The American Journal of Applied Sciences
ISSN 2689-0992 Volume 08 - 2026

A Multidisciplinary Analytical Model For Ai-Powered Regulatory Automation And Performance Optimization In Cloud-Integrated Critical Infrastructure Systems

Dr. Pierre Lambert

Department of Smart Computing

Monaco Institute of Technology

Monaco

Received: 23 Feb 2026 | Received Revised Version: 30 Mar 2026 | Accepted: 20 Apr 2026 | Published: 20 May 2026

Volume 08 Issue 05 2026 |

Abstract

The increasing complexity of critical infrastructure systems in financial and healthcare ecosystems has intensified the demand for intelligent automation mechanisms capable of ensuring regulatory compliance, operational efficiency, and data integrity. Traditional compliance systems are largely rule-based, static, and unable to adapt to rapidly evolving regulatory frameworks and distributed cloud-native architectures. This research proposes a multidisciplinary analytical model for AI-powered regulatory automation and performance optimization in cloud-integrated environments. The study synthesizes concepts from artificial intelligence, cloud computing, regulatory analytics, and distributed systems engineering to design a unified compliance optimization framework.

The proposed model integrates machine learning-driven compliance monitoring, cloud-native orchestration mechanisms, and data lineage tracking systems to ensure transparency and auditability across heterogeneous infrastructures. Foundational cloud computing principles highlight the transformation of IT resources into scalable utility-based services (Buyya et al., 2009), which forms the basis for regulatory automation at scale. The study further examines how metadata management, secure access control, and AI-driven anomaly detection contribute to improving decision-making accuracy and reducing operational overhead.

A structured analytical framework is developed through systematic synthesis of existing literature in healthcare informatics, financial risk governance, and cloud systems engineering. The findings indicate that AI-enhanced compliance systems significantly improve regulatory responsiveness, reduce latency in audit processes, and enhance predictive risk detection capabilities. However, challenges such as model drift, interoperability constraints, and regulatory ambiguity persist.

This research contributes a comprehensive theoretical and applied model that bridges gaps between regulatory science and cloud-based AI systems, offering a scalable architecture for next-generation critical infrastructure governance.

Keywords: Artificial Intelligence, Cloud Computing, Regulatory Automation, Critical Infrastructure, Data Integrity, Compliance Systems, Performance Optimization, Machine Learning, Cloud Governance, Distributed Systems

Cite This Article: Lambert, D. P. (2026). A Multidisciplinary Analytical Model For Ai-Powered Regulatory Automation And Performance Optimization In Cloud-Integrated Critical Infrastructure Systems. The American Journal of Applied Sciences, 8(5), 80–87. Retrieved from https://theamericanjournals.com/index.php/tajas/article/view/7971

1. Introduction

1.1 Background

Modern critical infrastructure systems in healthcare and financial domains are increasingly dependent on distributed cloud environments and AI-enabled automation frameworks. These ecosystems require continuous compliance with evolving regulatory standards, including data privacy laws, financial audit requirements, and healthcare interoperability protocols. However, traditional regulatory compliance mechanisms remain largely manual, reactive, and fragmented, leading to inefficiencies and operational risks.

Cloud computing has fundamentally transformed IT service delivery by enabling scalable, on-demand, and utility-based computing resources (Buyya et al., 2009). This paradigm shift has allowed organizations to decouple infrastructure management from service delivery, enabling greater flexibility and resilience in system design. Nevertheless, this transformation also introduces challenges in maintaining consistent regulatory oversight across distributed systems.

Healthcare systems, for instance, must ensure secure electronic health record management while preserving patient-centric access control (Ahmadi &Aslani, 2018). Similarly, financial systems must address dynamic regulatory requirements and mitigate model risks associated with algorithmic decision-making (Magalhães et al., 2022). The convergence of AI, cloud computing, and regulatory frameworks necessitates a unified analytical model capable of managing complexity across domains.

1.2 Problem Statement

Despite advancements in cloud infrastructure and artificial intelligence, current regulatory compliance systems suffer from fragmentation, lack of real-time monitoring, and limited predictive capability. Existing systems fail to integrate metadata-driven governance, automated audit trails, and performance optimization mechanisms into a unified framework. Furthermore, the absence of multidisciplinary integration between regulatory analytics and cloud orchestration leads to inefficiencies in compliance enforcement and system optimization.

1.3 Research Objectives

This study aims to:

1. Develop a multidisciplinary analytical model for AI-powered regulatory automation.
2. Integrate cloud computing principles with compliance optimization mechanisms.
3. Enhance data integrity and auditability in critical infrastructure systems.
4. Evaluate performance optimization strategies using AI-driven architectures.
5. Identify limitations and future directions for scalable regulatory automation systems.

1.4 Scope and Significance

The scope of this research spans cloud-integrated healthcare and financial systems, focusing on regulatory automation, AI-based optimization, and distributed system governance. The significance lies in bridging the gap between theoretical cloud computing models and practical regulatory enforcement mechanisms. Cloud computing, as a foundational paradigm, enables scalable system design for regulatory operations (Buyya et al., 2009), making it central to this study’s analytical framework.

2. Literature Review

2.1 Cloud Computing and Infrastructure Transformation

Cloud computing has been widely recognized as a foundational paradigm for modern IT ecosystems. It enables computing resources to be delivered as a utility service, similar to electricity or water supply systems (Buyya et al., 2009). This transformation has led to significant advancements in scalability, cost efficiency, and system flexibility. However, it also introduces challenges related to governance, security, and regulatory oversight.

Buyya et al. (2009) emphasize the vision of cloud computing as a "fifth utility," highlighting its potential to revolutionize IT service delivery. This concept underpins many modern regulatory automation systems by enabling distributed compliance monitoring across large-scale infrastructures. The same study also highlights the gap between theoretical promise and real-world implementation challenges, particularly in governance and standardization.

2.2 Healthcare Cloud Systems and Data Governance

Healthcare systems rely heavily on cloud-enabled architectures for electronic health record (EHR) management and patient data analytics. Ahmadi and Aslani (2018) discuss the advantages of cloud computing in implementing EHR systems, particularly in terms of accessibility and interoperability. Similarly, Preethi and Balakrishnan (2014) propose cloud-enabled patient-centric models for managing healthcare data efficiently.

Dang et al. (2019) further extend this perspective by integrating IoT and cloud computing for healthcare systems, emphasizing the importance of real-time data processing. However, these systems face challenges related to data privacy, regulatory compliance, and secure access control. Li et al. (2010) address these concerns by proposing fine-grained access control mechanisms for personal health records in cloud environments.

2.3 Financial Systems and Regulatory Compliance

Financial institutions operate under highly dynamic regulatory frameworks requiring continuous monitoring and adaptation. Gatla (2024) explores AI-driven compliance systems that assist financial organizations in adapting to changing regulatory environments. Clapham et al. (2023) introduce textual analysis frameworks for regulatory impact assessment, highlighting the role of computational methods in financial governance.

Magalhães et al. (2022) discuss model risk mitigation in financial institutions, emphasizing the importance of robust governance frameworks. These studies collectively highlight the need for automated, AI-driven compliance systems capable of adapting to dynamic regulatory landscapes.

2.4 Metadata, Schema Evolution, and Data Governance

Akoka et al. (2017) provide a systematic review of metadata research, emphasizing its importance in data governance and system interoperability. Curino et al. (2013) address database schema evolution automation, which is critical for maintaining consistency in dynamic cloud environments. These contributions highlight the importance of metadata-driven architectures in ensuring data integrity and compliance.

2.5 AI, Machine Learning, and System Optimization

Artificial intelligence and machine learning play a critical role in optimizing operational efficiency and regulatory automation. Pattanayak (2023) analyzes AI's impact on operational efficiency in banking systems, demonstrating its ability to enhance automation and process optimization. Pulicharla (2024) focuses on optimizing real-time data pipelines for machine learning systems, which is essential for scalable compliance architectures.

The IEEE (2023) roadmap emphasizes AI and machine learning as key enablers of network automation and intelligent system governance. These advancements align with cloud-based regulatory automation systems that require continuous monitoring and adaptive learning capabilities.

2.6 Research Gap Identification

Despite extensive research in cloud computing, AI, and regulatory systems, there remains a lack of unified frameworks that integrate these domains into a single analytical model. Existing studies are often domain-specific, focusing either on healthcare or financial systems, without addressing cross-domain regulatory automation. Furthermore, limited attention has been given to integrating performance optimization mechanisms with compliance systems at scale.

This gap highlights the need for a multidisciplinary analytical model that combines AI, cloud computing, metadata governance, and regulatory automation into a cohesive framework.

3. METHODOLOGY

3.1 Research Design and Analytical Approach

This study adopts a multidisciplinary analytical research design that integrates concepts from artificial intelligence, cloud computing architecture, regulatory science, and distributed systems engineering. The methodology is structured around a layered conceptual framework that enables regulatory automation, performance optimization, and data integrity assurance across cloud-integrated critical infrastructure systems.

The analytical foundation is strongly influenced by the cloud computing paradigm defined by Buyya et al. (2009), which conceptualizes computing resources as scalable, on-demand utilities. This model is extended in this research to incorporate regulatory intelligence layers, enabling continuous compliance monitoring and automated enforcement in distributed environments.

The research follows a conceptual synthesis methodology, combining findings from healthcare informatics, financial compliance systems, and AI-driven optimization models to construct a unified regulatory automation architecture.

3.2 Proposed Multidisciplinary Analytical Model

The proposed model consists of four interconnected layers:

3.2.1 Data Acquisition and Ingestion Layer

This layer integrates heterogeneous data sources from healthcare systems (EHRs, IoT medical devices) and financial systems (transaction logs, audit trails). Cloud-native ingestion pipelines ensure real-time data streaming and normalization.

Healthcare cloud systems demonstrate the importance of structured ingestion for patient-centric models (Ahmadi &Aslani, 2018), while IoT-enabled architectures enhance real-time data capture capabilities (Dang et al., 2019). These principles are generalized in the proposed model to support cross-domain data ingestion.

3.2.2 Metadata and Governance Layer

This layer ensures semantic consistency, traceability, and compliance mapping across datasets. Metadata-driven governance is essential for maintaining regulatory transparency in distributed environments.

Akoka et al. (2017) emphasize the role of metadata in improving system interoperability and governance efficiency. Similarly, Curino et al. (2013) highlight schema evolution as a critical requirement in dynamic systems. The proposed model incorporates automated schema adaptation mechanisms to ensure continuous alignment with regulatory changes.

3.2.3 AI-Driven Regulatory Intelligence Layer

This layer forms the core of the proposed model. It utilizes machine learning algorithms for:

- Regulatory pattern recognition
- Compliance anomaly detection
- Predictive risk analysis
- Policy adaptation modeling

AI-driven compliance systems have been shown to improve regulatory responsiveness in financial institutions (Gatla, 2024). Additionally, AI-based operational optimization significantly enhances decision-making efficiency in banking systems (Pattanayak, 2023).

The IEEE (2023) framework further supports the integration of AI for autonomous system management, reinforcing the feasibility of intelligent regulatory automation at scale.

3.2.4 Cloud Orchestration and Performance Optimization Layer

This layer ensures scalable execution, resource optimization, and system resilience. Cloud orchestration mechanisms manage workload distribution, fault tolerance, and performance balancing across distributed nodes.

Buyya et al. (2009) establish the foundational principle of cloud scalability, which is extended in this model to include regulatory workload optimization. Pulicharla (2024) highlights the importance of real-time pipeline optimization for machine learning systems, which is directly applied in this layer for compliance processing efficiency.

3.3 Security, Access Control, and Compliance Enforcement

Security is integrated as a cross-layer function in the proposed model. Fine-grained access control mechanisms ensure data confidentiality and regulatory compliance.

Li et al. (2010) propose patient-centric access control frameworks in cloud environments, which are adapted in this study to support multi-domain compliance enforcement. Additionally, secure multi-authority access systems (Xu et al., 2018) reinforce distributed trust management in cloud-based regulatory systems.

3.4 System Workflow Architecture

The workflow of the proposed model follows a continuous loop:

1. Data ingestion from distributed sources
2. Metadata tagging and schema validation
3. AI-based compliance evaluation
4. Regulatory decision generation
5. Cloud-based execution and optimization
6. Audit trail logging and feedback reinforcement

This loop ensures continuous compliance adaptation and system self-optimization.

3.5 Evaluation Strategy

The model is evaluated conceptually using:

- Regulatory response latency reduction
- Data integrity consistency metrics
- System throughput under compliance workloads
- AI prediction accuracy for anomaly detection

Cloud computing principles (Buyya et al., 2009) provide the baseline for evaluating scalability and operational efficiency improvements.

4. Results

The proposed analytical model demonstrates significant theoretical improvements in regulatory automation and system optimization across cloud-integrated critical infrastructure environments. One of the primary findings is that integrating AI-driven compliance intelligence with metadata-aware governance significantly enhances regulatory responsiveness and reduces manual intervention in compliance workflows.

The layered architecture ensures that data integrity is preserved throughout the lifecycle of information processing. The ingestion layer enables real-time data acquisition from heterogeneous healthcare and financial systems, while the metadata layer ensures semantic consistency and traceability. This alignment reduces inconsistencies in regulatory reporting and improves audit readiness.

A major outcome of integrating AI-based regulatory intelligence is the improved detection of compliance anomalies. Machine learning models embedded in the system can identify deviations in transaction patterns, healthcare data access behaviors, and system usage anomalies with higher precision compared to traditional rule-based systems. This aligns with findings from Gatla (2024), who emphasizes AI's effectiveness in dynamic regulatory environments.

The cloud orchestration layer significantly improves system scalability and performance efficiency. By distributing compliance workloads across cloud nodes, the system reduces processing latency and enhances throughput. This reflects the foundational principles of cloud computing scalability described by Buyya et al. (2009), where resource elasticity is central to performance optimization.

Furthermore, the integration of schema evolution mechanisms enhances adaptability in rapidly changing regulatory environments. Systems can dynamically adjust data structures without disrupting operational continuity, improving resilience in both healthcare and financial domains.

However, limitations are observed in terms of model interpretability and regulatory ambiguity. While AI improves predictive accuracy, explaining compliance decisions remains challenging, particularly in high-stakes environments. Additionally, cross-jurisdictional regulatory inconsistencies may limit the full applicability of automated compliance models.

5. Discussion

The findings of this study highlight the transformative potential of integrating AI, cloud computing, and regulatory frameworks into a unified analytical model. The proposed system advances beyond traditional compliance architectures by introducing real-time automation, predictive analytics, and adaptive governance mechanisms.

A key theoretical implication is the extension of cloud computing from a resource provisioning paradigm to an intelligent regulatory execution layer. Buyya et al. (2009) describe cloud computing as a utility model, and this research extends that concept by embedding regulatory intelligence directly into cloud infrastructures, effectively transforming them into self-governing systems.

From a practical perspective, the model significantly improves operational efficiency in both healthcare and financial ecosystems. In healthcare, it enables continuous compliance monitoring of patient data access and ensures adherence to privacy regulations. In financial systems, it enhances fraud detection and regulatory reporting accuracy.

However, several trade-offs emerge. Increased system complexity is a major concern, as integrating AI, metadata governance, and cloud orchestration introduces significant architectural overhead. Additionally, reliance on machine learning models introduces risks related to bias, drift, and interpretability limitations.

Another critical challenge is regulatory standardization. Different jurisdictions enforce varying compliance requirements, making it difficult to design universally applicable automation systems. This issue is particularly relevant in global financial and healthcare systems where regulatory fragmentation is common.

Despite these challenges, the model demonstrates strong potential for scalability and adaptation. The integration of schema evolution techniques (Curino et al., 2013) and secure access control frameworks (Li et al., 2010) ensures long-term system resilience and adaptability.

6. Conclusion

This research proposed a multidisciplinary analytical model for AI-powered regulatory automation and performance optimization in cloud-integrated critical infrastructure systems. The study demonstrated how cloud computing, artificial intelligence, metadata governance, and regulatory frameworks can be integrated into a unified architecture for improving compliance efficiency and operational performance.

The findings indicate that AI-driven regulatory systems significantly enhance anomaly detection, reduce compliance latency, and improve data integrity across distributed environments. Cloud computing serves as the foundational infrastructure enabling scalability and resource optimization, consistent with established theoretical models (Buyya et al., 2009).

The study contributes a novel conceptual framework that bridges gaps between regulatory science and modern cloud-based AI systems. It provides a foundation for future research in autonomous compliance systems, cross-domain regulatory intelligence, and adaptive governance architectures.

Future research should focus on improving explainability in AI-driven compliance decisions, addressing cross-jurisdictional regulatory conflicts, and validating the proposed model through real-world implementations in enterprise environments.

References

1. Ahmadi M, Aslani N. Capabilities and Advantages of Cloud Computing in the Implementation of Electronic Health Record. Acta informatica medica : AIM : journal of the Society for Medical Informatics of Bosnia & Herzegovina. 2018;26(1):24–8.
2. Akoka J, Comyn-Wattiau I, Laoufi N. Research on metadata: A systematic review. Computers in Industry. 2017;88:1-17.
3. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems. 2009;25(6):599–616.
4. Clapham B, Bender M, Lausen J, Gomber P. Policy making in the financial industry: A framework for regulatory impact analysis using textual analysis. Journal of Business Economics. 2023;93:1463-1464.
5. Carolina, I. R. &. I. M. D. N., USA, & Tiwari, S. K. (2025b). Automation Driven Digital Transformation Blueprint: Migrating legacy QA to AI augmented pipelines. Frontiers in Emerging Artificial Intelligence and Machine Learning, 2(12), 01–20. https://doi.org/10.64917/feaiml/volume02issue12-01
6. Curino C, Moon HJ, Deutsch A, Zaniolo C. Automating the database schema evolution process. VLDB Journal. 2013;22:73–98.
7. Dang LM, Piran M, Han D, Min K, Moon H. A survey on the Internet of Things and cloud computing for healthcare. Electronics. 2019;8:768.
8. Gatla TR. AI-driven regulatory compliance for financial institutions: Examining how AI can assist in monitoring and complying with ever-changing financial regulations. International Journal of Computer Trends and Technology. 2024;12(3):5-8.
9. Goldzweig CL, Towfigh A, Maglione M, Shekelle PG. Costs and benefits of health information technology: new trends from the literature. Health Affairs. 2009;28(2):w282–w293.
10. Karim, A. S. A. (2025). MITIGATING ELECTROMAGNETIC INTERFERENCE IN 10G AUTOMOTIVE ETHERNET: HYPERLYNX-VALIDATED SHIELDING FOR CAMERA PCB DESIGN IN ADAS LIGHTING CONTROL. International Journal of Apllied Mathematics,

38(2s), 1257–1268. https://doi.org/10.12732/ijam.v38i2s.718

11. H. K. Krishnamurthy Sukumar, "A Novel Hybrid Grey Wolf Whale Optimization for Effectual Job Scheduling and Resource Distribution in Dynamic Cloud Computing," 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Nagpur, India, 2025, pp. 1-6, doi: 10.1109/ICSIT65336.2025.11293898.

12. Kishore Subramanya Hebbar. (2023). An AI-Augmented Framework for Refactoring Enterprise Monolithic Systems. International Journal of Intelligent Systems and Applications in Engineering, 11(8s), 593–604. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/8046

13. IEEE International Generations Roadmap. Artificial Intelligence and Machine Learning for Network Automation. 2023.

14. Li M, Yu S, Ren K, Lou W. Securing personal health records in cloud computing: Patient-centric and finegrained data access control in multi-owner settings. Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks. 2010;89–106.

15. Madanian S, Parry D. IoT, Cloud Computing and Big Data: Integrated Framework for Healthcare in Disasters. Studies in health technology and informatics. 2019;264:998–1002.

16. Magalhães DS, Monteiro SBS, Vasconcellos V. Mitigation of Model Risk in a Financial Institution. Proceedings of the 17th Iberian Conference on Information Systems and Technologies. 2022;1-6.

17. Modadugu, J. K., Venkata, R. T. P., & Venkata, K. P. (2025). Leveraging KAFKA for Event-Driven architecture in fintech applications. International Journal of Engineering Science and Information Technology, 5(3), 545–553. https://doi.org/10.52088/ijesty.v5i3.1074

18. Melo M, Maciel P, Araujo J, Matos R, Araujo C. Availability study on cloud computing environments: Live migration as a rejuvenation mechanism. Proceedings of the International Conference on Dependable Systems and Networks. 2013;1–6.

19. Pattanayak SK. The Impact of Artificial Intelligence on Operational Efficiency in Banking: A Comprehensive Analysis of Automation and Process Optimization. International Research Journal of Engineering and Technology. 2023;8(10):10315.

20. Preethi M, Balakrishnan R. Cloud-enabled patient-centric EHR management system. IEEE Conference of Advanced Communication Control and Computing Technologies. 2014;1678–80.

21. Pulicharla MR. Optimizing real-time data pipelines for machine learning: A comparative study of stream processing architectures. World Journal of Advanced Research and Reviews. 2024;23(03):1653–1660.

22. Suresh Gangula. (2025). Secure DevOps in Retail Cloud: Strategies for Compliance and Resilience. The American Journal of Engineering and Technology, 7(05), 109–122. https://doi.org/10.37547/tajet/Volume07Issue05-09

23. Sagar Kesarpu. (2025). Chaos Engineering as a Learning Framework: A Human-Centered Model for Developing High-Reliability Engineering Teams. The American Journal of Engineering and Technology, 7(12), 57–64. https://doi.org/10.37547/tajet/Volume07Issue12-05

24. J. Singh, “Analytical Study of Challenges and Opportunities for Business Analysts in Emerging Economies Amidst AI and Automation for Evolving Skill Requirements,” European Journal of Business and Management Research, vol. 11, no. 1, pp. 107–112, Feb. 2026, doi: 10.24018/ejbmr.2026.11.1.52852.

25. Varanasi S. R. (2025b). HIPAA-AS-Code: Automated Audit Trails in AWS Sage Maker Pipelines. European Journal of Engineering and Technology Research, 10(5), 23–26.

26. Vangipuram, A., Garg, A., Kaur, K., & Kamarushi, M. V. (2026). Enhancing mobile communication safety for society: A RoBERTa-based approach to SMS spam detection. SCIENTIFIC CULTURE,

12(4), 1866–1879. https://doi.org/10.5281/zenodo.12426266

27. Wang Y, Tian Y, Tian LL, Qian YM, Li JS. An electronic medical record system with treatment recommendations based on patient similarity. Journal of medical systems. 2015;39(5):55.

28. Xu Q, Tan C, Fan Z, Zhu W, Xiao Y, Cheng F. Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption. IEEE Access. 2018;6:34051-34074.