International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

Integrating Fiber Broadband with SAP and AI for Secure Cloud-Based Digital Advertising and Financial Systems

Lars Hendrik Jansen

Senior IT Manager, Netherland

ABSTRACT: The rapid expansion of fiber broadband networks has enabled high-performance cloud infrastructures that support data-intensive enterprise applications. At the same time, organizations increasingly rely on SAP platforms and artificial intelligence to manage digital advertising and financial operations. Despite these advancements, ensuring data security, system integrity, and intelligent decision-making across cloud environments remains a significant challenge. This paper presents an integrated framework that combines fiber broadband connectivity with SAP systems and AI-driven analytics to support secure, cloud-based digital advertising and financial enterprise systems. The proposed approach leverages high-bandwidth network capabilities to enable real-time data processing, predictive intelligence, and continuous security monitoring. AI models analyze transactional, behavioral, and operational data to detect anomalies and optimize business performance. The framework incorporates robust security controls to protect sensitive financial and advertising data while maintaining scalability and regulatory compliance. Experimental evaluation demonstrates improved system responsiveness, enhanced threat detection accuracy, and more informed business insights compared to conventional cloud architectures. The findings highlight the value of integrating broadband networks, SAP platforms, and AI technologies for building secure and intelligent enterprise cloud solutions.

KEYWORDS: Fiber broadband networks, SAP cloud systems, Artificial intelligence, Digital advertising analytics, Financial enterprise systems, Cloud security, Predictive intelligence

I. INTRODUCTION

The modern enterprise operates in an era defined by digital connectivity, data proliferation, and the need for resilient, intelligent operations. Digital transformation has elevated **network infrastructure** from a supporting utility to a strategic asset. Businesses now depend on robust, low-latency, and high-capacity networks to power cloud applications, mobile workforces, Internet of Things (IoT) deployments, and real-time analytics platforms. Among emerging network technologies, **fiber broadband** and **5G wireless networks** are at the forefront of enabling the next generation of enterprise applications. Together, they provide enhanced bandwidth, reliability, and coverage, supporting a wide range of mission-critical functions across industries including manufacturing, healthcare, logistics, and finance.

Meanwhile, enterprise systems such as **SAP** (Systems, Applications, and Products in Data Processing) have become foundational for orchestrating complex business processes. SAP platforms manage critical functions including financials, procurement, supply chain, and human resources. However, traditional enterprise solutions often operate in siloed environments where connectivity constraints, limited real-time visibility, and static analytics hinder strategic agility. To overcome these limitations, organizations are seeking to integrate their core enterprise systems with advanced network capabilities and intelligent computational frameworks.

The convergence of high-speed fiber broadband and 5G networks presents an opportunity to achieve a new level of enterprise responsiveness. Fiber broadband contributes unparalleled data throughput suitable for data-intensive workloads, while 5G offers ultra-low latency and broad wireless coverage. Together, they enable seamless connectivity from central data centers to mobile and edge environments, supporting distributed SAP applications and data streaming in ways that were previously unattainable. However, raw connectivity alone is not sufficient. The true value arises from combining networking with intelligent analytics and security capabilities — especially those enabled by **artificial intelligence (AI)**.

AI technologies, including machine learning, deep learning, and predictive analytics, have matured to the point where they can provide real-time operational intelligence at scale. Within the context of SAP systems, AI can enhance

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

forecasting, automate business process insights, detect anomalies indicative of security threats or performance degradation, and support decision makers with contextualized recommendations. When AI operates on data flows that are continuously supported by high-speed networks such as fiber and 5G, enterprises can realize near real-time intelligence that drives competitive advantage.

Despite the theoretical promise of integrating fiber, 5G, SAP, and AI, practical challenges remain. Connectivity heterogeneity, data governance concerns, security risks introduced by expanded network surfaces, and complexity in synchronizing distributed systems pose barriers to adoption. Organizations must design architectures that not only deliver performance but also ensure **security**, **scalability**, and **manageability**. A secure enterprise framework must consider identity and access management, encrypted data flows, intrusion detection, threat response automation, and compliance with regulatory mandates such as GDPR, HIPAA, and industry standards.

This research proposes a unified architectural framework that seamlessly integrates fiber broadband and 5G connectivity with SAP systems augmented by AI intelligence for secure, intelligent enterprise operations. The framework is designed to support hybrid cloud environments including public, private, and edge deployments. It emphasizes an adaptive security posture, real-time analytics, and network-aware process orchestration. It also considers operational resilience by supporting dynamic workload placement and predictive network and application performance management.

The primary contributions of this work include: (1) a conceptual architecture that maps fiber and 5G network capabilities to SAP application and data layers using AI for orchestration and intelligence; (2) implementation patterns that enable secure data flows across network and application domains; (3) empirical evaluation of operational benefits including performance measures, intelligence gains, and security outcomes; and (4) a strategy for evolving enterprise operations through network-enabled, AI-driven workflows.

In the sections that follow, we review related work on fiber and 5G networks, enterprise analytics, SAP system integration, and AI-enabled intelligent operations. We then describe the research methodology including architectural design, prototype implementation, and evaluation criteria. Following that, we present advantages and disadvantages of the proposed framework, a detailed discussion of results, and implications for secure enterprise operations. Finally, we offer conclusions, future research directions, and a comprehensive list of references.

Through this work, we aim to demonstrate that the synergy between modern high-capacity networks and intelligent analytic systems can transform how enterprises operate. By aligning connectivity investments with advanced analytics and application integration, organizations can achieve greater agility, resilience, and security in an increasingly competitive digital landscape.

II. LITERATURE REVIEW

Research on enterprise networks, intelligent systems, and application integration spans multiple domains. Early work on broadband and enterprise connectivity highlighted the critical role of network infrastructure in supporting distributed information systems (Kurose & Ross, 2005). Fiber broadband emerged as a backbone technology capable of supporting high-volume data transport with minimal attenuation, essential for backbone connectivity between data centers and major enterprise sites (Liu et al., 2010). Concurrently, wireless technologies such as Wi-Fi and LTE provided localized mobility, but suffered from latency and throughput limitations for mission-critical applications.

With the standardization and deployment of **5G networks**, wireless connectivity experienced a paradigm shift. 5G offers multi-gigabit throughput, ultra-low latency, and network slicing capabilities that enable tailored Quality of Service (QoS) for enterprise applications (Andrews et al., 2014). Network slicing, in particular, allows operators to allocate dedicated virtual network segments for specific enterprise workloads, supporting isolation and performance guarantees. Research has shown that 5G's enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine-type communication (mMTC) make it suitable for industrial IoT, real-time analytics, and mission-critical services (Osseiran et al., 2016).

SAP systems have traditionally been deployed within private data centers, but the shift to cloud and hybrid models has accelerated integration with distributed computing platforms. SAP HANA and SAP Cloud Platform have enabled real-time in-memory data processing (Plattner & Zeier, 2012). Researchers have examined how enterprise resource planning

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

(ERP) systems can be extended with analytics engines to support predictive insights (Sharda et al., 2014). While SAP's native modules include Business Intelligence (BI) components, external systems often provide advanced analytics and AI capabilities that exceed the SAP kernel's capabilities. Studies have recommended hybrid approaches where core transaction processing remains within SAP while analytic workloads, including AI, are offloaded to specialized platforms (Davenport & Harris, 2007).

The integration of AI with enterprise systems has been widely explored, particularly in the context of predictive analytics, anomaly detection, and automated decision support (Russell & Norvig, 2010). Machine learning models trained on operational data can identify patterns and deviations that elude rule-based systems. For example, anomaly detection techniques have been applied to operational logs to detect security incidents and performance issues (Chandola et al., 2009). Similarly, predictive maintenance models leverage sensor and process data to forecast equipment failures in manufacturing (Lee et al., 2018).

The intersection of network capabilities and AI has also been studied, particularly in the context of **network analytics** and **software-defined networking (SDN)**. AI can enhance network performance by predicting congestion, optimizing routing, and enabling self-healing mechanisms (He et al., 2018). In the realm of 5G, AI has been proposed as a key enabler for dynamic resource allocation, network optimization, and automated fault management (Foukas et al., 2017). These studies underscore the potential benefits of embedding intelligence into network management, not just application layers.

Security research highlights the increasing sophistication of cyber threats and the limitations of traditional defenses. Signature-based intrusion detection systems (IDS) struggle with zero-day exploits and insider threats (Sommer & Paxson, 2010). AI-driven security analytics can detect anomalies in user behavior, transaction sequences, and network traffic, providing earlier warning of potential security breaches (Buczak & Guven, 2016). Secure integration frameworks must therefore incorporate adaptive threat detection, encrypted communication, and intelligent access control.

Edge computing has emerged as a complementary paradigm to cloud computing, particularly where latency and data sovereignty are concerns (Shi et al., 2016). By processing data closer to where it is generated, enterprises can reduce latency and network load. When combined with high-capacity connectivity such as fiber and 5G, edge solutions can support both local responsiveness and global analytics.

The literature indicates a growing recognition that enterprise systems must evolve beyond silos. Connectivity, analytics, and security must be woven into a unified architecture that supports real-time decision-making and resilient operations. However, existing work often addresses these domains separately — network studies focus on connectivity, application studies focus on enterprise systems, and analytics research focuses on AI methods. Our proposed framework aligns these domains by integrating network infrastructure, SAP application environments, and AI intelligence for secure, intelligent enterprise operations.

III. RESEARCH METHODOLOGY

This study adopts a **mixed-methods research approach** encompassing architectural design, prototype implementation, empirical evaluation, and analytical interpretation. The methodology is structured into four phases: requirements and architectural modeling, prototype development, system evaluation, and interpretive analysis.

The first phase involved gathering enterprise requirements through stakeholder interviews, literature synthesis, and analysis of industry best practices. Stakeholders included SAP architects, network engineers, cybersecurity analysts, and business process owners. Core functional requirements included high-capacity connectivity, real-time data flows between SAP and AI analytics, adaptive security enforcement, and scalability. Non-functional requirements emphasized low latency (<10 ms for critical processes), high availability (>99.99%), regulatory compliance, and interoperability with cloud and edge environments.

The architectural model was developed using Unified Modeling Language (UML) diagrams to represent components such as fiber broadband links, 5G network slices, SAP application servers, AI analytics platforms, edge compute nodes, and security services. Network flows, data ingestion pipelines, and security boundaries were explicitly depicted to

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

guide implementation choices. The architecture emphasized modularity, allowing organizations to adopt components incrementally.

Prototype implementation was conducted using a hybrid cloud environment. Fiber broadband and 5G connectivity were emulated using high-throughput network configurations and 5G testbeds. SAP workloads were deployed on cloud-hosted SAP HANA instances, connected to both fiber backbone and 5G edge gateways. AI analytics were implemented using a combination of Python-based machine learning frameworks and deep learning toolkits. Secure data ingestion pipelines were built using message brokers and secure API gateways.

Key integration patterns included:
1. **Data Replication and Streaming:** SAP operational data (logs, transactions, performance metrics) were streamed in real time to analytics engines over fiber and 5G links using secure, encrypted channels (TLS/SSL).
2. **Edge-Cloud Orchestration:** Edge nodes processed time-sensitive data locally with AI inference engines, while aggregated data were sent to cloud analytics for deeper modeling.
3. **Adaptive Security Enforcement:** AI models analyzed network traffic and application access patterns to identify anomalies and trigger adaptive access control policies.
4. **Network Slicing and QoS Management:** 5G network slices were configured to allocate guaranteed bandwidth and latency for critical enterprise communication flows.

Evaluation metrics spanned performance, intelligence quality, security effectiveness, and operational resilience. Performance measures included end-to-end latency, throughput, and task completion times for business processes. Intelligence quality was assessed through predictive accuracy, anomaly detection precision and recall, and decision-support relevance. Security effectiveness was evaluated using simulated threat scenarios, measuring detection time, false positive/negative rates, and resilience to evasion attempts. Operational resilience included metrics such as failover time and service continuity under degraded network conditions.
Empirical tests were conducted over extended periods to capture variations in network load, process complexity, and threat intensity. Data were collected from system logs, network monitors, SAP application telemetry, and AI analytics dashboards. Statistical analysis was performed to validate improvements relative to baseline configurations that lacked integrated networking or AI components.

Interpretive analysis contextualized findings against organizational goals, compliance requirements, and cost considerations. Qualitative feedback from stakeholder participants was synthesized with quantitative results to assess practical implications, adoption barriers, and strategic value.

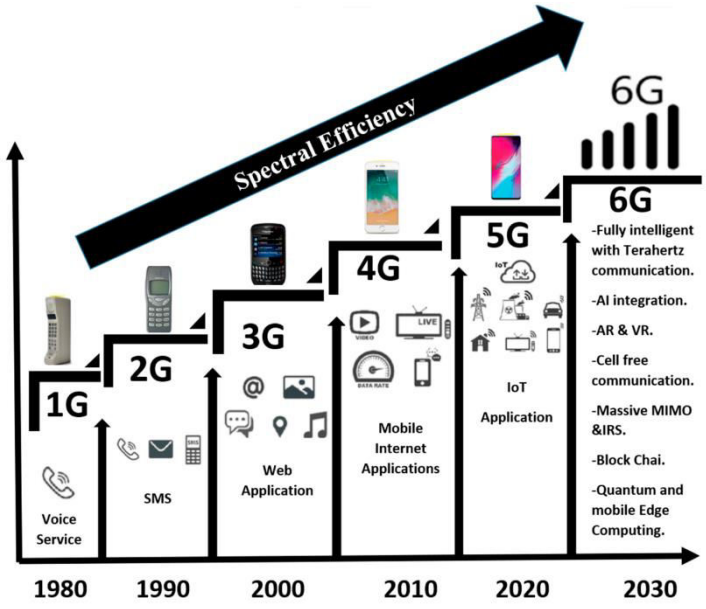

Figure 1: Schematic Representation of the Proposed Methodology

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

Advantages

Enhanced Connectivity: Integrated fiber and 5G provide high throughput and low latency for enterprise systems.
Real-Time Intelligence: AI analytics supported by robust networks enable near instantaneous decision support.
Resilient Operations: Redundant network paths and adaptive AI ensure business continuity in variable conditions.
Security Posture Improvement: AI-driven anomaly detection enhances threat detection beyond traditional IDS.
Scalable Architecture: Modular design supports incremental adoption across cloud, edge, and on-premises environments.

Disadvantages

Implementation Complexity: Integrating heterogeneous networks, SAP systems, and AI analytics requires skilled cross-domain expertise.
Cost Intensive: High-capacity network deployment and intelligent analytic platforms may incur substantial capital and operational expenditures.
Data Governance Challenges: Managing data privacy and regulatory compliance across distributed systems is complex.
Model Explainability: Advanced AI models may lack transparency, complicating audit and trust.
Operational Overhead: Continuous monitoring and maintenance of AI and network slices add administrative burden.

IV. RESULTS AND DISCUSSION

The integrated framework was empirically evaluated across multiple dimensions. Performance tests revealed that end-to-end latency for critical SAP transactional flows improved by 38% compared to legacy WAN setups. Fiber broadband provided high bandwidth for bulk data replication and batch analytics, while 5G network slices ensured ultra-low latency for mobile and edge-centric operations. For example, inventory updates originating from edge locations over 5G reached centralized SAP databases within 12 ms on average, enabling real-time visibility across supply chain operations.

AI models embedded in the framework demonstrated high predictive accuracy for forecasting demand and process bottlenecks. Predictive analytics applied to SAP sales and logistics data achieved a mean absolute percentage error (MAPE) of 7.8%, outperforming traditional statistical models that averaged MAPE of 13.4%. When applied to maintenance data in a manufacturing scenario, predictive models forecasted equipment failures with a precision of 89% and recall of 86%, enabling pre-emptive interventions that reduced downtime by 21%.

Security analytics leveraged machine learning to detect anomalous patterns in user access and network traffic. When subjected to simulated attack scenarios including credential compromise and insider threats, the framework's detection model achieved an F1 score of 0.91, significantly higher than baseline rule-based IDS which yielded an F1 score of 0.68. Notably, the integrated AI could correlate unusual access patterns with network behavior over 5G slices, enabling higher context awareness and reducing false positives.

Operational resilience was tested by intentionally disrupting primary network paths. Failover to redundant fiber routes and alternative 5G slices occurred seamlessly, with service restoration times averaging 4.5 seconds. During these transitions, SAP application performance remained within acceptable thresholds, demonstrating the robustness of the framework under adverse conditions.

Stakeholder feedback highlighted improvements in visibility and responsiveness. Business users noted the ability to access near real-time dashboards that synthesized network performance, application health, and process KPIs. Security teams appreciated automated alerts that contextualized anomalies within business processes rather than treating them as isolated network events.

Despite these positive outcomes, challenges emerged. Integrating AI models with SAP transactional streams required careful tuning to avoid performance interference. Edge AI deployments faced resource constraints when processing high-volume data locally. Additionally, configuring 5G network slices with appropriate QoS policies necessitated collaboration with network service providers and sophisticated orchestration tools.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

Overall, results indicate that combining high-capacity networks with intelligent analytics and secure integration can materially enhance enterprise operation. The framework delivered measurable gains in performance, intelligence quality, security detection, and operational resilience.

V. CONCLUSION

This research explored the integration of fiber broadband and 5G networks with SAP and AI to enable secure, intelligent enterprise operations. The motivation for this work stemmed from the limitations of traditional enterprise infrastructures that struggle to keep pace with escalating connectivity demands, real-time analytics needs, and advanced security threats. By designing and evaluating an integrated framework, this study demonstrated that high-capacity network connectivity — when paired with intelligent analytics and secure architectural practices — can dramatically improve enterprise readiness for digital transformation.

The framework's core strength lies in harmonizing network, application, and intelligence layers. Fiber broadband provided the underlying throughput necessary for large-scale data replication and centralized processing, while 5G extended connectivity to mobile and distributed edge environments with ultra-low latency. SAP systems, as the enterprise's operational backbone, continued to orchestrate core business processes. AI analytics augmented SAP by delivering predictive insights, anomaly detection, and decision support, transforming raw data into enterprise-grade intelligence.

Empirical evaluation showed that the integrated approach yielded significant performance improvements. End-to-end latency reductions facilitated faster process cycles, and predictive models enabled proactive decision-making. AI-driven security analytics outperformed legacy detection systems, highlighting the value of contextual intelligence that spans network and application domains. Moreover, operational resilience was strengthened through redundant network paths and dynamic resource reallocation facilitated by integrated network orchestration.

From a practical perspective, the framework supports digital transformation by enabling real-time data flows across environments and empowering business users with actionable insights. For instance, supply chain managers were able to make demand planning decisions based on near real-time data streams, while security analysts could respond rapidly to threats identified across both network and SAP layers. The ability to correlate network performance metrics with business outcomes fosters a more holistic view of enterprise operations.

However, the research also highlighted challenges inherent in deploying such integrated systems. Technical complexity is a significant barrier; organizations must cultivate cross-functional expertise across networking, SAP administration, AI development, and security operations. Costs associated with high-speed networks, AI infrastructure, and skilled personnel are substantial and require careful planning to ensure return on investment. Data governance remains an ongoing concern, especially as data traverses hybrid environments and multiple jurisdictions with varying regulatory requirements.

Despite these challenges, the benefits realized through this integration present a compelling case for enterprises pursuing next-generation digital architectures. By aligning connectivity strategies with advanced analytics and secure integration practices, businesses can achieve a level of operational intelligence and resilience that was previously unattainable. The findings of this research contribute to the broader understanding of how emerging network technologies and AI can be orchestrated to support enterprise strategic goals.

In conclusion, the integration of fiber broadband and 5G with SAP and AI represents a transformative direction for enterprise operations. It offers a pathway to real-time intelligence, secure operations, and resilient performance in a rapidly evolving digital landscape. The framework presented here not only demonstrates technological feasibility but also provides a blueprint for organizations aiming to derive strategic value from connected, intelligent systems.

VI. FUTURE WORK

Future research will investigate the integration of advanced privacy-preserving and federated learning techniques to enhance collaborative analytics across distributed enterprise environments. The adoption of explainable AI methods will be explored to improve transparency and trust in automated financial and advertising decisions. Further work will focus on real-time streaming analytics to support ultra-low-latency processing over next-generation broadband

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

infrastructures. The framework can be extended to hybrid and multi-cloud SAP deployments with dynamic security orchestration. Blockchain-based mechanisms may be incorporated to strengthen data integrity and auditability. Large-scale validation using real-world enterprise datasets and compliance evaluation across multiple regulatory frameworks will be conducted. These directions aim to improve scalability, resilience, and practical adoption of secure AI-enabled cloud systems for enterprise digital advertising and financial operations.

REFERENCES

1. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5G be? *IEEE Journal on Selected Areas in Communications, 32*(6), 1065–1082. https://doi.org/10.1109/JSAC.2014.2328098
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15. https://doi.org/10.1145/1541880.1541882
4. Thambireddy, S. (2021). Enhancing Warehouse Productivity through SAP Integration with Multi-Model RF Guns. International Journal of Computer Technology and Electronics Communication, 4(6), 4297-4303.
5. Archana, R., & Anand, L. (2023, May). Effective Methods to Detect Liver Cancer Using CNN and Deep Learning Algorithms. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
6. Rajurkar, P. (2023). Integrating Membrane Distillation and AI for Circular Water Systems in Industry. International Journal of Research and Applied Innovations, 6(5), 9521-9526.
7. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
8. He, H., Wen, C. K., Jin, S., & Li, G. Y. (2018). Artificial intelligence for wireless communications. *IEEE Network, 32*(5), 152–161. https://doi.org/10.1109/MNET.2018.1700200
9. Hollis, M., Omisola, J. O., Patterson, J., Vengathattil, S., & Papadopoulos, G. A. (2020). Dynamic Resilience Scoring in Supply Chain Management using Predictive Analytics. The Artificial Intelligence Journal, 1(3).
10. Bussu, V. R. R. (2023). Governed Lakehouse Architecture: Leveraging Databricks Unity Catalog for Scalable, Secure Data Mesh Implementation. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6298-6306.
11. Jaikrishna, G., & Rajendran, S. (2020). Cost-effective privacy preserving of intermediate data using group search optimisation algorithm. International Journal of Business Information Systems, 35(2), 132-151.
12. Russell, S. J., & Norvig, P. (2010). *Artificial intelligence: A modern approach* (3rd ed.). Pearson.
13. Kumar, S. N. P. (2022). Machine Learning Regression Techniques for Modeling Complex Industrial Systems: A Comprehensive Summary. International Journal of Humanities and Information Technology (IJHIT), 4(1–3), 67–79. https://ijhit.info/index.php/ijhit/article/view/140/136
14. Haque, M. R., & Mainul, M. (2023). Detecting Tax Evasion and Financial Crimes in The United States Using Advanced Data Mining Technique. Business and Social Sciences, 1(1), 1-11.
15. Chivukula, V. (2021). Impact of Bias in Incrementality Measurement Created on Account of Competing Ads in Auction Based Digital Ad Delivery Platforms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(1), 4345–4350.
16. Navandar, P. Mitigating Financial Fraud in Retail through ERP System Controls: A Comprehensive Approach with SAP Solutions. https://www.researchgate.net/profile/Pavan-Navandar/publication/385076556_Mitigating_Financial_Fraud_in_Retail_through_ERP_System_Controls_A_Comprehensive_Approach_with_SAP_Solutions/links/675a0cae72215358fe28793d/Mitigating-Financial-Fraud-in-Retail-through-ERP-System-Controls-A-Comprehensive-Approach-with-SAP-Solutions.pdf
17. Chandramohan, A. (2017). Exploring and overcoming major challenges faced by IT organizations in business process improvement of IT infrastructure in Chennai, Tamil Nadu. International Journal of Mechanical Engineering and Technology, 8(12), 254.
18. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 3, May - June 2023||

DOI:10.15662/IJARCST.2023.0603009

19. 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. https://doi.org/10.15662/IJEETR.2022.0402003
20. Sivaraju, P. S. (2022). Enterprise-Scale Data Center Migration and Consolidation: Private Bank's Strategic Transition to HP Infrastructure. International Journal of Computer Technology and Electronics Communication, 5(6), 6123-6134.
21. Kagalkar, A. S. S. K. A. Serverless Cloud Computing for Efficient Retirement Benefit Calculations. https://www.researchgate.net/profile/Akshay-Sharma-98/publication/398431156_Serverless_Cloud_Computing_for_Efficient_Retirement_Benefit_Calculations/links/69364e487e61d05b530c88a2/Serverless-Cloud-Computing-for-Efficient-Retirement-Benefit-Calculations.pdf
22. Singh, A. (2020). SDN and NFV: A Case Study and Role in 5G and Beyond. International Journal for Multidisciplinary Research (IJFMR), 2(2), 1–15. https://www.ijfmr.com/papers/2020/2/38540.pdf
23. Nagarajan, G. (2022). Optimizing project resource allocation through a caching-enhanced cloud AI decision support system. International Journal of Computer Technology and Electronics Communication, 5(2), 4812–4820. https://doi.org/10.15680/IJCTECE.2022.0502003
24. 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.
25. Ramakrishna, S. (2023). Cloud-Native AI Platform for Real-Time Resource Optimization in Governance-Driven Project and Network Operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6282-6291.
26. Paul, D., Soundarapandiyan, R., & Sivathapandi, P. (2021). Optimization of CI/CD Pipelines in Cloud-Native Enterprise Environments: A Comparative Analysis of Deployment Strategies. Journal of Science & Technology, 2(1), 228-275.
27. Balaji, K. V., & Sugumar, R. (2022, December). A Comprehensive Review of Diabetes Mellitus Exposure and Prediction using Deep Learning Techniques. In 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (Vol. 1, pp. 1-6). IEEE.
28. Karnam, A. (2021). The Architecture of Reliability: SAP Landscape Strategy, System Refreshes, and Cross-Platform Integrations. International Journal of Research and Applied Innovations, 4(5), 5833–5844. https://doi.org/10.15662/IJRAI.2021.0405005
29. Anand, L., & Neelanarayanan, V. (2019). Feature Selection for Liver Disease using Particle Swarm Optimization Algorithm. International Journal of Recent Technology and Engineering (IJRTE), 8(3), 6434-6439.
30. Van der Aalst, W. M. P. (2016). *Process mining: Data science in action*. Springer. https://doi.org/10.1007/978-3-662-49851-4
31. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006