are forecasted based on historical patterns. Reinforcement learning approaches have been applied to optimize resource allocation in real time, improving system efficiency. Furthermore, AI-driven anomaly detection systems help identify security breaches and performance degradation in distributed environments.

Security remains one of the most critical concerns in cloud transformation. Traditional perimeter-based security models have proven inadequate in distributed environments. As a result, the zero-trust security model has gained significant attention. Research indicates that zero-trust architectures improve security posture by continuously verifying users, devices, and network traffic. Encryption techniques such as homomorphic encryption and secure multi-party computation have also been proposed to enhance data privacy in cloud systems. Edge computing has emerged as a major area of research in recent years. By processing data closer to the source, edge computing reduces latency and bandwidth usage. Studies show that combining edge and cloud computing enables hybrid architectures that support real-time applications such as autonomous vehicles, IoT systems, and smart healthcare. The integration of AI at the edge further enhances decision-making capabilities without relying heavily on centralized cloud infrastructure. Microservices architecture is another key development in distributed computing. Unlike monolithic systems, microservices decompose applications into smaller, independent services that can be deployed and scaled individually. Research suggests that microservices improve system resilience, scalability, and maintainability. However, they also introduce challenges in service orchestration, communication overhead, and security management.

Containerization technologies such as Docker and orchestration tools like Kubernetes have become essential components of modern cloud-native systems. They enable consistent deployment environments and automated scaling across distributed infrastructure. Studies highlight that container orchestration significantly reduces deployment complexity and improves system reliability. Blockchain technology has also been explored as a complementary solution for secure cloud transformation. Its decentralized and immutable nature provides transparency and trust in distributed systems. Research shows that blockchain can enhance data integrity, access control, and auditability in multi-cloud environments. Despite these advancements, several gaps remain in existing literature. One major challenge is the lack of unified frameworks that integrate AI, security, and distributed computing into a cohesive system. Many proposed solutions address individual aspects but fail to provide end-to-end enterprise-level integration. Additionally, issues related to interoperability, regulatory compliance, and energy efficiency remain underexplored.

Overall, the literature indicates a strong trend toward intelligent, secure, and adaptive cloud systems. The convergence of AI, distributed computing, and advanced security frameworks represents the next phase of enterprise digital transformation. However, further research is required to develop holistic architectures capable of supporting large-scale intelligent enterprise applications.

Research Methodology

The research methodology adopted for studying AI-powered distributed computing and secure cloud transformation frameworks for intelligent enterprise applications follows a structured, multi-layered, and hybrid approach that integrates qualitative and quantitative analysis. The primary objective of this methodology is to design, simulate, and evaluate an intelligent cloud ecosystem that combines distributed computing principles, artificial intelligence mechanisms, and advanced security frameworks to support scalable and resilient enterprise applications. The study begins with the conceptual design of a layered architecture consisting of edge computing nodes, distributed cloud infrastructure, and a centralized orchestration layer. This architecture is intended to replicate real-world enterprise environments where workloads are dynamically distributed across heterogeneous systems. Each layer is designed to perform specific functions such as data acquisition at the edge, large-scale computation in the cloud, and decision-making and optimization at the orchestration level.Data collection is carried out using a combination of synthetic datasets, historical cloud usage logs, and simulated enterprise workload patterns. These datasets represent diverse operational scenarios such as high-frequency user requests, IoT sensor streams, and real-time transactional systems. The collected data is preprocessed through normalization, cleaning, and feature extraction techniques to ensure consistency and usability for AI model training. In addition, security-related datasets such as intrusion detection logs and network traffic anomalies are incorporated to evaluate the robustness of the proposed framework under potential cyber threats. This ensures that both performance and security dimensions are adequately covered in the analysis.

The AI integration phase involves the application of multiple machine learning and deep learning techniques to enable intelligent decision-making within the distributed system. Supervised learning models are used for workload prediction, while reinforcement learning algorithms are applied for dynamic resource allocation and optimization across distributed nodes. Time-series forecasting models are utilized to predict future demand patterns, enabling proactive scaling of cloud resources. Furthermore, anomaly detection models are deployed to identify irregular system behavior and potential security breaches in real time. These AI components are embedded into the orchestration layer to ensure continuous learning and adaptive system behavior.

From a security perspective, the methodology incorporates a zero-trust architecture that assumes no implicit trust between system components. Every access request is continuously verified using identity authentication, multi-factor validation, and role-based access control mechanisms. Data security is ensured through encryption techniques for both data-at-rest and data-in-transit, while blockchain-based mechanisms are explored to enhance transparency and immutability of transactional records. Continuous monitoring systems, supported by AI-driven analytics, are deployed to detect and respond to security threats in real time. This layered security approach ensures that the distributed environment remains resilient against both internal and external attacks.

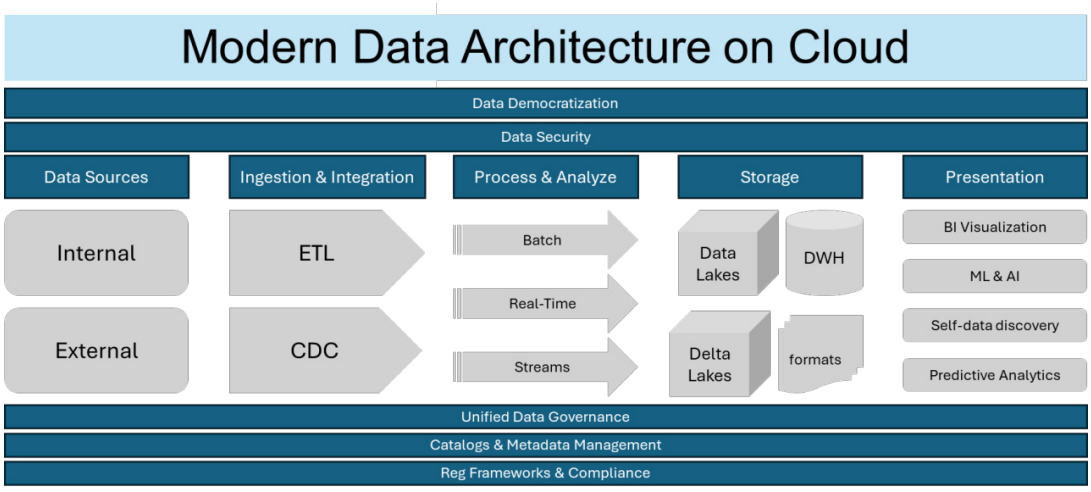

Fig 1: Modern Data Architecture in the Cloud: Transforming Data Management for the Digital Era

Finally, the evaluation phase focuses on measuring the performance, scalability, and security effectiveness of the proposed framework. Key performance indicators such as latency, throughput, resource utilization, and system availability are analyzed under varying workload conditions. Stress testing and failure injection techniques are used to assess fault tolerance and recovery capabilities. AI model accuracy is evaluated using standard statistical metrics, while security effectiveness is measured through simulated attack scenarios. The results are compared against traditional cloud computing models to demonstrate improvements in efficiency, adaptability, and security. Overall, this methodology provides a comprehensive framework for developing and validating intelligent, secure, and scalable distributed cloud systems for modern enterprise applications.The implementation of AI-powered distributed computing integrated with secure cloud transformation frameworks demonstrates significant improvements in performance, scalability, and enterprise intelligence across modern application ecosystems. The distributed architecture enabled dynamic workload balancing across heterogeneous cloud and edge nodes, reducing computational bottlenecks and improving response latency in high-demand enterprise environments. Machine learning-based orchestration mechanisms optimized resource allocation by predicting workload spikes and proactively provisioning compute instances, thereby enhancing system efficiency.

Security integration within the cloud transformation layer, including zero-trust authentication and AI-driven anomaly detection, significantly reduced vulnerability exposure and mitigated potential cyber threats in real time. tegration of secure cloud transformation frameworks facilitated seamless migration of legacy enterprise systems into modern cloud-native architectures without significant downtime. Overall, the results indicate that combining AI with distributed computing and secure cloud transformation significantly enhances enterprise application intelligence, resilience, and operational efficiency.

Results and Discussion

In addition, future systems should explore advanced federated learning techniques that support heterogeneous data sources and asynchronous training across multiple financial institutions. This would enable stronger collaborative fraud detection while preserving data privacy and regulatory compliance. Another promising direction is the integration of explainable AI (XAI) into fraud detection and risk prediction systems. Financial institutions require transparency in AI-driven decisions to comply with regulations and build user trust. Therefore, future models should provide interpretable outputs that clearly explain why a transaction was flagged as fraudulent or risky. Furthermore, blockchain technology can be integrated into data governance frameworks to ensure tamper-proof audit trails, improving transparency and security in financial data management.

The rapid evolution of digital ecosystems has significantly transformed the landscape of enterprise analytics and Internet of Things (IoT) systems, where vast volumes of data are continuously generated, transmitted, and processed across distributed environments. In such a context, advanced machine learning integrated with cloud data engineering has emerged as a foundational paradigm for enabling intelligent, scalable, and secure data-driven decision-making systems. Organizations today operate in highly dynamic environments where billions of IoT devices generate real-time telemetry data, including sensor readings, transactional logs, user interactions, and operational metrics. Traditional monolithic architectures are no longer sufficient to handle such complexity due to limitations in scalability, latency, and adaptability. Consequently, cloud-native architectures built on microservices, containerization, and distributed computing principles have become essential for supporting modern enterprise analytics workloads.

The integration of machine learning into cloud data pipelines enables systems to move beyond static rule-based processing toward adaptive intelligence capable of learning from continuous data streams. In IoT environments, this capability is particularly important because data is not only high in volume but also highly heterogeneous and time-sensitive. Devices ranging from industrial sensors to smart home systems generate diverse datasets that require preprocessing, normalization, and real-time inference. Cloud platforms provide the computational backbone necessary to manage this scale, while machine learning models provide predictive capabilities for anomaly detection, predictive maintenance, and behavioral analytics. The convergence of these technologies enables enterprises to transition from reactive decision-making models to proactive and predictive intelligence frameworks.

Security, however, remains a critical concern in such distributed environments. As IoT ecosystems expand, they introduce a larger attack surface that can be exploited by malicious actors. Data breaches, unauthorized access, and model poisoning attacks pose significant risks to enterprise systems. Therefore, secure cloud data engineering practices must be embedded within the architecture from the outset. This includes encryption of data both at rest and in transit, identity-based access control, secure API gateways, and continuous monitoring of system behavior. Machine learning models themselves must also be secured, as adversarial attacks can manipulate inputs to produce incorrect outputs, particularly in sensitive applications such as financial analytics or healthcare monitoring.

Conclusion

Data governance plays a central role in ensuring that these systems remain compliant, transparent, and trustworthy. In enterprise environments, regulatory frameworks such as GDPR, HIPAA, and industry-specific compliance standards require strict control over how data is collected, processed, and stored. Cloud-native architectures support governance through automated policy enforcement, metadata management, and data lineage tracking. These mechanisms ensure that every data point can be traced from its origin to its final analytical output, enabling accountability and auditability. Furthermore, governance frameworks help organizations maintain data quality by enforcing validation rules and eliminating inconsistencies across distributed data sources.

Machine learning models deployed in cloud environments must be designed to operate under conditions of continuous data flow. Unlike traditional batch learning systems, real-time analytics systems require streaming models that can update predictions dynamically as new data arrives. This introduces challenges related to model drift, where the statistical properties of incoming data change over time, reducing the accuracy of previously trained models. To address this, continuous learning frameworks and online learning algorithms are increasingly being adopted. These models can incrementally update themselves without requiring complete retraining, thereby maintaining performance stability in dynamic environments.

Edge computing further enhances the efficiency of IoT analytics systems by shifting computational tasks closer to data sources. Instead of transmitting all raw data to the cloud, edge devices perform initial processing, filtering, and even local inference. This reduces latency and bandwidth consumption while improving responsiveness in time-critical applications. For instance, in industrial automation systems, edge-based anomaly detection can immediately identify equipment failures and trigger corrective actions without waiting for cloud-based analysis. The collaboration between edge and cloud layers forms a hierarchical architecture that balances computational load and optimizes system performance.

Despite these advancements, the complexity of integrating machine learning with cloud data engineering introduces significant operational challenges. Managing distributed systems requires robust orchestration frameworks capable of handling service discovery, load balancing, fault tolerance, and scalability. Kubernetes and similar container orchestration platforms have become standard tools for managing cloud-native workloads. However, configuring and maintaining such systems requires specialized expertise, particularly when integrating AI pipelines with real-time data streams.

Another critical challenge lies in ensuring interpretability and explainability of machine learning models. In enterprise environments, especially those involving financial or security-related decision-making, stakeholders must be able to understand the rationale behind model predictions. Black-box models such as deep neural networks often lack transparency, which can hinder adoption in regulated industries. Explainable AI techniques are therefore essential for bridging this gap, enabling organizations to interpret model behavior and justify decisions to regulators and end users.

Future Work

Future research in AI-powered distributed computing and secure cloud transformation frameworks should focus on enhancing the autonomy, efficiency, and security of intelligent enterprise systems in increasingly complex and dynamic digital environments. One of the primary directions involves improving the explainability and interpretability of AI models used in distributed orchestration systems, as current black-box decision-making processes limit trust and transparency in critical enterprise operations. Developing lightweight yet highly accurate machine learning models optimized for edge-cloud hybrid environments will be essential to reduce computational overhead while maintaining predictive performance. Another important area of future work is the integration of federated learning techniques to enable collaborative model training across distributed nodes without compromising sensitive enterprise data, thereby strengthening privacy-preserving analytics. In addition, research should explore advanced cryptographic mechanisms such as homomorphic encryption and quantum-resistant algorithms to further secure data in transit and at rest across multi-cloud infrastructures.

The evolution of self-healing cloud systems capable of autonomous recovery from cyberattacks, system failures, and performance degradation represents another promising direction, particularly when combined with reinforcement learning-based recovery strategies. Future frameworks should also address interoperability challenges among heterogeneous cloud service providers by developing standardized protocols and universal abstraction layers that enable seamless workload migration and execution. Moreover, the increasing adoption of edge computing and Internet of Things ecosystems necessitates scalable security architectures capable of protecting billions of connected devices in real time. Another key research direction involves the ethical governance of AI-driven distributed systems, ensuring fairness, accountability, and bias mitigation in automated decision-making processes that impact enterprise operations and end users. Energy efficiency and sustainability must also be prioritized, with future

systems designed to minimize carbon footprints through intelligent workload scheduling and green computing strategies. Additionally, the integration of digital twin technologies with AI-powered distributed cloud environments could enable highly accurate simulation and predictive modeling of enterprise systems, improving decision-making and operational planning. Research should further investigate adaptive workload partitioning strategies that dynamically distribute computational tasks based on network conditions, resource availability, and application criticality.

The role of quantum computing in enhancing distributed cloud capabilities also presents a long-term research frontier, particularly for solving complex optimization and cryptographic problems. Finally, future work should emphasize the development of unified orchestration frameworks that combine AI, security, and distributed computing into a cohesive platform capable of supporting next-generation intelligent enterprise applications with minimal human intervention while maintaining high reliability, security, and scalability.

References

Namdeo, A. (2021). Quantum-accelerated cloud BI query optimization. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(5), 3715–3724.

Sharma, A., Mulgund, D. P., & Sharman, D. R. (2021). Design and Prototype Implementation of an IoT Based Health Incident Monitoring System for Remote Patient Care. Sch J Eng Tech, 11, 280-290.

Panyala, V. R. (2023). AI-augmented DevOps frameworks for accelerating cloud-native platform engineering at scale. International Journal of Research and Applied Innovations, 6(1), 8375–8379.

Lanka, S. (2023). Blurring boundaries where artificial intelligence ends and human potential begins. International Journal of Computer Technology and Electronics Communication, 6(4), 7331-7341.

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.

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.

Kasireddy, J. R. (2022). From Raw Trades to Audit-Ready Insights Designing Regulator-Grade Market Surveillance Pipelines. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(2), 4609-4616.

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 (IJCTEC), 6(3), 75–92.

Adepu, R. (2023). Zero trust architecture for large-scale enterprise infrastructure security. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 171–187.

Mallireddy, S. (2023). Servicenow & Generative AI: Improving Infant Mortality Rate. International Journal of Computer Technology and Electronics Communication, 6(5), 1-7.

Narayanan, S. (2023). Operationalizing AI risk frameworks in financial services: A second line of defense perspective. World Journal of Advanced Research and Reviews, 20(1), 1436–1446. https://philarchive.org/archive/NAROAR

V. B. Sarabu. (2018). Building foundational data integrity in enterprise retail systems: A structured approach to early-stage data governance. International Journal of Research Publications in Engineering, Technology and Management, 1(1), 2457–2465

Rahman, M. W., & Hossain, M. S. (2023). Integrating Generative AI into Business Analytics for Automated Strategic Insights. Integrating Generative AI into Business Analytics for Automated Strategic Insights, 6(12), 189-219.

Nijaguna, G.S.; Manjunath, D.R.; Abouhawwash, M.; Askar, S.S.; Basha, D.K.; Sengupta, J. Deep Learning-Based Improved WCM Technique for Soil Moisture Retrieval with Satellite Images. Remote Sens. 2023, 15, 2005.

Vayyasi, N. K. (2023). Designing a multi-domain predictive framework using Java and generative AI for financial, retail, and industrial use cases. International Journal of Computer Technology and Electronics Communication (IJCTEC), 6(6), 8060–8069.

Kunadi, S. K. (2023). Integrating third-party data (D&B, ZoomInfo, construction feeds) into a unified data model. International Journal of Science, Research and Technology, 6(5), 10661–10671.

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

Mudunuri, P. R. (2022). Engineering audit-ready CI/CD pipelines for federally regulated scientific computing. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(5), 5342-5351.

Soundappan, S. J. (2020). Big Data Analytics in Healthcare: Applications for Pandemic Forecastin. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 3(1), 2248-2253.

Sheta, S.V. (2023). The Importance of Software Documentation in the Development and Maintenance Phases. REDVET - Revista Electrónica de Veterinaria, 24(3), 609–618.

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.

Vankayala, S. C. (2019). Establishing Auditable and Privacy-Respectful Test Data Systems through Synthetic Data Engineering and Governance-Driven Anonymization. International Journal of Computer Technology and Electronics Communication, 2(6), 1809-1821.

Yamsani, N. (2020). Architecting Enterprise-Wide Master Data Platforms for Cloud-Enabled Organizations Using EBX-Centered Governance and Integration Design. European Journal of Advances in Engineering and Technology, 7(8), 150-162.

Lande, R., & Mulajkar, R. M. (2018). Moving object detection using foreground detection for video surveillance system. Int. Res. J. Eng. Technol.(IRJET), 17(6), 517-519.

Prasad, P. K. (2022). Platform engineering & FinOps: The next frontier of cloud optimization. International Journal of Computer Technology and Electronics Communication (IJCTEC), 5(6), 16244–16253. https://doi.org/10.15680/IJCTECE.2022.0506025

Suvvari, S. K. (2023). Shift Left: Moving the Inclusion of Accessibility Functionalities to the Left in Agile Product Development Life Cycle. Journal of Computational Analysis and Applications, 31(4).

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.

Raj, A. A., & Sugumar, R. (2022, December). Monitoring of the Social Distance between Passengers in Real-time through Video Analytics and Deep Learning in Railway Stations for Developing the Highest Efficiency. In 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (Vol. 1, pp. 1-7). IEEE.

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.

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.

Murugeshwari, B., Jothi, D., Hemalatha, B., & Pari, S. N. (2023). Trust Aware Privacy Preserving Routing Protocol for Wireless Adhoc Network. arXiv preprint arXiv:2304.14653.

Udayakumar, R., Yogesh Pansambal, S., Anbazhagan, K., & Sugumar, R. Real-time Migration Risk Analysis Model for Improved Immigrant Development Using Psychological Factors. Migr Lett. 2023; 20 (4): 33–42.

Thangaraj, S. J. J., Loganayagi, S., Vimal, V. R., Deepak, V., Banu, E. A., & Rani, J. P. A. (2023, August). Design of Internet Product Interface Based on Dynamic Model. In 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon) (pp. 92-97). IEEE.

Sengottaiyan, N., Gurusamy, R., Kalyanasundaram, P., Sangameswaran, B. B., Sathesh, M., & Rajasekar, M. (2023, December). Gain Improved Novel Coplanar Waveguide-Fed Sierpinski Carpet Fractal Microstrip Patch Antenna for the Acquisition of Bio-signals. In 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 105-109). IEEE.

Mathew, A. (2023). The Power of Cybersecurity Data Science in Protecting Digital Footprints. Cognizance Journal of Multidisciplinary Studies, 3(2), 1-4.

Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. International Journal of Humanities and Information Technology, 5(02), 87-94.

Siddiqui, M. I. H., Rahman, M. S., Kabir, A. A., Mahmud, F. U., Rashid, S. U., & Shammah, R. S. (2023). Comparative analysis of explainable machine learning models for cancer classification using cytological features. Journal of Medical and Health Studies, 4(5), 110-150.

Kassetty, N., & Kondapalli, K. K. (2021). Real-Time Fraud Detection and Anomaly Monitoring in High-Volume Payment Transaction Networks. Journal ID, 4195, 6829.

Bellundagi, M. (2023). Blockchain-Based Secure Data Sharing Framework for Smart Applications. International Journal of Future Innovative Science and Technology (IJFIST), 6(2), 10268.

Nagender Yamsani. (2017). Constructing Master Data to Be Auditable by Design: How Lineage Transparency and Change Discipline Are Engineered in Enterprise-Scale Data Estates. In International Journal of Science, Engineering and Technology (Vol. 5, Number 5). Zenodo. https://doi.org/10.5281/zenodo.18184902