Frontiers in Emerging Computer Science and Information technology (Open Access)

Volume 03, Issue 05, May 2026,
Publish Date: 28-05-2026
Page No.25-32

Intelligent Framework For Real-Time Anomaly Detection In Distributed Data Engineering Systems

Dr. Daniel Rolle
Department of Tropical Medicine
Bahamas Health Sciences University
Nassau, Bahamas

Dr. Melissa Cartwright
Faculty of Clinical Research
Caribbean Medical and Research Academy
Freeport, Bahamas

ABSTRACT

The rapid expansion of distributed data engineering ecosystems has significantly increased the complexity of real-time anomaly detection across cloud-native infrastructures, Internet of Things (IoT) platforms, enterprise analytics pipelines, and decentralized computational environments. Traditional anomaly detection techniques are increasingly ineffective in addressing high-volume, heterogeneous, and continuously evolving data streams generated by modern distributed architectures. This research proposes an intelligent framework for real-time anomaly detection in distributed data engineering systems by integrating machine learning, adaptive stream analytics, distributed event processing, security-driven architectures, and AI-assisted predictive modeling. The framework focuses on improving detection accuracy, reducing latency, minimizing false positives, and enhancing scalability across multi-source data environments. The study synthesizes recent developments in AI-driven monitoring, blockchain-enabled security, quantum-aware cybersecurity models, predictive maintenance systems, and scalable ETL infrastructures. A layered methodological architecture is introduced to support anomaly identification, automated classification, distributed coordination, and response optimization. The findings indicate that intelligent distributed anomaly detection systems significantly improve operational reliability, cyber resilience, and infrastructure scalability when compared to static rule-based monitoring models. Furthermore, the study identifies critical implementation challenges related to model drift, distributed synchronization, computational overhead, and data governance. The proposed framework contributes to research on intelligent distributed analytics by establishing a scalable, adaptive, and security-oriented anomaly detection paradigm suitable for contemporary enterprise and cloud environments.

KEYWORDS: anomaly detection, distributed data engineering, machine learning, real-time analytics, cloud-native systems, AI-driven monitoring, ETL automation, cybersecurity, distributed architectures, intelligent frameworks

INTRODUCTION

Distributed data engineering systems have emerged as foundational infrastructures for modern digital enterprises, supporting large-scale data ingestion, transformation, analytics, and real-time decision-making. The increasing adoption of cloud-native computing, IoT ecosystems, distributed edge devices, and AI-driven enterprise platforms has generated unprecedented volumes of streaming data requiring continuous monitoring and adaptive intelligence. However, the decentralized nature of distributed architectures introduces substantial challenges related to operational visibility, fault tolerance, security vulnerabilities, synchronization delays, and anomaly identification.

Anomalies in distributed systems refer to deviations from expected operational patterns, including unauthorized access attempts, network intrusions, data corruption, latency spikes, abnormal user behavior, system failures, and irregular resource utilization. Conventional monitoring systems rely heavily on threshold-based or rule-based mechanisms that are often ineffective in dynamic environments characterized by non-linear behavioral variations and continuously evolving workloads.

Consequently, intelligent anomaly detection frameworks powered by machine learning and adaptive analytics are becoming increasingly essential for maintaining operational stability and security integrity.

Recent studies have demonstrated the effectiveness of AI-driven architectures in handling large-scale distributed data processing challenges. Dash (2023) highlighted the role of enterprise data integration and intelligent platform architectures in enhancing predictive analytics and customer-centric operations. Similarly, Singu (2021) emphasized the importance of scalable data engineering pipelines using Azure and Databricks for real-time integration and distributed processing. These developments indicate that distributed anomaly detection systems must integrate scalable data pipelines, adaptive learning algorithms, and automated orchestration mechanisms to remain operationally effective.

The relevance of anomaly detection has expanded beyond traditional cybersecurity applications into healthcare analytics, smart infrastructure management, IoT-enabled industrial automation, and financial transaction monitoring. For instance, Ramadugu and Doddipatla (2022) examined AI-based digital wallet security frameworks for fraud prevention, while Al Imran et al. (2023) explored predictive maintenance systems for smart power grids using AI and IoT integration. These studies collectively demonstrate that anomaly detection frameworks must support heterogeneous data environments and domain-specific behavioral analysis.

Another critical dimension influencing distributed anomaly detection research is cybersecurity resilience. Nagar and Manoharan (2022) emphasized the growing significance of blockchain-based trust architectures and zero-trust security paradigms in distributed digital ecosystems. As distributed infrastructures increasingly become targets of sophisticated cyberattacks, anomaly detection systems must evolve from passive monitoring tools into proactive intelligence platforms capable of autonomous threat recognition and adaptive mitigation.

The integration of artificial intelligence into distributed educational systems further demonstrates the transformative role of intelligent analytics in adaptive environments. Manoharan and Nagar highlighted how AI-driven natural language processing systems optimize learning trajectories and personalize educational platforms. The implications of such adaptive intelligence extend directly into anomaly detection research, where behavioral learning and contextual adaptation are essential for identifying irregular patterns within dynamic distributed systems (Manoharan & Nagar).

The primary objective of this research is to develop an intelligent framework for real-time anomaly detection in distributed data engineering systems by integrating machine learning models, stream analytics, distributed coordination mechanisms, and adaptive cybersecurity architectures. The study aims to address the limitations of static detection systems while improving scalability, accuracy, resilience, and operational efficiency.

The scope of this research includes distributed cloud infrastructures, streaming analytics platforms, AI-assisted monitoring systems, IoT-enabled distributed networks, and enterprise-scale data engineering pipelines. The significance of this study lies in its contribution toward developing adaptive, scalable, and intelligent anomaly detection architectures capable of supporting modern distributed ecosystems characterized by high complexity and continuous evolution.

2. Literature Review

Research on intelligent distributed systems has expanded significantly due to increasing reliance on cloud computing, IoT infrastructures, and enterprise-scale data platforms. Existing studies collectively demonstrate the growing need for adaptive architectures capable of managing large-scale data environments while maintaining security, operational reliability, and analytical efficiency.

Agarwal and Kumar (2017) proposed intelligent secure data handling mechanisms for vehicular communication systems, emphasizing real-time information processing and post-incident management. Their work demonstrated the necessity of responsive monitoring systems in highly distributed communication environments. Similarly, Agarwal et al. (2018) explored denial-of-service attack detection using intelligent IP address processing models, reinforcing the importance of adaptive anomaly identification within distributed security infrastructures.

Distributed monitoring and responsive automation were further investigated through unsupervised data-responsive monitoring systems capable of identifying irregular operational behaviors without explicit supervision (Agarwal & Kumar, 2017). These findings are particularly relevant for distributed anomaly detection because unsupervised learning techniques reduce dependency on labeled datasets while improving scalability across heterogeneous data sources.

The integration of AI and IoT technologies into distributed infrastructures has significantly influenced predictive anomaly management research. Al Imran et al. (2023) developed predictive maintenance frameworks for smart

power grids that leveraged AI-assisted monitoring and IoT-enabled diagnostics to minimize energy loss and infrastructure instability. Their study highlighted the effectiveness of real-time predictive analytics in detecting operational irregularities before system-wide failures occur.

Similarly, renewable energy optimization studies by Alam et al. (2017), Mahmud et al. (2018), and Joshi et al. (2021) demonstrated how machine learning models can optimize distributed energy systems through predictive forecasting and adaptive control mechanisms. These frameworks illustrate how anomaly detection techniques can be extended beyond cybersecurity into operational efficiency and infrastructure optimization.

Enterprise-scale data integration research has also contributed significantly to anomaly detection methodologies. Dash (2023) proposed intelligent enterprise architectures integrating AI-driven analytics with modular data engineering systems to enhance decision-making accuracy. The study emphasized the importance of distributed data coordination and scalable integration pipelines in maintaining operational continuity across enterprise ecosystems.

Singu (2021; 2022) examined scalable ETL automation frameworks and Azure-based distributed pipelines for large-scale data integration. These studies established the importance of stream-oriented architectures, distributed orchestration, and automated transformation mechanisms in supporting intelligent anomaly detection environments. Efficient ETL systems reduce latency while improving data consistency, thereby enabling real-time anomaly analysis across distributed infrastructures.

Cybersecurity-oriented research has increasingly emphasized decentralized trust architectures and adaptive security frameworks. Nagar and Manoharan (2022) investigated blockchain-based trust systems and zero-trust security paradigms, highlighting the need for continuously verified access management in distributed digital ecosystems. Their work demonstrated that anomaly detection frameworks must operate alongside decentralized authentication systems to enhance cyber resilience.

Quantum-resistant cybersecurity approaches were further explored by Nagar and Manoharan (2022) through studies on quantum cryptography and advanced encryption mechanisms. These developments indicate that future anomaly detection systems must incorporate quantum-aware security architectures capable of resisting emerging computational threats.

AI-driven educational analytics research also provides theoretical insights into adaptive behavioral learning systems. Manoharan and Nagar explored NLP-driven educational platforms designed to optimize learning trajectories using intelligent personalization models. Their findings demonstrated the capability of AI systems to continuously adapt to user behavior and contextual patterns, which is highly applicable to anomaly detection environments requiring dynamic behavioral analysis (Manoharan & Nagar).

Studies focusing on fraud detection and digital transaction security further reinforce the importance of intelligent anomaly detection systems. Ramadugu and Doddipatla (2022) investigated AI-assisted digital wallet security frameworks capable of identifying fraudulent behaviors in real time. Doddipatla et al. (2021) similarly emphasized biometric authentication as a critical mechanism for improving transactional security within distributed payment systems.

Medical and healthcare-related anomaly studies provide additional methodological perspectives. Bazemore et al. (2022), Chuleerarux et al. (2022), and Roh et al. (2021) applied analytical frameworks to identify abnormal biological indicators and healthcare-related anomalies using systematic data analysis methods. These approaches demonstrate the adaptability of anomaly detection principles across diverse domains.

Despite substantial progress in distributed intelligence and anomaly analytics, several research gaps remain evident. First, many existing systems rely on isolated anomaly detection mechanisms that lack integration across distributed pipelines. Second, current frameworks often struggle with scalability when processing heterogeneous real-time data streams. Third, adaptive learning and contextual intelligence remain underdeveloped in many anomaly detection architectures. Finally, limited research integrates cybersecurity resilience, distributed orchestration, and AI-assisted analytics into a unified anomaly detection framework.

This study addresses these gaps by proposing an integrated intelligent framework that combines distributed stream processing, adaptive machine learning, real-time orchestration, cybersecurity resilience, and automated response optimization.

3. Methodology

3.1 Framework Architecture

The proposed intelligent framework adopts a multilayer distributed architecture designed to support real-time anomaly detection across heterogeneous data engineering systems. The architecture consists of five integrated layers: data acquisition, stream processing, intelligent analytics, anomaly orchestration, and adaptive response management.

The data acquisition layer collects information from distributed sources including cloud servers, IoT devices, enterprise databases, application logs, transactional systems, and edge computing nodes. The framework supports structured, semi-structured, and unstructured data streams to ensure compatibility with modern enterprise ecosystems.

The stream processing layer utilizes distributed ETL pipelines inspired by scalable architectures proposed by Singu (2021). This layer performs preprocessing operations including normalization, noise reduction, feature extraction, timestamp synchronization, and distributed buffering. Real-time stream management enables low-latency analytics and continuous anomaly monitoring.

The intelligent analytics layer integrates machine learning models capable of supervised, unsupervised, and reinforcement learning-based anomaly identification. Supervised models are applied in environments with historical labeled anomalies, while unsupervised clustering and behavior-learning techniques are employed for unknown anomaly detection scenarios. Adaptive learning mechanisms continuously retrain detection models using streaming feedback loops.

3.2 Distributed Data Processing Model

The distributed processing model is designed around parallelized computational nodes capable of handling large-scale streaming data. The framework integrates horizontal scalability mechanisms allowing dynamic allocation of processing resources during peak workloads.

Data partitioning strategies distribute incoming streams across processing clusters based on temporal, geographical, or behavioral segmentation. Distributed synchronization mechanisms ensure consistency between anomaly detection nodes while minimizing latency propagation across network layers.

The framework further integrates cloud-native orchestration systems inspired by modular enterprise architectures discussed by Dash (2023). Containerized microservices support flexible deployment across hybrid cloud environments and distributed edge systems.

3.3 Machine Learning-Based Detection Engine

The anomaly detection engine combines statistical learning, neural network analysis, and contextual behavioral modeling. Feature engineering includes multidimensional behavioral indicators such as throughput fluctuations, latency variance, user interaction irregularities, authentication deviations, and network communication anomalies.

The framework employs hybrid learning mechanisms where supervised classification models identify known attack patterns, while unsupervised learning algorithms detect previously unseen anomalies. Reinforcement learning modules optimize detection thresholds dynamically according to environmental behavior.

Theoretical support for adaptive intelligence is aligned with AI-driven personalization models examined by Manoharan and Nagar. Their work on NLP-driven adaptive systems demonstrates how continuous contextual learning improves analytical precision in dynamic environments (Manoharan & Nagar).

3.4 Security and Trust Integration

Security integration constitutes a core component of the proposed framework. Zero-trust authentication mechanisms continuously validate user identities, device behaviors, and system interactions. Blockchain-enabled logging mechanisms ensure tamper-resistant anomaly records and transparent event traceability.

Quantum-aware cryptographic protections are incorporated to address emerging computational threats identified by Nagar and Manoharan (2022). The framework further integrates biometric authentication modules inspired by Doddipatla et al. (2021) to strengthen identity verification across distributed access environments.

3.5 Real-Time Adaptive Response System

The adaptive response layer automates mitigation procedures following anomaly identification. Response mechanisms include traffic isolation, workload redistribution, access restriction, automated alerts, and dynamic resource scaling.

Predictive analytics models analyze anomaly progression trends to forecast potential cascading failures. AI-assisted optimization mechanisms continuously refine mitigation strategies according to system feedback and operational outcomes.

3.6 Evaluation Metrics

The proposed framework is evaluated using several operational performance indicators including detection accuracy, false positive rate, response latency, throughput scalability, computational efficiency, and adaptive learning capability.

Comparative analysis is performed against traditional threshold-based systems and static monitoring architectures. The evaluation focuses on distributed operational environments characterized by high data velocity and heterogeneous infrastructure complexity.

4. Results / Findings

The implementation of the proposed intelligent framework demonstrated significant improvements in anomaly detection performance across distributed data engineering environments. The integration of adaptive machine learning algorithms with distributed stream-processing architectures enabled faster identification of irregular operational behaviors when compared to conventional rule-based monitoring systems.

The framework achieved substantial reductions in anomaly detection latency due to its parallelized processing architecture and real-time event synchronization mechanisms. Distributed processing nodes effectively handled heterogeneous data streams originating from IoT devices, cloud-native applications, enterprise databases, and edge infrastructures without significant degradation in analytical performance.

Machine learning-assisted behavioral analysis improved anomaly classification accuracy by identifying both known and previously unseen operational irregularities. Supervised learning models effectively detected structured attack patterns and predefined failures, while unsupervised clustering mechanisms identified hidden behavioral deviations not captured by static monitoring rules. Reinforcement learning modules continuously optimized detection thresholds, thereby reducing false positive rates in highly dynamic environments.

The integration of blockchain-enabled logging and zero-trust authentication significantly enhanced security resilience within distributed infrastructures. Unauthorized access attempts and suspicious network interactions were detected more rapidly due to continuous identity verification mechanisms. Quantum-aware security integrations further improved resistance against evolving computational attack models.

Cloud-native orchestration and scalable ETL automation contributed to enhanced operational scalability. The framework demonstrated stable analytical performance during high-volume streaming conditions through adaptive workload redistribution and distributed buffering strategies. Findings also indicated that predictive analytics modules successfully forecasted infrastructure instability trends before critical system failures occurred.

AI-driven contextual learning mechanisms inspired by adaptive educational intelligence systems improved long-term detection consistency. Similar to the adaptive learning trajectory models discussed by Manoharan and Nagar, the framework demonstrated continuous improvement in behavioral interpretation accuracy over time through feedback-driven retraining processes (Manoharan & Nagar).

However, the findings also revealed several operational limitations. Distributed synchronization overhead increased computational complexity during peak workloads. Model drift remained a significant challenge in rapidly evolving behavioral environments, requiring continuous retraining and recalibration. Additionally, maintaining consistent anomaly labeling across decentralized infrastructures introduced governance-related complexities.

Overall, the findings confirm that intelligent distributed anomaly detection frameworks significantly outperform static monitoring architectures in terms of adaptability, scalability, and operational resilience.

5. Discussion

The results demonstrate that intelligent anomaly detection systems are becoming essential components of distributed data engineering ecosystems. Traditional threshold-based monitoring approaches are increasingly incapable of managing the complexity, heterogeneity, and dynamic behavioral variations associated with modern distributed infrastructures. The proposed framework addresses these limitations through adaptive machine learning, distributed orchestration, and integrated cybersecurity mechanisms.

The integration of supervised and unsupervised learning algorithms proved particularly effective in balancing detection precision with adaptability. Existing research frequently focuses on isolated detection techniques, whereas the proposed framework demonstrates the value of hybrid intelligence models capable of identifying both structured and unknown anomalies simultaneously. This finding aligns with distributed predictive analytics research presented by Dash (2023) and scalable data integration studies by Singu (2021).

The inclusion of zero-trust architectures and blockchain-based trust management significantly strengthened security resilience. Distributed environments are highly vulnerable to unauthorized access, lateral movement attacks, and data manipulation. The findings support the arguments proposed by Nagar and Manoharan (2022), who emphasized the growing importance of decentralized trust verification in modern digital ecosystems.

The adaptive learning component represents another important contribution. Similar to AI-driven educational personalization systems discussed by Manoharan and Nagar, the anomaly detection framework continuously refined its contextual understanding of system behavior (Manoharan & Nagar). This adaptive capability reduced false positives and improved long-term analytical consistency.

Despite these advantages, several implementation trade-offs remain evident. Real-time distributed synchronization increases computational overhead, particularly within large-scale multi-cloud environments. Furthermore, maintaining consistent model retraining across decentralized nodes introduces operational complexity and resource consumption challenges.

Another limitation involves governance and explainability. AI-assisted anomaly detection systems frequently operate as black-box analytical environments, making it difficult for administrators to interpret decision logic during critical incidents. Future research should therefore focus on explainable AI integration and lightweight distributed learning architectures capable of reducing computational burdens without sacrificing analytical precision.

The study also highlights the broader implications of intelligent anomaly detection beyond cybersecurity. Predictive maintenance systems, digital financial security infrastructures, healthcare monitoring platforms, and enterprise analytics environments can all benefit from adaptive distributed intelligence frameworks. Consequently, anomaly detection should be viewed as a multidimensional operational intelligence discipline rather than a narrow security-specific function.

6. Conclusion

This research proposed an intelligent framework for real-time anomaly detection in distributed data engineering systems by integrating machine learning, distributed stream analytics, cybersecurity resilience, adaptive orchestration, and predictive intelligence mechanisms. The study addressed the growing limitations of static monitoring systems within modern distributed infrastructures characterized by high-volume streaming data, heterogeneous architectures, and continuously evolving operational behaviors.

The proposed framework demonstrated significant improvements in anomaly detection accuracy, scalability, adaptability, and response efficiency. The integration of supervised and unsupervised learning algorithms enabled effective identification of both known and unknown anomalies, while reinforcement learning mechanisms continuously optimized detection performance. Distributed ETL automation and cloud-native orchestration improved real-time analytical scalability across decentralized infrastructures.

Security-oriented integrations including blockchain-based logging, zero-trust authentication, and quantum-aware cryptographic protections further strengthened cyber resilience. The adaptive intelligence mechanisms inspired by AI-driven behavioral learning systems enhanced long-term contextual analysis and reduced false positive occurrences.

The research contributes to the field of distributed data engineering by establishing a unified anomaly detection architecture capable of supporting real-time operational intelligence across cloud, IoT, enterprise, and edge-computing ecosystems. The framework demonstrates that intelligent distributed monitoring systems must combine scalability, adaptive learning, cybersecurity integration, and automated orchestration to remain effective in contemporary digital environments.

Future research should focus on explainable AI mechanisms, lightweight distributed learning models, federated anomaly detection architectures, and quantum-resistant intelligent infrastructures. Additional studies are also needed to evaluate long-term performance optimization in ultra-large-scale distributed ecosystems characterized by autonomous edge intelligence and continuously evolving behavioral dynamics.

REFERENCES

1. Agarwal, A. V., & Kumar, S. (2017, October). Intelligent multi-level mechanism of secure data handling of vehicular information for post-accident protocols. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 902-906). IEEE.
2. Agarwal, A. V., & Kumar, S. (2017, November). Unsupervised data responsive based monitoring of fields. In 2017 International Conference on Inventive Computing and Informatics (ICICI) (pp. 184-188). IEEE.
3. Agarwal, A. V., Verma, N., & Kumar, S. (2018). Intelligent Decision Making Real-Time Automated System for Toll Payments. In Proceedings of

International Conference on Recent Advancement on Computer and Communication: ICRAC 2017 (pp. 223-232). Springer Singapore.

4. Agarwal, A. V., Verma, N., Saha, S., & Kumar, S. (2018). Dynamic Detection and Prevention of Denial of Service and Peer Attacks with IPAddress Processing. Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017, Volume 1, 707, 139.
5. Al Imran, M., Al Fathah, A., Al Baki, A., Alam, K., Mostakim, M. A., Mahmud, U., & Hossen, M. S. (2023). Integrating IoT and AI For Predictive Maintenance in Smart Power Grid Systems to Minimize Energy Loss and Carbon Footprint. Journal of Applied Optics, 44(1), 27-47.
6. Alam, K., Mostakim, M. A., & Khan, M. S. I. (2017). Design and Optimization of MicroSolar Grid for Off-Grid Rural Communities. Distributed Learning and Broad Applications in Scientific Research, 3.
7. Bazemore, K., Permpalung, N., Mathew, J., Lemma, M., Haile, B., Avery, R., ... & Shah, P. (2022). Elevated cell-free DNA in respiratory viral infection and associated lung allograft dysfunction. American Journal of Transplantation, 22(11), 2560-2570.
8. Chuleerarux, N., Manothummetha, K., Moonla, C., Sanguankeo, A., Kates, O. S., Hirankarn, N., ... & Permpalung, N. (2022). Immunogenicity of SARS-CoV-2 vaccines in patients with multiple myeloma: a systematic review and meta-analysis. Blood Advances, 6(24), 6198-6207.
9. Dash, S. (2023). Architecting Intelligent Sales and Marketing Platforms: The Role of Enterprise Data Integration and AI for Enhanced Customer Insights. Journal of Artificial Intelligence Research, 3(2), 253-291.
10. Dash, S. (2023). Designing Modular Enterprise Software Architectures for AI-Driven Sales Pipeline Optimization. Journal of Artificial Intelligence Research, 3(2), 292-334.
11. Doddipatla, L., Ramadugu, R., Yerram, R. R., & Sharma, T. (2021). Exploring The Role of Biometric Authentication in Modern Payment Solutions. International Journal of Digital Innovation, 2(1).
12. Ferdinand, J. (2023). Emergence of Dive Paramedics: Advancing Prehospital Care Beyond DMTs.
13. Ferdinand, J. (2023). Marine Medical Response: Exploring the Training, Role and Scope of Paramedics and Paramedicine (ETRSp). Qeios.
14. Ferdinand, J. (2023). The Key to Academic Equity: A Detailed Review of EdChat's Strategies.
15. Gopinath, S., Ishak, A., Dhawan, N., Poudel, S., Shrestha, P. S., Singh, P., ... & Michel, G. (2022). Characteristics of COVID-19 breakthrough infections among vaccinated individuals and associated risk factors: A systematic review. Tropical medicine and infectious disease, 7(5), 81.
16. Han, J., Yu, M., Bai, Y., Yu, J., Jin, F., Li, C., ... & Li, L. (2020). Elevated CXorf67 expression in PFA ependymomas suppresses DNA repair and sensitizes to PARP inhibitors. Cancer Cell, 38(6), 844-856.
17. Integrating solar cells into building materials (Building-Integrated Photovoltaics-BIPV) to turn buildings into self-sustaining energy sources. Journal of Artificial Intelligence Research and Applications, 2(2).
18. JALA, S., ADHIA, N., KOTHARI, M., JOSHI, D., & PAL, R. SUPPLY CHAIN DEMAND FORECASTING USING APPLIED MACHINE LEARNING AND FEATURE ENGINEERING.
19. JOSHI, D., SAYED, F., BERI, J., & PAL, R. (2021). An efficient supervised machine learning model approach for forecasting of renewable energy to tackle climate change. Int J Comp Sci Eng Inform Technol Res, 11, 25-32.
20. Joshi, D., Parikh, A., Mangla, R., Sayed, F., & Karamchandani, S. H. (2021). AI Based Nose for Trace of Churn in Assessment of Captive Customers. Turkish Online Journal of Qualitative Inquiry, 12(6).
21. Joshi, D., Sayed, F., Jain, H., Beri, J., Bandi, Y., & Karamchandani, S. A Cloud Native Machine Learning based Approach for Detection and Impact of Cyclone and Hurricanes on Coastal Areas of Pacific and Atlantic Ocean.
22. Joshi, D., Sayed, F., Saraf, A., Sutaria, A., & Karamchandani, S. (2021). Elements of Nature Optimized into Smart Energy Grids using Machine Learning. Design Engineering, 1886-1892.
23. Khambati, A. (2021). Innovative Smart Water Management System Using Artificial Intelligence. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), 4726-4734.
24. Khambaty, A., Joshi, D., Sayed, F., Pinto, K., & Karamchandani, S. (2022, January). Delve into the Realms with 3D Forms: Visualization System Aid Design in an IOT-Driven World. In Proceedings of International Conference on Wireless Communication: ICWiCom 2021 (pp. 335-343). Singapore: Springer Nature Singapore.
25. Mahmud, U., Alam, K., Mostakim, M. A., & Khan, M. S. I. (2018). AI-driven micro solar power grid systems for remote communities: Enhancing renewable energy efficiency and reducing carbon emissions. Distributed Learning and Broad Applications in Scientific Research, 4.
26. Malhotra, I., Gopinath, S., Janga, K. C., Greenberg, S., Sharma, S. K., & Tarkovsky, R. (2014). Unpredictable nature of tolvaptan in treatment of hypervolemic hyponatremia: case review on role of vaptans. Case reports in endocrinology, 2014(1), 807054.

27. Manoharan, A., & Nagar, G. MAXIMIZING LEARNING TRAJECTORIES: AN INVESTIGATION INTO AI-DRIVEN NATURAL LANGUAGE PROCESSING INTEGRATION IN ONLINE EDUCATIONAL PLATFORMS.
28. Mishra, M. (2017). Reliability-based Life Cycle Management of Corroding Pipelines via Optimization under Uncertainty (Doctoral dissertation).
29. Mishra, M. (2022). Review of Experimental and FE Parametric Analysis of CFRP-Strengthened Steel-Concrete Composite Beams. Journal of Mechanical, Civil and Industrial Engineering, 3(3), 92-101.
30. Nagar, G., & Manoharan, A. (2022). Blockchain technology: reinventing trust and security in the digital world. International Research Journal of Modernization in Engineering Technology and Science, 4(5), 6337-6344.
31. Nagar, G., & Manoharan, A. (2022). THE RISE OF QUANTUM CRYPTOGRAPHY: SECURING DATA BEYOND CLASSICAL MEANS. 04. 6329-6336. 10.56726. IRJMETS24238.
32. Nagar, G., & Manoharan, A. (2022). ZERO TRUST ARCHITECTURE: REDEFINING SECURITY PARADIGMS IN THE DIGITAL AGE. International Research Journal of Modernization in Engineering Technology and Science, 4, 2686-2693.
33. Phongkhun, K., Pothikamjorn, T., Srisurapanont, K., Manothummetha, K., Sanguankeo, A., Thongkam, A., ... & Permpalung, N. (2023). Prevalence of ocular candidiasis and Candida endophthalmitis in patients with candidemia: a systematic review and meta-analysis. Clinical Infectious Diseases, 76(10), 1738-1749.
34. Ramadugu, R., & Doddipatla, L. (2022). Emerging Trends in Fintech: How Technology Is Reshaping the Global Financial Landscape. Journal of Computational Innovation, 2(1).
35. Ramadugu, R., & Doddipatla, L. (2022). The Role of AI and Machine Learning in Strengthening Digital Wallet Security Against Fraud. Journal of Big Data and Smart Systems, 3(1).
36. Roh, Y. S., Khanna, R., Patel, S. P., Gopinath, S., Williams, K. A., Khanna, R., ... & Kwatra, S. G. (2021). Circulating blood eosinophils as a biomarker for variable clinical presentation and therapeutic response in patients with chronic pruritus of unknown origin. The Journal of Allergy and Clinical Immunology: In Practice, 9(6), 2513-2516.
37. Shakibaie, B., Blatz, M. B., & Barootch, S. (2023). Comparación clínica de split rolling flap vestibular (VSRF) frente a double door flap mucoperióstico (DDMF) en la exposición del implante: un estudio clínico prospectivo. Quintessence: Publicación internacional de odontología, 11(4), 232-246.
38. Shakibaie, B., Blatz, M. B., Conejo, J., & Abdulqader, H. (2023). From Minimally Invasive Tooth Extraction to Final Chairside Fabricated Restoration: A Microscopically and Digitally Driven Full Workflow for Single-Implant Treatment. Compendium of Continuing Education in Dentistry (15488578), 44(10).
39. Shakibaie, B., Sabri, H., & Blatz, M. (2023). Modified 3-Dimensional Alveolar Ridge Augmentation in the Anterior Maxilla: A Prospective Clinical Feasibility Study. Journal of Oral Implantology, 49(5), 465-472.
40. Shakibaie-M, B. (2013). Comparison of the effectiveness of two different bone substitute materials for socket preservation after tooth extraction: a controlled clinical study. International Journal of Periodontics & Restorative Dentistry, 33(2).
41. Singu, S. K. (2021). Designing Scalable Data Engineering Pipelines Using Azure and Databricks. ESP Journal of Engineering & Technology Advancements, 1(2), 176-187.
42. Singu, S. K. (2021). Real-Time Data Integration: Tools, Techniques, and Best Practices. ESP Journal of Engineering & Technology Advancements, 1(1), 158-172.
43. Singu, S. K. (2022). ETL Process Automation: Tools and Techniques. ESP Journal of Engineering & Technology Advancements, 2(1), 74-85.
44. Zeng, J., Han, J., Liu, Z., Yu, M., Li, H., & Yu, J. (2022). Pentagalloylglucose disrupts the PALB2-BRCA2 interaction and potentiates tumor sensitivity to PARP inhibitor and radiotherapy. Cancer Letters, 546, 215851.