International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Powered Governance with Modern Data Engineering for Regulatory Excellence in Healthcare and Fintech

Mani Kanta Pothuri

ManikantaPothuri1@gmail.com

Abstract:
Healthcare and FINTECH domains are rapidly digitalizing operations. The domains are taking bigger strides to address the intense demand for data-driven, intelligent, and reliable processes complying with regulations. These industries manage extremely sensitive content, including personal information of individuals and financial details. Conventional compliance methods struggle to keep pace with the dynamic data management regulations due to substantial dependency on human intervention. This paper attempts to develop a framework for integrating artificial intelligence (AI) based data governance into dataflow as an initiative to implement regulatory compliance into an initiative-taking approach rather than addressing incidents after their occurrence. The process involves exploring AI capabilities to flag random events automatically by monitoring compliance as an ongoing process to make transparent data-driven decisions and demonstrate scalability in enforcing policies.
Metadata-supported dataflows, lineage, and frameworks are added to support operations to leverage AI capabilities. Integration of intelligent data management frameworks into advanced data analytics technology processes comprehensively enables agile operations, thereby entrusting stakeholders strategically. The approach alters data strategy use from a good to have to a check-box level for enhancing digital integrity and enterprise to an organizational level commitment in this digital era.

Keywords: AI-powered governance for FINTECH, Data engineering regulations, Modern data engineering in healthcare.

1. Introduction

AI and advanced data infrastructure are revolutionary technologies generating new ways for highly regulated industrial domains. Healthcare institutions and FINTECH organizations manage overly sensitive data, including personal information and financial transaction information. Regulators, associates, and end-users continuously scrutinize the domain, indicating a demand to deploy sophisticated data engineering technologies. Conventional regulatory frameworks and data management methods face challenges in keeping up with dynamic challenges. This is due to the consideration of data governance as an external verification metric.

Using advanced data engineering and anomaly detection as a code design element with an automated and initiative-taking approach, enticed with dataflow holistically is effective. AI is an innovative digital advancement creating scope for monitoring and dynamic policy enforcement [1]. Integrated with a cloud data platform, AI supports adaptive compliance and addresses modern-day data demands while simultaneously creating a potential risk mitigation layer to empower modern-day data operations.

2. Regulatory landscapes of Healthcare and FINTECH

Healthcare

Healthcare pursuits are going through a maze of overlapping regulations.

- HIPAA(Health Insurance Portability and Accountability).
- GDPR (General Data Protection Regulations) for complying with international data protection guidelines and best practices in data management.
- Other state-level guidelines also extend data security measures above federal mandates [2]. Following ethical standards in processing and using personal health information is important for entrusting end-users and mitigating legal risks.

Key Challenges

- Privacy management while sharing data for clinical studies.
- Managing dynamic user consent across digital dataflows.
- Ensuring fairness of AI diagnostics with precision and transparency.

Digital sophistication like health records (EHR), wearable sensors, digital genome coding domains, and diagnostics imaging using AI enhances the data size and complexities simultaneously [3]. Evolving forms of AI introduce novel opportunities for governance and data privacy management.

FINTECH

The FINTECH domain needs to abide by the complex regulatory acts and guidelines.

- GLBA (Gramm-Leach-Bliley Act) enforces guidelines for financial institutions to elicit data transactions and protect sensitive customer data.
- BSA (Bank Secrecy Act) and rules mandate Anti-Money Laundering (AML) compliance.
- CFBP(Consumer Financial Protection Bureau) monitors fairness and transparency in credit scoring and loan disbursement.
- PCI DSS (Payment Card Industry Data Security)standards.
- State laws like CCPA(California Consumer Privacy) and other local guidelines also apply to organizations, according to data owners and transactions involved.
- GDPR and other cross-border data laws guide international financial data and operations.

Key challenges

- Executing compliance for dynamic data in digital payments, loans, and investments.
- Fraud detection across substantial transactions at granular levels.
- Ensuring transparency in credit scores and loan processing with unbiased algorithmic decisions.

FINTECH companies need a striking balance in providing an esteemed customer experience and regulatory mandates while addressing the rapid pace of market dynamics.

3. AI-powered Governance: Use case analysis

Healthcare

High-level AI governance in the healthcare domain includes operationalization of trust by entwining safety, security, and visibility into technologies empowering healthcare innovation [4]. The process involves focusing on ascertaining high-quality data inputs required to accomplish and sustain outcomes of care practices as depicted in **Figure 1**

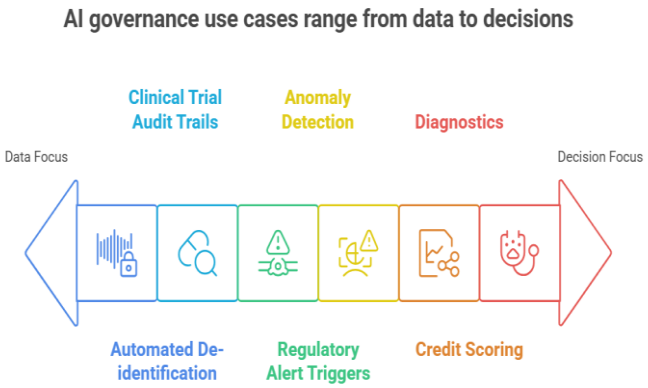

Figure 2: AI-powered Governance: Use case analysis

PHI(Personal Health Information) redaction: Using AI to detect and redact the usernames, time stamps, spatial and contextual elements from patient documents dramatically reduces the privacy issues in data engineering or transactions. Automated redaction for making AI defensive to deliver valuable clinical and commercial details while keeping security and compliance as paramount.

NLP(Natural language processing): NLP-based clinical trials empower the extraction of an extensive metadata framework from care providers' documents, trial plans, and patient reviews. This ensures transparency in documentation, consent management, divergence from regular therapeutic paths, and results. NLP for compliance management for Fairness in ensuring that data and AI algorithms are free from discrimination and bias by extracting critical compliance indicators.

Fair AI diagnostics: AI effectively supports in the interpretation of images and therapy suggestions. Reasoning suggested that therapeutic methods enable care providers to review and patients for insights is useful for preventing ambiguities and promoting fairness [5]. Implementing SHAP(Shapely Additive Elicitations and interpretable agnostic descriptions serves the purpose efficiently. Using AI-motivated DSS (Decision Support Systems) for expedition and accuracy in recommending the best therapeutic processes.

FINTECH

AI governance in FINTECH refers to different systems, principles, and process controls ascertaining that the technology is improved, deployed, and observed continuously [6]. The process emphasizes managing ethical standards and ascertaining compliance while acquiring sensitive content and reducing operational challenges depicted in **Figure 3**.

Detecting anomalous transactions: Behavioral patterns, ensuring AI decision-making transparency and legitimacy supports in analyzing the user trends across accounts and spatial inputs for detecting random and red flag activities. The models can adapt to the dynamics of financial processes over a period [7]. These generate new tactics for the detection of fraud and alerting organizations to act. AI is capable of accounting for different variables like buying frequency, location, and value of each transaction. Embedding AI-powered frameworks in cyber protection architecture allows FINTECH companies to expedite the detection of threats and gaps in networks.

Evaluating credit risks: AI algorithms support analyzing digital finance transaction trends and notify about suspicious activities continuously. These allow for securing user data and funds [8]. This real-time activity ascertains compliance by substituting regular statistical models for assessing credit score using income and transactional history. The time and efforts involved in the preparation of reports is reduced using AI. This streamlines the approval processes. Using supervised learning models for securing sensitive customer data and adaptable AI advancements with emerging regulations.

Event-based compliance alerts: Implementing compliance signal routing for risk management using AI models and complications and promoting ethical practices to promote fairness in results. AI can reduce human errors and bias in interpretation of data [9]. This strategically empowers compliance with industrial guidelines

and dynamics. Efficient data governance embedded in models enhances transparency and visibility to managers for making decisions. This adaptability bolsters wide-ranging FINTECH tools.

4. Advanced data engineering components embedded with AI

Empowering smart data governance for promoting resilient operations in organizations requires a visible data management framework.

- Using real-time data pipelines allows continuous governance and taking actions on random transactions, and freezing accounts.
- Using Data lakes and time travel algorithms allows collaboration of transactional productivity with audit results to conduct retrospective analysis.
- Using Metadata and lineage consistency supports transparent transactions according to data origin, transactions, and transformation with user details and time stamps.
- Integrating data models with continuous and unstructured data guided by decision governance rules generates results directly applicable to operational analytics.

5. AI ARCHITECTURE OVERVIEW

Healthcare stack: The ingestion layer of the AI compliance framework stack for the healthcare domain consists of connectors such as HL7 and FHIR APIs according to industrial standards. The storage layer consists of a data lake house established with PHI (Personal Health Information) segmentation and a governance layer established with role-based accessibility rules, data masking, and consent registry [10]. The AI layer contains tailored data models with an audit trail management system. Real-time data event scanning, accompanied by compliance dashboards, completes the system to implement an AI-based healthcare data governance architecture as in **Table 1**.

Layer	Tools/Technologies	Purpose
Ingestion	HL7/FHIR, APIs	Interoperable health data
Storage	Snowflake, Delta Lake	Secure, scalable PHI storage
Governance	Immuta, Collibra	Privacy controls, access policies
AI/ML	Azure ML, SAS	De-identification, predictions

Table 2: AI Architecture overview Healthcare stack

Fintech Stack: Data ingestion layer for FINTECH systems is equipped with Kafka streams and CDC (change data capture) controls. The storage mechanism involves cloud native data warehouses and continuous lineage tag addition [11]. Governance includes customer identification schema validation software and policy-motivated access rules enforced. AI layer includes a credit risk data engine coupled with explainability facilitations. Anomalous data are detected, and alerts are shared, including audit log details by the system as in **Table 2**.

Layer	Tools/Technologies	Purpose
Ingestion	Kafka, CDC streams	Real-time event data
Storage	Snowflake, S3	Historical and operational data
Governance	Atlan, Informatica	KYC schema enforcement, masking
AI/ML	DataRobot, Python	Fraud models, risk analytics

Table 3: AI Architecture overview Healthcare stack

6. PERFORMANCE METRICS AND COMPLIANCE OF AI-POWERED GOVERNANCE

Performance metrics

Data quality metrics: Measuring the performance of AI-powered healthcare and FINTECH data governance, including compliance certification initiatives, is important to demonstrate value, increase trust, and ascertain responsible AI according to the consistency score. The capability to completely trace data and its lineage. Anomaly detection metrics entice with high performance by depicting errors present in specific areas, resulting in regulatory compliance.

Accuracy and efficiency: The detection rates of fraudulent and non-compliant transactions are checked according to sensitivity. Recall rate of fraud events identified by AI accurately [12]. Specificity is the extent to of compliant events are identified accurately. False positives are known as Type I errors, as the extent of compliant events reported as non-compliant leads to operational issues. The false negatives that occurred are Type-II errors, indicating proportion of non-compliant events left undetected. Precision levels of flagged events by AI are verified for these error type classification F1 score is the harmonic mean value calculated for precision and recall events to assess efficiency and accuracy of process.

Human intervention reduced: The percentage of human efforts reduced by AI automation is measured. Efficiency is the processing time of AI to study data and generate flags, and accuracy compared to AI-generated alerts [13]. Throughput levels are measured by checking number of records or transactions per second.

Bias mitigation efficiency: The fairness metrics are quantified as AI governance system produces equitable results across various groups [14]. This is effective in avoiding bias and discrimination. The frequency of successful reduction of bias using model balancing is measured for the success rate.

7. COMPLIANCE METRICS

Audit transparency score: Success levels of AI AI-motivated system to verify user identities and flag ambiguous transactions according to regulations depict AML/KYC accuracy metrics.

Ethical fit index: Bias in treatment data models could result in a lack of accuracy due to data skewness. AI governance frequency and accuracy are measured by noticing potential biases in AI models and data processes.

Access compliance and automation levels: Verifying access to PHI and logging in compliance with regulations, exclusively to HIPAA, GDPR.

Risks and mitigations

Risk	Healthcare Example	Fintech Example	Mitigation
Bias in AI	Diagnosis errors	Credit score inaccuracy	XAI frameworks, diverse data
Data Drift	Genomics shifts	Market volatility	Model retraining, CI/CD pipelines
Policy Mismatch	Local consent laws	Cross-border AML gaps	Dynamic policy engines

Table 4: Domain -wise Risks and mitigations

Healthcare: AI bias is the primary risk involved with prioritizing or exclusion users due to data skewness. This is mitigated by conducting fairness audits continuously. Consent manager issues may occur if the opt-out by patients is not applied consistently [15]. This is mitigated by deploying a centralized event log system, and an application interface plug-in is added as in **Table 3**.

FINTECH: Algorithms may unintentionally deny marginalized groups. Implementing interpretable models and fairness limitations is effective for mitigating this risk. Alert fatigue may occur due to many false positives in fraudulent systems. Using a tiered alerting algorithm allows alerting according to context and relevance scores as in **Table 3**.

8. FUTURE RECOMMENDATIONS

Investing in explainable AI: Healthcare and FINTECH organizations are to invest in SHAP technologies for further improvement in data modeling and decisions [16]. Building governance into dataflow and inclusion in CI/CD, as well as ML operations for efficiency. Standardizing the FHIR ingestion and masking is important. Building data lineage followed by anonymization enhances model efficiency.

Digital twins and synthetic data: Creating a simulated environment mirroring real systems, such as hospital data structure, derisks the experimentation issues and unveils possible ethical or functional gaps before deployment [17]. Synthetic data is created using statistical modeling or generative AI for training models in regulated industries. These reduce compliance frictions and maintain the integrity of analytics. A combination of these techniques allows edge-case identification and prepares systems for regulatory compliance.

Federated learning(FL) for AI-privacy awareness: Using Federated learning allows organizations and edge devices to train models in collaboration without sharing raw content. Data stays locally while the model is updated across organizations by protecting PHI [18]. Combining differential privacy and multi-party computation, encryption, and FL allows compliance alignment and decentralized AI. These are effective for global collaboration of legal data transactions without restrictions.

9. CONCLUSION

AI-integrated governance empowered by advanced data engineering creates a way for excelling in operations of Healthcare and FINTECH domains, following regulations stringently. Comparing domain-specific technology deployments in healthcare and FINTECH illustrated AI capabilities in automating sensitive data protection, real-time fraud identification, and consent enforcement using advanced data analysis architecture. Alignment of infrastructure, intelligence, and policy organizing goes beyond compliance to develop secure, ethically trusted, and standard system designs. This is beyond a technology shift and transforms operations into said domains. Transparency and trust function as architectural principles for automation and resilience. The fusion of AI governance and advanced data engineering offers a future with regulatory excellence. In conclusion, technology is considered a catalyst for smarter and secure innovation.

REFERENCES:

[1] R. Verma and S. Jana, "AI-Powered Governance: Shaping the Future Landscape of Corporate Governance," SSRN, vol. 1, no. 1, pp. 1-26, 2025.
[2] A. Ahmadi and N. R. Ganji, "AI-Driven Medical Innovations: Transforming Healthcare through Data Intelligence," International Journal of BioLife Sciences (IJBLS), vol. 2, no. 2, pp. 132-142, 2023.
[3] S. G. Chawda and D. H. Fatima, "Revolutionizing Healthcare: The Power and Potential of AI Enablement," Journal of Nonlinear Analysis and Optimization, vol. 14, no. 2, pp. 1-11, 2023.
[4] K. Dubey, M. Bhowmik, A. Pawar, M. K. Patil, P. A. Deshpande and S. S. Khartad, "Enhancing Operational Efficiency in Healthcare with AI-Powered Management," International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), vol. 1, no. 1, pp. 1-7, 2023.
[5] J. David, "Revolutionizing Biomedical Engineering: AI-Driven Medical Devices in Cloud-Based Healthcare Systems," Researchgate, vol. 1, no. 1, pp. 1-8, 2024.
[6] C. Challoumis, "The Landscape of AI in Finance," XVII international scientific conference, vol. 1, no. 1, pp. 109-144, 2024.
[7] D. Bihani, B. C. Ubamadu and A. I. Daraojimba, "Integrating Blockchain with AI: A Data-Driven Model for Secure, Scalable Decentralized Finance (DeFi) Systems," World Journal of Innovation and Modern Technology, vol. 9, no. 5, pp. 1-28, 2025.
[8] O. Onesi-Ozigagun, Y. J. Ololade, N. L. Eyo-Udo and D. Oluwaseun, "AI-driven biometrics for secure fintech: Pioneering safety and trust," International Journal of Engineering Research Updates, vol. 6, no. 2, pp. 1-12, 2024.

[9] V. V. R. M. Bokka, "Transforming US banking: Leveraging AI-powered technology compliance platform (TCP) for regulatory excellence," World Journal of Advanced Research and Reviews, vol. 25, no. 1, pp. 2174-2187, 2025.
[10] S. Patil and H. Shankar, "Transforming Healthcare: Harnessing the Power of AI in the Modern Era," International Journal of Multidisciplinary Sciences and Arts, vol. 2, no. 2, pp. 60-70, 2023.
[11] H. Chikri and M. Kassou, "Financial Revolution: Innovation Powered by FINTECH and Artificial Intelligence," Journal of Theoretical and Applied Information Technology, vol. 102, no. 9, pp. 1-13, 2024.
[12] A. Dodda, "AI Governance and Security in Fintech: Ensuring Trust in Generative and Agentic AI Systems," American Advanced Journal for Emerging Disciplinaries, vol. 1, no. 1, pp. 1-14, 2023.
[13] S. Obeng, T. V. Iyelolu, A. A. Akinsulire and C. Idemudia, "The Transformative Impact of Financial Technology (FinTech) on Regulatory Compliance in the Banking Sector," World Journal of Advanced Research and Reviews, vol. 23, no. 1, p. 2008–2018, 2024.
[14] N. N. Ridzuan, M. Masri, M. Anshari, N. L. F. and M. Syafrudin, "AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility," Information, vol. 15, no. 8, pp. 1-30, 2024.
[15] A. Thirunagalingam, "AI-Powered Continuous Data Quality Improvement: Techniques, Benefits, and Case Studies," SSRN, vol. 1, no. 1, pp. 1-9, 2025.
[16] S. Paleti, "Data-First Finance: Architecting Scalable Data Engineering Pipelines for AI-Powered Risk Intelligence in Banking," SSRN, vol. 1, no. 1, pp. 1-27, 2025.
[17] R. Para, R. Bhatia and S. Sandiri, "AI-Powered Financial Digital Twins: The Next Frontier in Hyper-Personalized, Customer-Centric Financial Services," Journal of Next-Generation Research 5.0, vol. 1, no. 4, pp. 1-18, 2025.
[18] A. Ramrakhyani and N. K. Shrivastava, "Artificial Intelligence: Revolutionizing the Future of Fintech," Commerce Research Review, vol. 1, no. 2, pp. 1-13, 2024.