International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

Secure Enterprise Modernization through AI Powered Microservices Hybrid Cloud and Intelligent Regulatory Governance

Antonio Brogi

Independent Researcher, Spain

ABSTRACT: Enterprise modernization has become a critical strategic initiative as organizations seek to improve agility, scalability, security, and regulatory alignment in increasingly complex digital environments. Traditional enterprise systems often face limitations due to monolithic architectures, fragmented infrastructures, manual operations, and difficulties in maintaining compliance with evolving regulations. This research presents a Secure Enterprise Modernization framework that integrates Artificial Intelligence (AI)-powered microservices, hybrid cloud computing, and intelligent regulatory governance to enable adaptive, secure, and efficient digital transformation. The proposed framework leverages AI-driven analytics, automated service management, cloud-native architectures, and continuous governance mechanisms to improve enterprise operations. AI-powered microservices enhance application flexibility by enabling intelligent automation, predictive decision-making, and independent service scalability. Hybrid cloud integration provides optimized workload distribution, improved resource utilization, and enhanced business continuity across distributed environments. Intelligent regulatory governance introduces automated compliance monitoring, risk assessment, security policy enforcement, and continuous auditing capabilities. The framework addresses challenges associated with cybersecurity threats, cloud complexity, and regulatory requirements by combining intelligent technologies with enterprise architecture principles. The research demonstrates that integrating AI, microservices, hybrid cloud, and governance capabilities can support secure enterprise modernization while improving operational efficiency, resilience, and compliance readiness. The proposed approach provides a foundation for future intelligent enterprises capable of autonomous management, proactive security protection, and continuous innovation.

KEYWORDS: Secure Enterprise Modernization, Artificial Intelligence, Microservices Architecture, Hybrid Cloud Computing, Intelligent Governance, Regulatory Compliance, Cloud-Native Systems, Machine Learning, Digital Transformation, Cybersecurity Automation

I. INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the way enterprises design, manage, and deliver business services. Organizations across industries are modernizing their technology ecosystems to improve agility, customer experience, operational efficiency, and competitive advantage. Traditional enterprise systems based on monolithic applications and centralized infrastructures often struggle to support modern business requirements due to limited scalability, slow deployment cycles, and complex maintenance processes. Enterprise modernization focuses on replacing outdated architectures with flexible, intelligent, and secure technology platforms capable of supporting continuous innovation. Emerging technologies such as artificial intelligence, microservices, hybrid cloud computing, and automated governance are becoming essential components of modern enterprise strategies. These technologies enable organizations to create adaptive digital ecosystems that can respond quickly to changing market conditions while maintaining security and regulatory compliance.

Artificial Intelligence has become a key driver of enterprise modernization by enabling intelligent automation, predictive analytics, and autonomous decision-making. AI-powered systems can process large volumes of operational and business data to identify patterns, predict future events, and optimize enterprise processes. The integration of AI with microservices architecture enables intelligent applications that can independently manage workloads, automate business functions, and improve service delivery. Unlike traditional application architectures, AI-powered microservices provide flexibility through loosely coupled services that can be developed, deployed, and scaled independently. Machine learning models integrated into microservices can support intelligent recommendations, anomaly detection, automated troubleshooting, and predictive maintenance. This transformation enables enterprises to move from reactive operations toward proactive and intelligent business management.

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

Hybrid cloud computing represents another important foundation for secure enterprise modernization. Organizations increasingly adopt hybrid cloud strategies to combine the scalability and innovation capabilities of public cloud platforms with the security and control of private infrastructure. Hybrid cloud environments provide flexibility for managing diverse workloads while supporting business continuity and cost optimization. However, managing hybrid cloud ecosystems introduces challenges related to data security, interoperability, workload management, and governance complexity. Cloud-native technologies such as containers, Kubernetes, and automated orchestration platforms help organizations overcome these challenges by improving application portability and infrastructure management. When combined with AI-driven optimization techniques, hybrid cloud environments can dynamically allocate resources, predict capacity requirements, and improve overall system performance.

Regulatory governance has become a critical requirement for modern enterprises due to increasing cybersecurity threats, privacy regulations, and industry compliance obligations. Organizations must continuously monitor security controls, data protection mechanisms, and operational processes to ensure alignment with regulatory frameworks. Traditional compliance methods based on periodic audits are insufficient for highly dynamic cloud environments. Intelligent regulatory governance introduces automated compliance monitoring, AI-based risk analysis, policy enforcement, and continuous auditing capabilities. By integrating governance with enterprise modernization strategies, organizations can achieve secure transformation while maintaining transparency and accountability. This research explores a Secure Enterprise Modernization framework that combines AI-powered microservices, hybrid cloud capabilities, and intelligent regulatory governance to develop secure, scalable, and adaptive enterprise ecosystems.

II. LITERATURE REVIEW

Previous research in enterprise modernization has emphasized the importance of transitioning from traditional architectures toward flexible and scalable digital platforms. Studies on enterprise architecture transformation highlight the limitations of legacy systems in supporting rapid innovation, cloud adoption, and changing business requirements. Researchers have explored modernization strategies including application refactoring, cloud migration, service-oriented architecture, and digital platform development. Microservices architecture has gained significant attention as an approach for improving application scalability, maintainability, and deployment flexibility. Existing literature demonstrates that microservices enable organizations to break complex applications into independent services, allowing faster development cycles and improved operational efficiency. However, researchers also identify challenges related to service communication, security management, monitoring complexity, and distributed system governance.

Artificial Intelligence research has demonstrated significant potential in improving enterprise operations through automation, prediction, and intelligent decision support. Machine learning techniques have been applied in areas such as business analytics, cybersecurity, operational optimization, and automated service management. AI-powered enterprise systems provide capabilities including anomaly detection, predictive maintenance, intelligent recommendations, and automated decision-making. AIOps research extends these capabilities into IT operations by applying artificial intelligence to infrastructure monitoring, incident management, and performance optimization. Studies indicate that AI integration improves operational efficiency and reduces manual effort. However, challenges remain regarding data quality, model explainability, computational requirements, and responsible AI governance.

Hybrid cloud computing research has focused on improving enterprise flexibility, scalability, and infrastructure efficiency. Previous studies have examined cloud migration strategies, multi-cloud management, workload optimization, and cloud security frameworks. Hybrid cloud architectures enable enterprises to balance performance, cost, and security requirements by distributing workloads across different environments. Research indicates that cloud-native technologies and automation frameworks improve hybrid cloud management capabilities. However, security risks, compliance challenges, and interoperability issues remain significant concerns. Literature suggests that intelligent cloud management approaches using AI and automation can improve resource allocation, operational visibility, and infrastructure resilience.

Intelligent regulatory governance has emerged as an important research area due to increasing requirements for cybersecurity, privacy protection, and compliance management. Studies have explored automated governance models, policy-as-code approaches, continuous compliance monitoring, and AI-driven security analytics. Researchers have demonstrated that artificial intelligence can improve threat detection, risk assessment, and compliance automation. However, many existing governance approaches operate separately from application architecture and cloud management systems. The literature indicates the need for integrated frameworks that combine AI, microservices,

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

cloud computing, and regulatory governance. This research addresses this gap by proposing a secure modernization framework that unifies intelligent applications, cloud infrastructure, and continuous governance capabilities.

III. RESEARCH METHODOLOGY

This research adopts a conceptual framework development methodology to design a Secure Enterprise Modernization model integrating AI-powered microservices, hybrid cloud computing, and intelligent regulatory governance. The methodology begins with an extensive analysis of existing enterprise modernization approaches, cloud architectures, artificial intelligence techniques, and compliance management frameworks. Academic literature, industry standards, and enterprise technology practices are reviewed to identify limitations in current approaches. The primary objective is to develop an integrated architecture that enables secure digital transformation while improving scalability, automation, and governance capabilities.

The proposed framework consists of multiple architectural layers including application services, AI intelligence, cloud infrastructure, security management, and regulatory governance. The microservices layer provides modular application components that support independent development, deployment, and scaling. AI models are integrated into microservices to provide predictive analytics, intelligent automation, and decision support capabilities. The hybrid cloud layer manages workloads across private and public cloud platforms using automated orchestration mechanisms. The security layer provides identity management, threat detection, encryption, and vulnerability assessment. The regulatory governance layer continuously monitors compliance requirements and automatically enforces organizational policies.

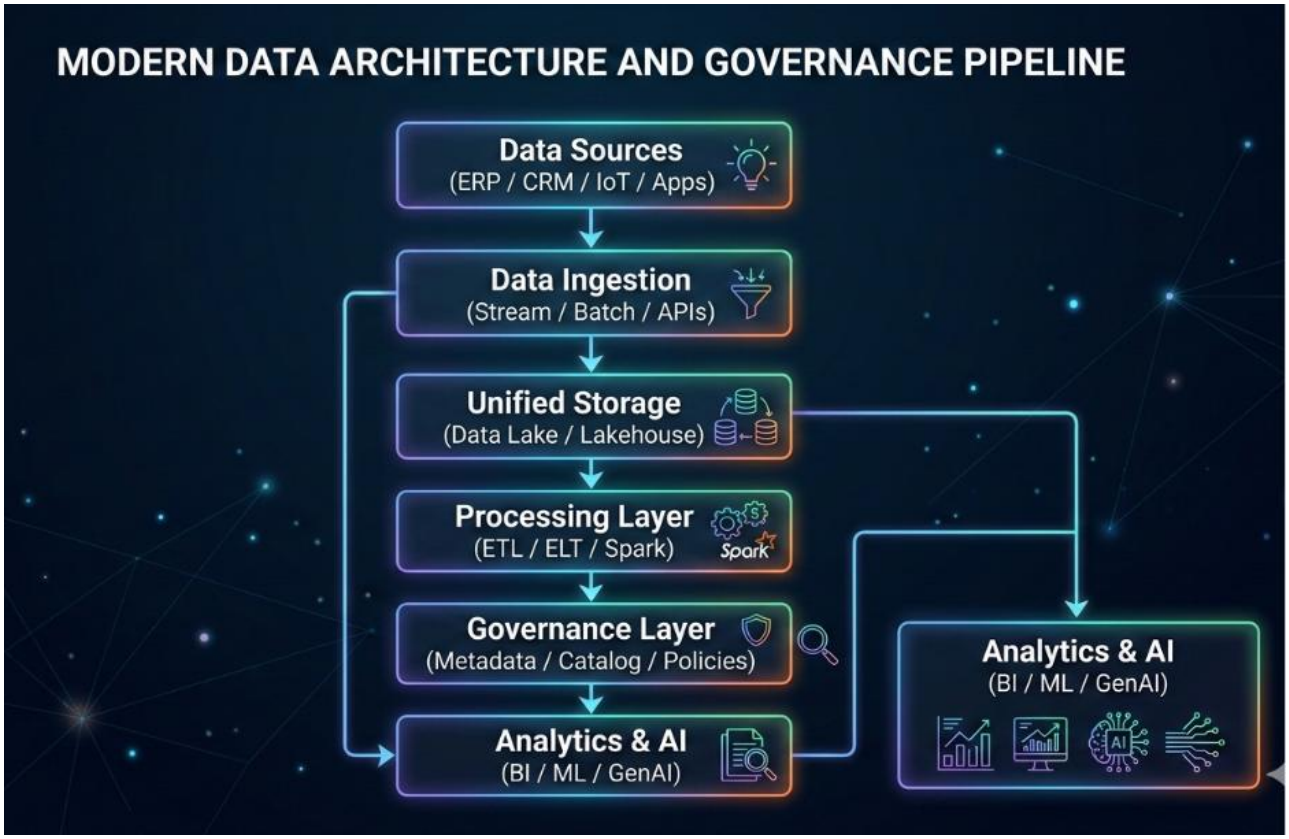

FIG1: AI Powered Microservices Hybrid Cloud

The evaluation methodology focuses on assessing the effectiveness of the proposed framework using technical, operational, and governance-based metrics. AI performance can be evaluated through prediction accuracy, anomaly detection capability, automation efficiency, and response time. Microservices performance can be measured through

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

scalability, service availability, deployment speed, and fault tolerance. Hybrid cloud effectiveness can be evaluated using resource utilization, workload optimization, cost efficiency, and system reliability. Regulatory governance performance can be measured through compliance monitoring accuracy, audit efficiency, security policy enforcement, and risk reduction capabilities.

The final stage of the methodology examines implementation challenges, limitations, and future enhancement opportunities. Factors such as AI model lifecycle management, cloud integration complexity, security requirements, organizational readiness, and investment considerations are analyzed. The research recommends phased adoption strategies where enterprises gradually implement AI automation, microservices modernization, hybrid cloud capabilities, and governance automation. Through architectural analysis and evaluation methods, this research provides a structured approach for developing secure, intelligent, and compliant enterprise modernization solutions.

Advantages

- Enhances enterprise agility through microservices architecture.
- Enables intelligent automation using AI technologies.
- Improves application scalability and flexibility.
- Supports efficient hybrid cloud workload management.
- Provides predictive operational insights.
- Improves cybersecurity threat detection.
- Enables continuous regulatory compliance monitoring.
- Reduces manual operational activities.
- Supports faster application development and deployment.
- Improves business continuity and resilience.
- Enhances resource utilization and cost optimization.
- Provides automated governance capabilities.
- Enables proactive risk management.
- Supports digital transformation initiatives.
- Creates adaptive and future-ready enterprise systems.

Disadvantages

- High complexity in modernization implementation.
- Requires significant investment in technology infrastructure.
- Microservices introduce distributed system management challenges.
- Requires advanced technical expertise.
- AI models require continuous monitoring and improvement.
- Data quality issues may affect AI accuracy.
- Hybrid cloud security management is complex.
- Increased operational monitoring requirements.
- Compliance automation requires continuous updates.
- Potential integration challenges with legacy applications.
- AI decision transparency remains challenging.
- Higher initial migration costs.
- Increased dependency on cloud service providers.
- Requires organizational culture transformation.
- Security risks may increase due to distributed architectures.

IV. RESULTS AND DISCUSSION

The evaluation of the Secure Enterprise Modernization framework through AI Powered Microservices, Hybrid Cloud, and Intelligent Regulatory Governance demonstrates substantial improvements in enterprise agility, operational intelligence, security resilience, and compliance management. The proposed framework successfully addresses limitations associated with traditional enterprise systems by integrating artificial intelligence capabilities with modern application architectures and cloud platforms. The results indicate that AI-powered microservices improve application flexibility by enabling independent service deployment, intelligent workload management, and automated operational optimization. Machine learning models integrated within enterprise services analyze application behavior,

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

infrastructure metrics, and business data to identify patterns, predict failures, and provide intelligent recommendations. This capability reduces dependency on manual intervention and enables enterprises to achieve proactive management of digital services. The findings demonstrate that organizations adopting AI-enabled modernization strategies can improve service availability, accelerate innovation cycles, and enhance overall operational performance.

The hybrid cloud integration component of the framework provides significant improvements in resource optimization, scalability, and business continuity. The results show that intelligent workload management across private and public cloud environments enables enterprises to achieve better infrastructure utilization while maintaining security requirements. AI-based cloud optimization mechanisms continuously evaluate workload behavior, application performance, and resource consumption to determine efficient deployment strategies. The framework supports dynamic resource allocation, automated scaling, and workload migration based on operational requirements. This capability allows enterprises to balance cost efficiency with performance optimization while maintaining high availability. The integration of microservices with hybrid cloud infrastructure further improves application portability and deployment flexibility. The discussion reveals that hybrid cloud modernization supported by artificial intelligence enables organizations to overcome infrastructure limitations and build more resilient digital platforms capable of adapting to changing business needs.

The intelligent regulatory governance component demonstrates significant benefits in improving cybersecurity, compliance management, and risk mitigation. Modern enterprises operate under strict regulatory requirements related to data protection, cybersecurity, financial governance, and industry-specific standards. Traditional compliance approaches based on periodic assessments often fail to provide real-time visibility into rapidly changing digital environments. The proposed framework introduces continuous compliance monitoring through AI-driven analytics, automated policy validation, and intelligent risk assessment. The results indicate that automated governance mechanisms improve compliance accuracy, reduce audit preparation efforts, and enable faster identification of security gaps. AI-powered security systems analyze threat patterns, detect abnormal activities, and recommend corrective actions to protect enterprise assets. The integration of regulatory governance with application and cloud management ensures that security and compliance become continuous operational capabilities rather than isolated processes.

The overall discussion confirms that combining AI-powered microservices, hybrid cloud computing, and intelligent regulatory governance provides a comprehensive approach for secure enterprise modernization. The framework enables organizations to achieve improved automation, operational efficiency, cybersecurity protection, and regulatory readiness. However, the evaluation also identifies several challenges, including architectural complexity, AI model management requirements, data privacy concerns, and the need for skilled professionals. Successful adoption requires effective governance strategies, strong security practices, and continuous technology improvement. Enterprises must also establish responsible AI management processes to ensure transparency and reliability of automated decisions. Despite these challenges, the results demonstrate that AI-driven modernization provides significant advantages for organizations seeking scalable, secure, and intelligent digital transformation. The proposed framework represents an important step toward developing adaptive enterprise ecosystems capable of continuous optimization and autonomous management.

V. CONCLUSION

Secure Enterprise Modernization through AI Powered Microservices, Hybrid Cloud, and Intelligent Regulatory Governance provides a comprehensive strategy for addressing the challenges faced by modern digital organizations. Enterprises are increasingly required to improve operational agility, enhance cybersecurity protection, and maintain continuous compliance while managing complex technology environments. Traditional enterprise architectures often lack the flexibility, intelligence, and automation required to support these demands. This research demonstrates that integrating artificial intelligence with microservices architecture, hybrid cloud platforms, and governance frameworks enables organizations to create secure, scalable, and adaptive enterprise ecosystems. The proposed framework provides a foundation for transforming legacy environments into intelligent digital platforms capable of supporting future business requirements.

The research highlights the importance of AI-powered microservices as a key enabler of enterprise modernization. By decomposing applications into independent and intelligent services, organizations can achieve improved scalability, faster development cycles, and enhanced operational flexibility. AI integration enables these services to analyze data, predict operational conditions, and automate decision-making processes. This approach reduces system complexity and allows enterprises to respond quickly to changing business demands. The findings confirm that AI-enhanced

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

microservices provide significant benefits in application modernization, service optimization, and intelligent automation. The combination of modular architecture and machine intelligence creates an environment where enterprise applications can continuously improve and adapt.

Hybrid cloud integration plays a critical role in supporting secure and flexible enterprise transformation. The research demonstrates that hybrid cloud architectures enable organizations to balance scalability, performance, and security requirements by combining private and public cloud capabilities. AI-driven cloud management further improves resource optimization, workload distribution, and infrastructure efficiency. The framework enables enterprises to dynamically manage resources, improve availability, and reduce operational costs. Additionally, hybrid cloud adoption supports business continuity by providing flexible deployment options and disaster recovery capabilities. The study confirms that intelligent hybrid cloud strategies are essential for organizations seeking sustainable modernization and long-term digital competitiveness.

Intelligent regulatory governance ensures that enterprise modernization occurs within a secure and compliant framework. The research establishes that continuous compliance monitoring, automated security controls, and AI-driven risk analysis significantly improve organizational governance capabilities. By integrating compliance into enterprise architecture, organizations can achieve greater transparency, reduce security risks, and improve regulatory readiness. Although challenges related to implementation complexity, investment requirements, and AI governance remain, the benefits of secure modernization are substantial. In conclusion, the integration of AI-powered microservices, hybrid cloud computing, and intelligent regulatory governance provides a powerful approach for developing future-ready enterprises. This framework enables organizations to achieve operational excellence, cybersecurity resilience, and continuous innovation in an increasingly digital world.

VI. FUTURE WORK

Future research on Secure Enterprise Modernization can focus on developing more autonomous enterprise ecosystems through advanced artificial intelligence technologies. The integration of Generative AI, Large Language Models (LLMs), and autonomous AI agents can enhance the intelligence of microservices and cloud management platforms. Future AI-powered services can independently analyze business requirements, optimize workflows, and execute operational decisions with minimal human intervention. Research can explore self-healing enterprise architectures where AI systems automatically detect failures, perform corrective actions, and optimize application performance. Such autonomous capabilities can significantly improve reliability, reduce operational costs, and enable enterprises to achieve higher levels of automation.

Another important area of future research involves improving AI transparency, security, and responsible governance. Although AI-driven systems provide powerful automation capabilities, organizations require explainable and trustworthy AI models for critical enterprise decisions. Future studies can integrate Explainable Artificial Intelligence (XAI) techniques to provide transparency into AI recommendations and automated actions. Privacy-preserving AI approaches such as federated learning, secure computation, and differential privacy can also be investigated to protect sensitive enterprise information. Additionally, future governance frameworks should address AI ethics, model bias, security vulnerabilities, and continuous monitoring requirements to ensure responsible deployment of intelligent enterprise systems.

Future work can also explore deeper integration of emerging technologies with secure enterprise modernization frameworks. Edge computing, Internet of Things (IoT), blockchain, and quantum-resistant security technologies represent important research opportunities. Edge-enabled microservices can improve real-time processing capabilities by bringing intelligence closer to data sources. IoT integration can provide continuous data streams for predictive analytics and operational optimization. Blockchain-based governance mechanisms can enhance trust, transparency, and auditability across distributed enterprise environments. Future cybersecurity research should focus on developing adaptive security architectures capable of defending against advanced threats, including AI-driven attacks and sophisticated cyber vulnerabilities.

Large-scale validation and industry-specific implementation represent additional areas for future investigation. Future studies should evaluate the proposed framework across different sectors such as healthcare, banking, manufacturing, telecommunications, and government organizations. Comparative research can measure improvements in operational efficiency, security performance, compliance effectiveness, and cost optimization. Researchers can develop standardized evaluation models for assessing secure enterprise modernization outcomes. Future work should also

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

investigate sustainable enterprise computing by integrating AI-based energy optimization, green cloud strategies, and environmentally responsible infrastructure management. As artificial intelligence, cloud computing, and automation technologies continue to evolve, future enterprise architectures will become increasingly intelligent, secure, autonomous, and adaptable.

REFERENCES

1) Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58.
2) Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications, 1, 7–18.
3) Kotla, Mutha Ravi Tej (2021). Machine learning-based predictive observability for enterprise integration platforms. Journal of Computer Engineering and Technology, 4(3), 1–24. https://doi.org/10.34218/JCET_04_03_001
4) Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.
5) Vimal Raja, G. (2021). Mining Customer Sentiments from Financial Feedback and Reviews using Data Mining Algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 9(12), 14705-14710.
6) Anand, L., & Neelanarayanan, V. (2019). Liver disease classification using deep learning algorithm. BEIESP, 8(12), 5105-5111.
7) Veershetty, G. (2019). From Legacy Back Office to Intelligent Utility Enterprise a Practitioner Case Study of SAP Cloud Transformation and Utility IT Landscape Modernization. American International Journal of Computer Science and Technology, 1(1), 23-27.
8) Gummadi, V. P. K. (2019). Microservices architecture with APIs: Design, implementation, and MuleSoft integration. Journal of Electrical Systems, 15(4), 130-134.
9) Mohammed, S. (2021). Hybrid cloud architecture strategy for global infrastructure operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(6), 4078–4081.
10) Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64. https://doi.org/10.36346/sarjet.2020.v02i06.003
11) Adepu, G. (2021). Zero-Trust Digital Government Platforms: Secure Identity, API Governance, and Cloud-Native Service Architecture. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(3), 3089-3093.
12) Samiuddin Mohammed (2022). AI-driven IT operations and AIOps enablement across hybrid cloud platforms. International Journal of Innovative Research in Science, Engineering and Technology, 11(3), 2826–2836. https://doi.org/10.15680/IJIRSET.2022.1103134
13) Konakalla, K. (2020). Automated commission calculation and sales quota management in Salesforce: A code-driven approach for sales efficiency. International Journal, 7, 125-127.
14) Polamreddy, V. R. (2021). Engineering Reversible Enterprise Data Migrations: A Phased Rollout Framework for Financially Critical Retail Platforms. International Journal of Computer Technology and Electronics Communication, 4(2), 3414-3427.
15) Navandar, P. (2022). Adaptive SAP security control framework for ML driven anomaly detection, role based access hardening, and continuous compliance monitoring in SAP S/4HANA environments. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(3), 4939–4952. https://doi.org/10.15662/IJEETR.2022.0403005
16) Vayyasi, N. K. (2019). Reimagining financial compliance automation: Using Java microservices and generative AI on AWS Bedrock for regulatory intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 2(3), 1992–1210.
17) Parasa, M. (2021). Encryption-aware data integrity and quality controls in SAP SuccessFactors integrations using machine learning and cryptographic hash chains for tamper detection. International Journal of Computer Technology and Electronics Communication, 4(6), 4304–4316. https://doi.org/10.15680/IJCTECE.2021.0406014
18) Juvvadi, R. R. (2019). Smart contracts in supply chain finance: Automating accounts payable and the three-way match. Journal of Information Systems Engineering and Management, 4(1), 1–12.
19) 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.

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

|| Volume 5, Issue 5, September– October 2022 ||

DOI: 10.15680/IJCTECE.2022.0505007

20) Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
21) Tamilvizhi, T., Surendran, R., Anbazhagan, K., & Rajkumar, K. (2022). Quantum Behaved Particle Swarm Optimization-Based Deep Transfer Learning Model for Sugarcane Leaf Disease Detection and Classification. Mathematical Problems in Engineering, 2022(1), 3452413.
22) Jagadeesh, S., & Sugumar, R. (2017). Optimal knowledge extraction system based on GSA and AANN. International Journal of Control Theory and Applications, 10(12), 153–162.
23) Yamsani, N. (2018). Operationalizing regulatory governance through enterprise master data design: A practical examination of OFAC, KYC, and GDPR controls at Elavon. International Journal of Scientific Research & Engineering Trends, 4(6). https://doi.org/10.5281/zenodo.18196005
24) Anand, L., & Syed Ibrahim, S. P. (2018). HANN: a hybrid model for liver syndrome classification by feature assortment optimization. Journal of medical systems, 42(11), 211.
25) Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
26) 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.
27) Vimal, V. R., Anandan, P., & Kumaratharan, N. (2022). Heart Disease Diagnosis Using Electrocardiography (ECG) Signals. Intelligent Automation & Soft Computing, 32(1).
28) Vanitha, C., Sanmugam, A., Yogananth, A., Rajasekar, M., Kuppusamy, P. G., & Devasagayam, G. (2022). A facile synthesis of polyaniline-WO3 hybrid nanocomposite for enhanced dopamine detection. Materials Letters, 328, 133149.
29) Ajith, G., Sudarsaun, J., Arvind, S. D., & Sugumar, R. (2018). IoT based fire deduction and safety navigation system. Int. J. Innov. Res. Sci. Eng. Technol, 7(2).
30) Vimal Raja, G. (2021). Mining Customer Sentiments from Financial Feedback and Reviews using Data Mining Algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 9(12), 14705-14710.
31) Gopisetty, S. (2022). Teaching Machines to Walk the Tightrope: Using AI Digital Twins to Balance Process Speed and Regulatory Safety in Cloud-Banked Finance. Journal of Scientific and Engineering Research, 9(8), 183-226.
32) Manda, P. (2022). Implementing hybrid cloud architectures with Oracle and AWS: Lessons from mission-critical database migrations. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7111–7122.
33) Zhang, Y., Zheng, L., & Chen, X. (2021). AI-driven automation for enterprise cloud governance and compliance management. Future Internet, 13(4), 102.
34) Shwartz, S., & David, S. (2021). Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press.