The Review Of
DIABETIC
STUDIES OPEN ACCESS

AI-Enhanced Data Governance: Automating Compliance In Healthcare Analytics Platforms

Bindu Madhavi Mangalampalli
Data Engineering Architect Team Lead, bindooo.madhaveee.3@gmail.com, ORCID ID: 0009-0001-1070-3856

Abstract
Automating compliance with complex, evolving, multi-jurisdictional privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, remains an open problem. Current solutions obtain some level of compliance but do not meet the complete requirements of these regulations. Advances in hardware and software support the argument that a new architectural approach is feasible. A broad architecture for AI-enhanced data governance has already been developed, clearing the way to addressing compliance automation in the context of Healthcare Analytics Platforms. Data governance is a primary focus; the deployment of such platforms tends to shift the cost–benefit structure of using personal data in data analytics. However, privacy laws remain fragmented and complex, and ensuring actual compliance still requires a high level of effort. AI-enhanced data governance has been proposed as a way to reduce the burden of performing the tedious, low-value tasks that support compliance. A simplified conceptual model of a Healthcare Analytics Platform highlights the areas of responsibility required to maintain privacy.
Healthcare service providers (HSPs) need to perform data analysis tasks that may require sharing the data they collect with external third parties. Using anonymization techniques may not be sufficient to protect the information of users of HSPs. Consequently, legislation such as HIPAA and the Personal Information Protection and Electronic Documents Act (PIPEDA) concentrates on how the data held by a HSP is used and by whom. AI-enhanced data governance can reduce the workload associated with ensuring compliance with such laws.
Keywords: AI-Enhanced Data Governance, Healthcare Analytics Platforms, Automated Privacy Compliance, Multi-Jurisdictional Data Regulation, Regulatory Technology (RegTech) in Healthcare, Data Usage Control Frameworks, Compliance Automation Architecture, Healthcare Data Privacy Management, Cross-Border Health Data Governance, Privacy-by-Design Implementation, Data Access and Accountability Controls, Secure Third-Party Data Sharing, Anonymization and De-Identification Techniques, Legal Interoperability Frameworks, Healthcare Service Provider (HSP) Compliance, AI-Supported Audit and Monitoring, Cost–Benefit Optimization in Data Governance, Policy-Aware Data Processing Systems, Privacy Risk Mitigation Models, Intelligent Compliance-as-a-Service Systems.

1. Introduction

Healthcare analytics platforms collect, store, and process sensitive patients' personal health information (PHI). They are subject to a multitude of data governance, regulatory, and compliance requirements to protect PHI against data misuse, data breach, or unauthorized access. Manual data governance is prone to error, time-consuming, labor-intensive, and costly. The architecture of AI-enhanced data governance automates the monitoring and auditing of compliance in large-scale multi-cloud healthcare analytics platforms. Its implementation leverages AI and machine learning technology and sensible utilization of a platform's own data. Empirical experiments have shown that it is feasible and efficient to enhance data governance with the aforementioned architecture and thus automate compliance in healthcare analytics platforms.
The regulatory landscape of healthcare analytics platforms is chaotic, with complex dependencies and dozens of constantly changing requirements. Fulfillment of these requirements is essential in healthcare analytics platforms as they process sensitive PHI and engage with various parties, including patients, service providers, healthcare providers, and insurance companies. The sheer complexity and continuously evolving nature of healthcare analytics require a tremendous labor investment to ensure compliance. This has led to a growing interest in automating data governance, compliance monitoring, and compliance auditing with AI-based approaches and solutions. However, it remains a cumbersome task that requires enormous amounts of engineering with limited data-driven guidance or assistance. Services provided by the healthcare analytics platform undergo a multilevel approval process, which includes eliciting and approving the compliance of a requested service. When a third-party data source is requested for integration or any integration is temporarily opened or designed into the healthcare analytics platform, the security and privacy compliance of the new or modified connection with healthcare data must also be approved.

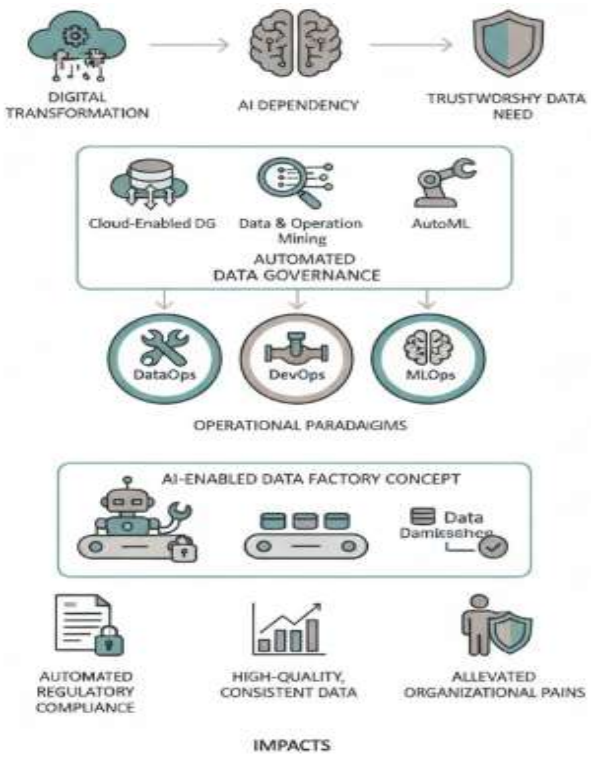
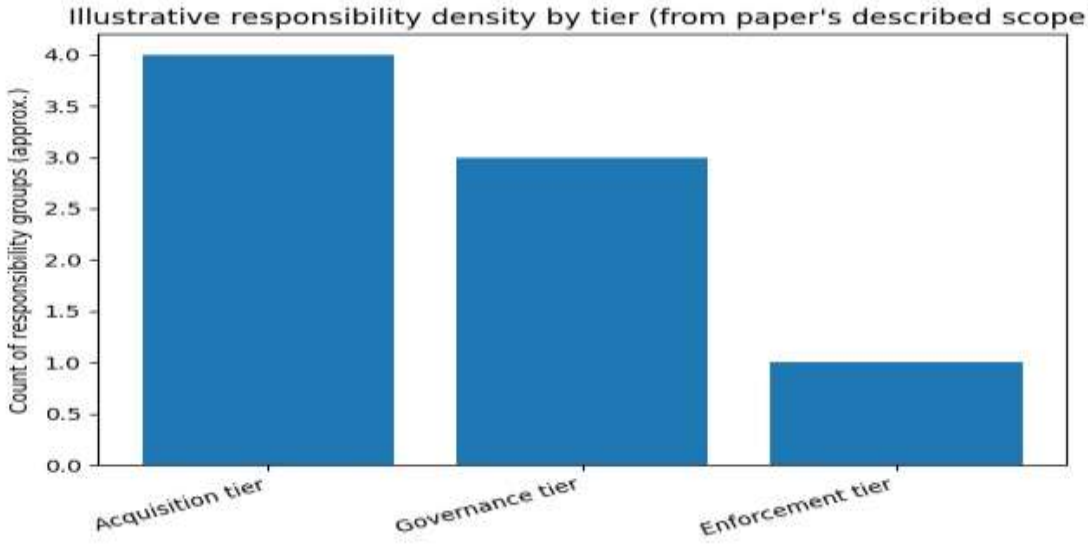


Fig 1: The AI-Enabled Data Factory: Automating Governance and Regulatory Compliance in Healthcare Analytics Platforms

1.1. Data Governance in the Era of AI: A Comprehensive Overview

Ongoing digital transformation is creating a "new normal" for how people live and work. Algorithms are reshaping user experiences, leading organizations to become increasingly dependent on artificial intelligence (AI). However, as organizations rely more on data, the need for trustworthy data also grows. There is an obvious urge to establish data governance that supports automated compliance for healthcare analytics platforms. Regulatory frameworks are becoming stricter, and organizations are being held accountable for failure to comply with regulations and misusing personal data.

New technologies, frameworks, and paradigms such as the Cloud enabled Data Governance framework, the Data and Operation Mining techniques based Intelligent Data Governance framework, and AutoML assist in automating data governance. With the advent of DataOps, along with DevOps and MLOps, the need to automate the data-driven decision-making process with a strong focus on delivering accurate, consistent, and high-quality data has increased. Organizations in each domain require domain-specific DataOps to deliver high-quality, compliant data. Automated Data Governance is necessary to alleviate these pains. AI is playing a key role in automating the compliance of healthcare analytics platforms by designing an AI-enabled Data Factory concept.



2. Background and Rationale

The maintenance of high-quality data in Healthcare Analytics Platforms (HAPs) is a fundamental requirement to drive business success. Data Governance (DG) enables the establishment of policies, controls, and processes that ensure the integrity, availability, maintainability, and security of data. In the medical domain, a DG framework

must also ensure that data is compliant with the regulatory requirements imposed by the authorities for the storage and processing of sensitive information.

Recent research works have introduced a novel architecture of AI-Enhanced DG in the context of HAPs that relies on purpose-aware virtualization of sensitive data and aligns Artificial Intelligence (AI) with DG concepts. By integrating AI algorithms directly in the DG architecture, three main purposes of DG-assisted sensitive data management may be addressed: risk management, compliance, and readiness for analytics processes. Risk management benefits from the AI-Enabled Risk Assessment Management System (AI-RAMs); compliance automation is supported by the AI-Enabled Regulation Specification System (AI-ReSS); and the AI-Enabled Data Quality Assessment System (AI-DQAS) copes with the assurance of a GDPR- and HIPAA-compliant readiness for analytics processes.

Equation 1) Core variables and sets

1.1 Healthcare Analytics Platform as data-flows

Define:

- Set of data sources:
  $\mathcal{S} = \{s_1, s_2, \dots\}$
  This corresponds to the paper's **DRS-Flowset-Src** (declared sources at flow level) .
- Set of data-flows:
  $\mathcal{F} = \{f_1, f_2, \dots\}$

Each flow is a structured object:

$$f = (src, dst, d, u, ctx)$$

where

- $src \in \mathcal{S}$ (source),
- dst = destination system/zone/vendor,
- d = data item(s) / dataset,
- u = "data undergoer" / actor (human/app/service),
- ctx = context (location, purpose, time, jurisdiction, etc.).

1.2 Regulations and ontology mapping

Let:

- Set of regulations:
  $\mathcal{R} = \{\text{HIPAA,GDPR,HITECH,GINA,ADA,FERPA, ...}\}$
  (these are explicitly mentioned) .
- Each regulation $r \in \mathcal{R}$ has a set of requirements:
  $\mathcal{Q}_r = \{q_{r,1}, q_{r,2}, \dots\}$
- The ontology is a graph:
  $\mathcal{O} = (\mathcal{C}, \mathcal{E})$
  with concepts $\mathcal{C}$ (e.g., PHI, consent, breach-notification, access-control) and edges $\mathcal{E}$ (relations).

Define a mapping (regulation → ontology concepts):

$$\phi: \bigcup_{r \in \mathcal{R}} \mathcal{Q}_r \to 2^{\mathcal{C}}$$

2.1. Significance of Data Governance in AI Applications

The successful application of corporate AI has become a crucial task for companies, regardless of whether they aim to innovate or merely maintain competitiveness and brand image. AI adoption considers economic, legal, social, and ethical aspects, particularly in regulating the use of resources needed to develop digital intelligence. Data governance associated with the use of data is an indicator of the success of AI in organizations.

Data governance is a necessary structure that determines how the management, monitoring, and use of data should occur. The term originally referred to the establishment of policies for the classification of information. A revised version of the procedure uses technology to categorize data, making it compliant with various standards and legislation. An AI-enhanced data governance model replaces human intervention with inference systems that monitor the contents of tables and files and automatically propagate changes to documented data or metadata throughout the information life cycle. With this information umbrella, managers are better equipped to assess the risks associated with adopting AI projects in their organizations.

3. Regulatory Landscape and Compliance Requirements

Compliance is regulated by existing laws and guidelines for data processing, such as security, privacy, and confidentiality mandates. Compliance-enabled system architectures facilitate rapid examination of compliance requirements proposed in Digital Health laws and Health Data Ecosystem Regulation (EA) and Mapping Study conducted for partner countries.

Information systems that collect, integrate, or disseminate sensitive data — health, banking, etc. — must comply with information protection laws. How and where data is processed, who accessed information, and when individuals' privacy is compromised are major issues. Data classification during the early stages of a data-processing cycle is thus the most critical aspect of the analytical pipeline or data-processing environment that assures compliance, enabling decisions to implement preventive, detective, or corrective controls and policy decisions.

The rapidly evolving regulatory environment in the healthcare sector is driven by a shift toward digital health policies worldwide. As illustrated, recommendations regarding digital health and AI are a crucial enabler of a secure and trusted Digital Health Ecosystem. The Digital Health Mapping Study highlights the growing clinical uptake of artificial intelligence solutions. Internationally, many countries either have already established or are developing Digital Health strategies and Digital Health Systems. The recommendations contained in the Digital Health Mapping Study cover dumping, privacy and confidentiality, security, and safety and liability. Hence, a Dedicated Compliance–Enabled Architecture for Cloud-Based Analytics and Disease Surveillance Platforms for Partner Countries Digital Health System is mentioned within the scope of the EA.

3.1. Overview of Key Regulations and Standards

Healthcare analytics platforms have to comply with a myriad of regulations, mandated technology standards, and guidelines in order to be used in regulated markets such as Europe and the United States. Among these, the Health Insurance Portability and Accountability Act (HIPAA), Genomic Information Nondiscrimination Act (GINA), Americans with Disabilities Act (ADA), Family Educational Rights and Privacy Act (FERPA), and the Health Information Technology for Economic and Clinical Health Act (HITECH) both restrict the processing of certain types of data and require enhanced attention to IT security.

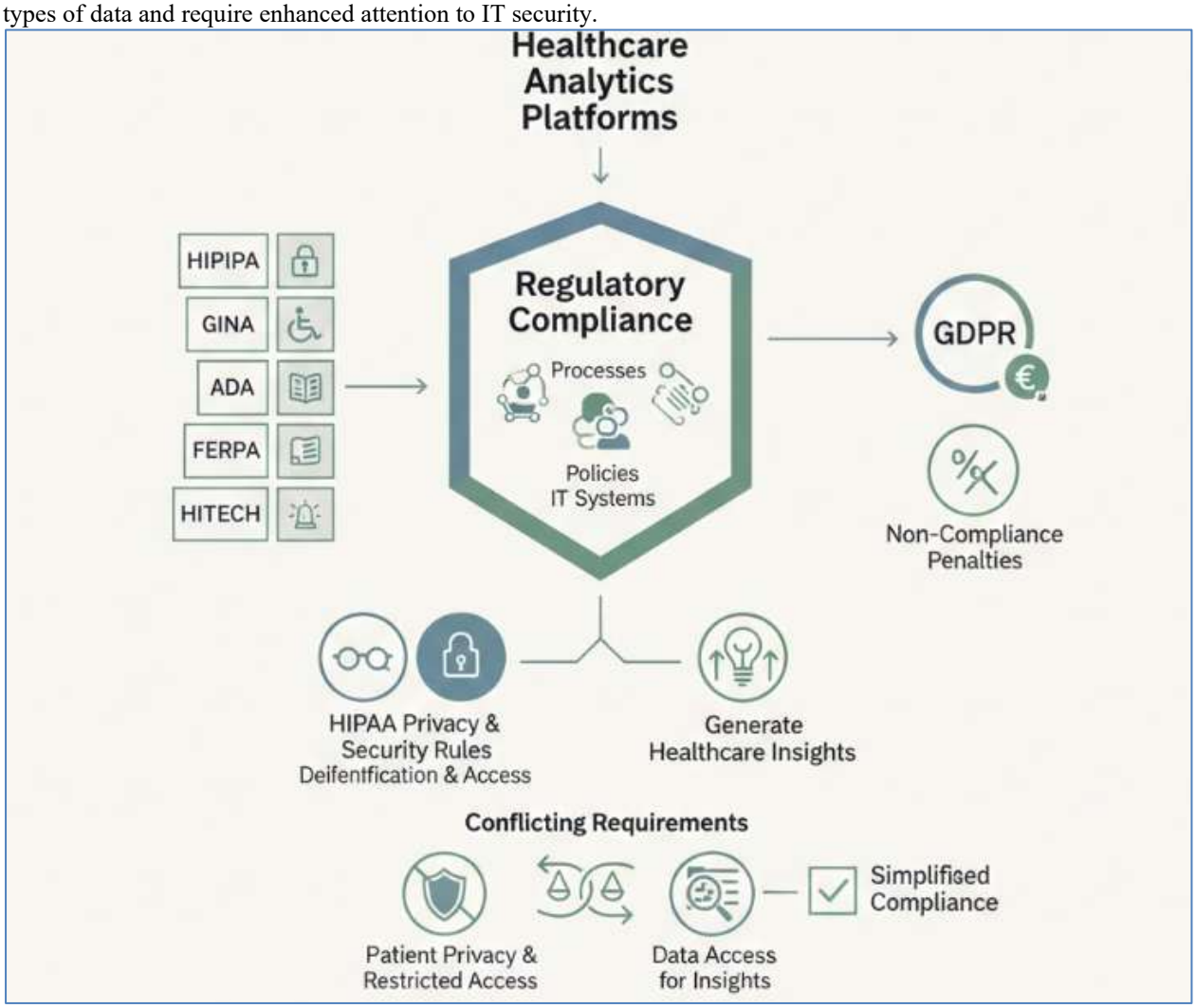


Fig 2: Global Regulatory Synthesis in Healthcare Analytics: A Framework for Automated Compliance Across HIPAA, GDPR, and Emerging IT Security Standards

At the same time, the European Union's General Data Protection Regulation (GDPR) mandates attention to data processing even outside of the EU. GDPR compliance is especially challenging due to the potential for noncompliance penalties of up to 4% of total turnover. To address these many compliance requirements, processes, policies, and IT systems must be put in place to ensure that core privacy and data protection principles are honored, while supporting the generation of healthcare insights.

The HIPAA Privacy Rule establishes the parameters for patient consent related to deidentification, including requirements for the controlled reidentification of data after deidentification, while the HIPAA Security Rule requires that IT security measures be in place to restrict access to PHI. The GINA prohibits discrimination in employment and health insurance on the basis of genetic information. The ADA strengthens patient privacy when seeking preventive medicine, while the FERPA protects the privacy of student records. The HITECH Act strengthens the HIPAA Security Rule requirements for notification in the case of a breach of unsecured PHI while

authorizing states to establish criminal penalties for violations of HIPAA provisions. Simplified methods for ensuring automated compliance with these complex and sometimes conflicting requirements are essential.

4. Architecture of AI-Enhanced Data Governance

The architecture of AI-enhanced data governance for compliance automation in healthcare analytics platforms is shown in the figure. It consists of three tiers: (1) acquisition tier, (2) governance tier, and (3) enforcement tier.

The acquisition tier builds the right information model by determining internal and external data sources, discovering data flows and data undergoers, identifying the applicable regulations, and modeling the compliance requirements. All these tasks are addressed through dedicated algorithms to obtain the data governance model, i.e., the data responsibility chain responsible for achieving compliance. The output of this tier includes (1) DRS-Flowset-Src, the set of internal and external data sources declared at data-flow level, (2) regulation-model, the formal mapping of the identified regulations into an ontology, (3) DRS-Req, the data-responsibility-set model specifying for each data flow the undergoing information, and (4) the regulation-requirements rationale enabling the subsequent implementation of the enforcement tier.

The governance tier maintains the information model through continuous monitoring. Periodically or triggered by internal events (e.g., a change in the location of a control-risk manager), dedicated algorithms identify new flows involving internal and external sources and determine whether new regulations affect these flows. When regulation changes, the new requirement sets serve as input for the reinforcement-learning algorithm trained to tune the modified compliance checks.

Equation 2) Acquisition tier outputs as equations

2.1 DRS-Flowset-Src

Define:

$$\text{DRS-Flowset-Src} = \{src(f) \mid f \in \mathcal{F}\} \subseteq \mathcal{S}$$

2.2 DRS-Req (requirements per flow)

Let the applicable regulations for a flow be:

$$\mathcal{R}(f) = \psi\big(ctx(f), d(f), src(f), dst(f)\big)$$

where $\psi(\cdot)$ is a decision function (jurisdiction + data type + transfer context).

Then the applicable requirements:

$$\mathcal{Q}(f) = \bigcup_{r \in \mathcal{R}(f)} \mathcal{Q}_r$$

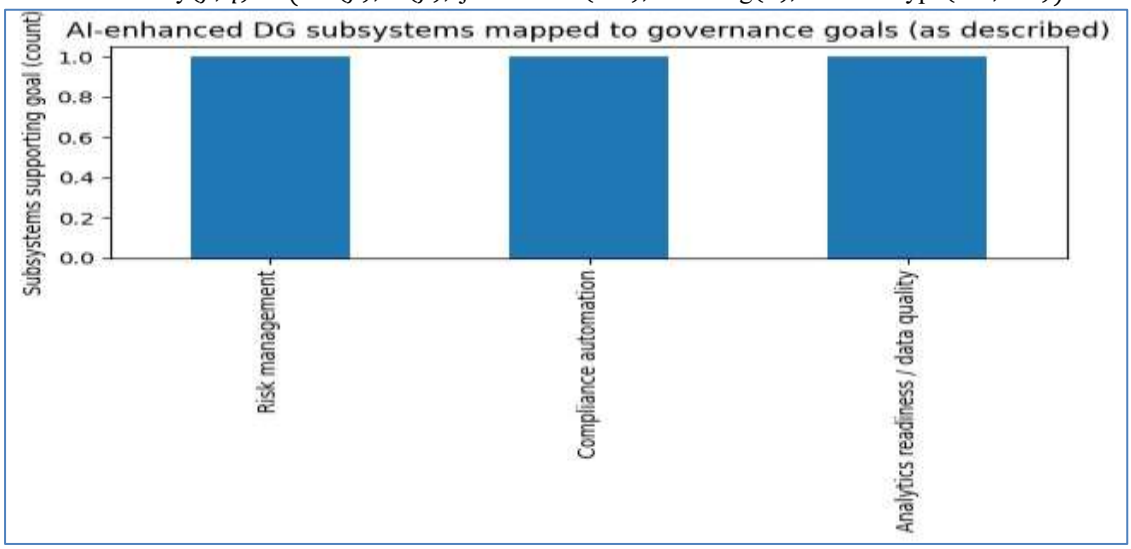
So:

$$\text{DRS-Req}(f) = \mathcal{Q}(f)$$

2.3 Regulation-requirements rationale

To support later enforcement, define a "rationale trace" for each requirement $q \in \mathcal{Q}(f)$:

$$\text{why}(f, q) = \big(ctx(f),\ d(f),\ \text{jurisdiction}(ctx),\ \text{PHI-flag}(d),\ \text{transfer-type}(src, dst)\big)$$



4.1. Data Stewardship and Provenance

The design of the AI-enhanced data governance architecture emphasizes a fundamental aspect of data governance: stewardship and domain expertise. Broadly defined, data stewardship refers to the exercise of appropriate custodial responsibility over data and its quality. For instance, given appropriate provenance data, it would be possible to automatically generate checks at data production time, checking that all relevant data quality criteria are evaluated before the dataset is made available for use. Within an AI-enhanced data governance architecture, stewarding the data registers with links to the different data sources would enable the automatic execution of these checks.

The use of provenance to check compliance with established quality criteria also extends to ensuring compliance for the part of the data that is collected through manual data entry. Automating the application of data quality checks based on provenance is technically challenging, especially when data from different providers and/or

shared registers are merged together. Nevertheless, providing the data quality checks is necessary for it to be trusted by those provided with access to its use.

Being able to review data creation, merging and cleansing procedures after data production would constitute a powerful tool for analysing the evolution of the data and ensuring minimal bias from design decisions. The problem is less about data provenance collection and more about enabling a flexible enough structure to allow for easy integration of the additional provenance information generated by different processes, spanning data ingest, fusion or cleansing algorithms.

The problem of automated provenance acquisition is related to that of analysis completeness, but has the opposite focus: while analysis completeness is concerned about what additional information is required to ensure that data quality checks can be evaluated, the objective here is to ensure that all provenance information is captured to allow detailing and auditing of data origin and the processing chain.

Equation 3) Governance tier monitoring + "RL tuning" as equations

3.1 Monitoring as change detection

Let time be discrete $t = 1,2, \ldots$

Observed flow set at time t:

$$\mathcal{F}_t$$

New flows:

$$\Delta\mathcal{F}_t = \mathcal{F}_t \backslash \mathcal{F}_{t-1}$$

Regulation requirement set at time t:

$$\mathcal{Q}^{(t)}(f)$$

Change in requirements:

$$\Delta\mathcal{Q}^{(t)}(f) = \mathcal{Q}^{(t)}(f) \backslash \mathcal{Q}^{(t-1)}(f)$$

Trigger condition for retuning:

$$\exists f\colon \Delta\mathcal{F}_t \neq \emptyset \text{ or } \Delta\mathcal{Q}^{(t)}(f) \neq \emptyset$$

3.2 Compliance checks as parameterized policies

Let a compliance check for requirement q be:

$$c_q(x; \theta_q) \in \{0,1\}$$

where x is the event (access request, data export, model execution, etc.), and θ_q are tunable parameters (thresholds, rules, classifier cutoffs).

Overall compliance decision:

$$C(x; \Theta) = \prod_{q \in \mathcal{Q}(f(x))} c_q\left(x; \theta_q\right)$$

($\prod$ works like AND in $\{0,1\}$ space.)

3.3 Reinforcement learning objective (derived)

Define:

- State s_t: snapshot of flows + requirement deltas + recent violations.
- Action a_t: adjust thresholds/parameters Θ.
- Reward r_t: balance between (i) reducing violations and (ii) minimizing operational friction.

A practical reward:

$$r_t = -\alpha \cdot \text{Violations}_t \; - \; \beta \cdot \text{FalseBlocks}_t \; - \; \gamma \cdot \text{AuditCost}_t$$

where $\alpha, \beta, \gamma > 0$.

Goal:

$$\max_{\pi} \mathbb{E}_{\pi}\left[\sum_{t=1}^{T} \lambda^{t-1} r_t\right]$$

4.2. Access Control and Identity Management

Healthcare data platforms impose constant and significant access control delays on user experiences. AI tools can optimize active access grants, learn from past interactions, automatically re-authenticate users, and identify and block secure state transitions in the event of an unauthorized session hijacking. AI role mining automates user-role assignments. ML models can predict near future role transitions and proactively issue grants to further reduce waiting delays. AI and ML can also passively analyze temporal patterns and relationships of past authenticated access to automatically detect anomalies like impossible, cubic, or improbable authentication in unexpected locations.

User Identities must be securely managed throughout their lifetimes (creation, update and deletion) – from the underlying operating system user definitions of the underlying hardware, through the supporting Cloud IaaS Provider, and extended to applications operating in the Platforms Zone. User Identities require separation of duties for creation, update and deletion between trusted Platform Administrators and its Cloud Service Provider. Enterprise and external roles used in connecting to other remote resources must be securely created, updated and deleted through supporting, dedicated, trusted tools. More generally, the management of User Identities, Management of sensitive Data, Development and management of custom applications, and of custom Data Models and Data Marts require providers complementary to the applications especially when operating across zones or hosted providers.

Regulation/Standard	Primary focus in the paper
GDPR	Broad data processing governance; cross-border impact; high penalties noted
GINA	Non-discrimination for genetic information
ADA	Privacy protections in preventive medicine context
FERPA	Privacy of student records

5. Automating Compliance in Healthcare Analytics Platforms

The architecture of AI-enhanced data governance provides a foundation on which a compliance automation solution can be developed. The analytics platform implements an AI-enhanced data governance framework that integrates an ontology-based knowledge representation module, supervised machine learning-based user access control management, AI/ML model checkability verification, and an open-source AI enablement and exposure interface. These components, together with other authorized third-party systems and components of the analytics platform, facilitate the automation of multiple, repetitive compliance requirements of a healthcare analytics platform, specifically the processing of sensitive health-related personal information.

Following a thorough assessment of the compliance-related components of the healthcare analytics platform, the compliance automation architecture is derived from the previously introduced AI-enhanced data governance architecture and depicted as an asynchronous interaction between participating systems. Though the FDA-designated case study platforms have not yet been enabled for the auditing of AI-based components and the monitoring of user access rights, the compliance automation capabilities within the previously described architecture are planned as future development activities. An AI-enhanced data governance layer enables third-party AI-exposed models to be reused and AI-exposed services hosted within other authorized platforms to be called from the healthcare analytics platform.

5.1. Data Ingestion and Quality Assurance

Data is assumed to be ingested into an analytics platform from heterogeneous sources, and the data quality must be ensured before any analysis is performed on it. Traditional data-quality assessment and cleansing applies to these disparate sources, with standard algorithms adapted to specific domains. An important addition that would benefit any analytics platform is to include such assessment as part of the ingestion process, along with automated data reds, greens, and blacks for visualisation. Restricted views on data for clients must also be implemented during ingestion, though these use adaptive classification techniques based on pseudo-label propagation.

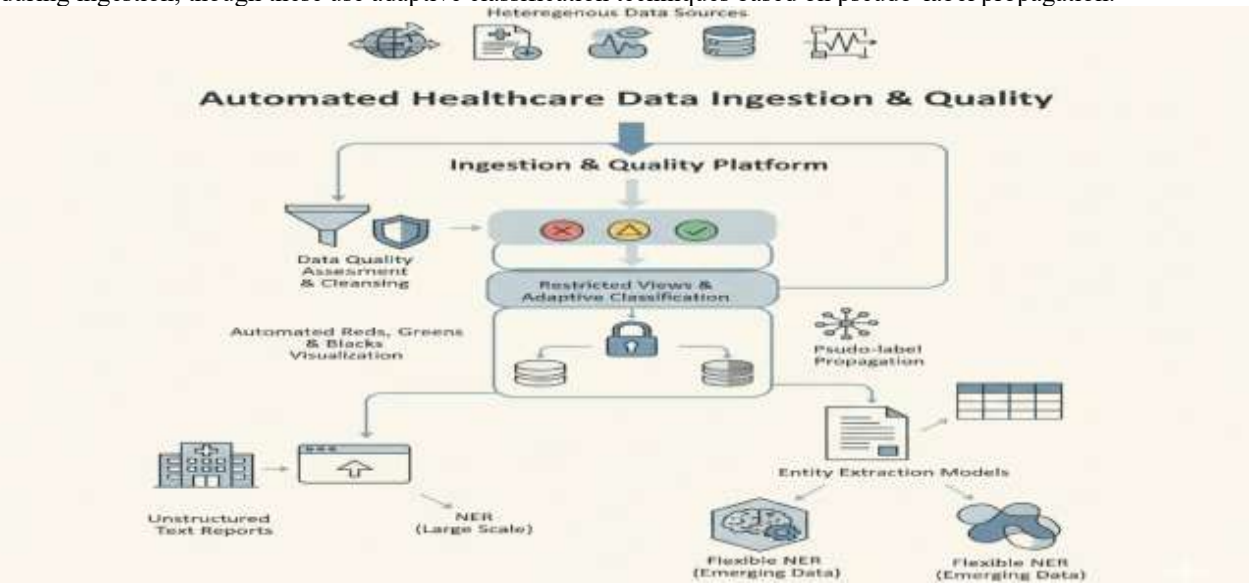


Fig 3: Adaptive Ingestion Frameworks for Heterogeneous Healthcare Data: Integrating Automated Quality Assessment and Pseudo-Label Propagation for Secure Analytics

Consider an example platform for automated tracking of COVID-19 vaccine administration by hospitals. Reports from hospitals are uploaded by users through a web interface, with the underlying data in unstructured text format. Suitable entity extraction task-specific models for the specific class of documents can be developed and used at the ingestion stage for automatic extraction of data in structured form from unstructured reports, to allow the data to be available for further processing and testing. Fixed and flexible named-entity-recognition models can also be developed for hospitals or doctors with a large number of unlabelled documents, with the large-scale information being captured by the fixed models, while flexible models can handle data for emerging hospitals with limited documents.

5.2. governance with AI-assisted policy enforcement

The GDPR describes a digital life cycle for individuals that is enhanced by supervised Machine Learning. The data labels are easily modifiable by the parties involved in the learning while maintaining physical data under their protection. The consequences of the most significant European regulation for data protection are analysed for business activity. Businesses of the European Union can obtain competitive advantages by selling fully GDPR-compliant Intelligent Systems based on strong Management System.

Artificial Intelligence presents new ethical dilemmas such as the invalidation of deontological choices even in sensitive fields. A new ethical algorithm is proposed to standardise the establishment of ethical parameters in Automated Decision Systems supervised by two (or more) Ethical Committees. Thus, the ethical enforcements of the Intelligent System are synergistic with Intelligence, with moral expectations, deontological choices, and the principles set out in the Constitution.AI technologies have improved their predictive power also in sensitive fields such as human health.

However, the digitalisation of KET Intelligent Systems does not appear to be rational and the strict regulation of the EU is considered a brake on the development of these systems, because of the metacentric approach that characterises GDPR. Recognition and management of KETs through an economic management structure are fundamental to their real development.

Tier	Key responsibilities (summarized)	Named outputs mentioned	#Key responsibilities
Acquisition tier	Identify data sources + flows; identify regulations; model requirements; build responsibility chain	DRS-Flowset-Src; regulation-model (ontology); DRS-Req; regulation-requirements rationale	4
Governance tier	Continuously monitor flows/regulations; detect changes; retune compliance checks with RL when needed	Updated requirement sets; RL-tuned compliance checks	3
Enforcement tier	Apply controls/checks: access control, auditing/monitoring, policy enforcement, approvals	Automated checks/controls (access control, monitoring, auditing)	1

6. Technical Methods and Algorithms

Technical methods and algorithms for an AI-enhanced data governance system that automates compliance in healthcare analytics platforms comprise planning and decision-making, machine learning for policy generation, metadata analysis for data discovery, data lineage for data accessibility analysis, data classification for risk assessment, rule-based logic for data release categorization, and a recommendation model for access control. Decision-making is based on a cognitive map that brings together the components of AI-enhanced data governance for compliance automation.

The policy generator derives the set of policies in a healthcare analytics platform by learning from its configuration. Metadata and service registries provide the required sources for data discovery. Data lineage analysis identifies the data components whose access must satisfy the data accessibility requirements of the data owners, while data classification assesses the risk of data releases. The rule-based engine categorizes a release request according to the classification result, generating an approval list matched with the category of each requester. Lastly, the recommendation model summarizes all the approval lists and suggests an access control procedure.

Equation 4) Enforcement tier: risk scoring, classification, rule engine, and access recommendation

4.1 Lineage / accessibility constraint (derived)

Let lineage graph be:

$$G = (V, E)$$

Nodes V are datasets/tables/models; edges are transforms.

For a requested dataset v, ancestor closure:

$$\text{anc}(v) = \{u \in V : u \rightsquigarrow v\}$$

Accessibility must satisfy owner constraints for all ancestors:

$$\forall u \in \text{anc}(v) : \text{Permit}(u, requester) = 1$$

4.2 Risk score from classification

Let features $\mathbf{z}$ describe the release request (PHI presence, quasi-identifiers, k-anon stats, destination trust, etc.).

A classifier outputs probability of high risk:

$$p = \Pr(\text{HighRisk} \mid \mathbf{z})$$

Define risk score:

$$\text{Risk}(\mathbf{z}) = p$$

4.3 Rule-based release categorization

Choose thresholds $0 \le \tau_1 < \tau_2 < 1$.

Category:

$$\text{Cat}(\mathbf{z}) = \begin{cases} \text{Green} & \text{if Risk}(\mathbf{z}) < \tau_1 \\ \text{Amber} & \text{if } \tau_1 \le \text{Risk}(\mathbf{z}) < \tau_2 \\ \text{Red} & \text{if Risk}(\mathbf{z}) \ge \tau_2 \end{cases}$$

4.4 Approval list generation

Let requester category be $\kappa(requester)$ (internal clinician, researcher, vendor, etc.).

Define allowed approvals as a policy table:

$$A = \text{Approvers}\big(\text{Cat}(\mathbf{z}), \kappa(requester)\big)$$

Decision:

$$\text{Approve}(x) = \begin{cases} 1 & \text{if AllRequiredApprovals}(A) \text{ obtained} \\ 0 & \text{otherwise} \end{cases}$$

4.5 Recommendation model for access control procedure

Suppose there are procedures $\mathcal{P} = \{p_1, p_2, \dots\}$ (auto-approve, manager-approve, DPO review, security review, block).

Score each:

$$\text{Score}(p_i) = w_1 \cdot \text{ComplianceFit}(p_i) - w_2 \cdot \text{UserDelay}(p_i) - w_3 \cdot \text{ResidualRisk}(p_i)$$

Pick:

$$p^* = \underset{p_i \in \mathcal{P}}{\text{argmax}} \text{Score}(p_i)$$

6.1. Machine Learning for Policy Compliance

Machine learning models play an important role in automated regulatory compliance. Custom solution software has been created for testing policy validation using inference-based machines such as random forest, decision tree classifier, or k-nearest neighbour implementation and various unsupervised or reinforcement learning systems. A systematic method has been created for determining patterns of satisfactory or unsatisfactory placement of students in computer science degree programs through regression analysis.

Detection of unwanted behaviours (or, conversely, desired behaviours) can be expressed as a classification problem. Anomaly detection is based on the premise that unwanted behaviours cannot be explicitly encoded, but can be detected by monitoring the data. When the inputs are successfully classified, covert abuse can be inhibited. A reinforcement learning model is being developed that will work "off policy" to learn to identify students with risk factors that lead to drop-out; the model will rely on historical data and will adapt in real time as new student data become available.

Other models focus on satisfying curriculum rules. Models have been trained to identify scenarios that violate prerequisites for courses and the relationship between course load and achievement. The systems are based on a combination of decision trees, random forest (or permutation importance of features) and association rule mining. Scenarios resulting from GOP completion rules for a Business School have also been classified.

Work is being done to automatically assess undergraduate curriculum development against institutional rules and educational philosophies. A system has been developed that identifies scenarios involving students breaking curriculum rules. The base machine has been implemented as a classifier with subsequent machines developed as association rule miners for enhancement before suspicion is raised. It learns using scenarios classified as "fit" and "ill-fit". Techniques are now being developed to detect and assist in stopping fraud and abuse of funding programs at the tenure and probation levels.

6.2. Natural Language Processing for Regulation Mapping

Mapping legal regulations onto product processes written in natural language—such as descriptions of data governance, software testing, and data control—is important for improving automation and presents many opportunities. AI and LLM technologies can help with this task: the automation of compliance regulation reading and mapping software product processes logical reduction is particularly noteworthy. An LLM-based approach to present features and limitations of the technology can simplify the process of regulation extraction and structure 10–20 regulations into a 2D or 3D matrix. Associated sets of questions can further oversee detailed regulation detection, mapping, and reading.

As a natural language processing task, regulation mapping reads legal regulations and finds corresponding sections of a product process regulation or set of details giving a clear and relevant answer to each regulation. Suppose ChatGPT, an LLM with question and answer capability, serves as the natural language engine. A product/process description (transcripts), regulation, and large set of simple(Basics) and advanced (Start divisions & Divisions) questions are prepared. Knowledge about the product and testing phase can develop these prerequisites. The product description describes the software package. The other transcript can describe a data governance function and its mapping to product logic testing; it also includes product features. The advanced question list allows the detailed detection of regulation answers.

The proposed task is to prepare paragraphs for process description. The Automation engine reads automation-description regulation first, automatically extracts the question list, checks for detected answers, and finally reads and presents detection. The same technology structure of presenting other features applies throughout the paragraphs. A second-tier engine, feature-point structure language detection, reads the description and automatically extracts all specified product ideas and functions, plus detected questions and answers.

7. Conclusion

Automating compliance using AI-enhanced data governance opens a new era in compliance and information security. The architecture, technical methods, and algorithms provide the foundation for AI-enhanced data governance and compliance automation modules, with direct application in a healthcare analytics platform supporting sensitive data. The proposed architecture reduces the focus on the business logic of analytical models, abstracting away compliance concerns and avoiding delays and reuse difficulties. Since the process relies on AI and natural language, it integrates naturally into the flow of data and analytics operations.

Regulation-based requirements rapidly expand with increasing contributions from data lakes, machine learning, and deep learning. Enterprises often invest considerably in regulatory compliance and ongoing support to protect business operations. Despite the costs, compliance is not guaranteed; service violations, fraud, or data theft remain major threats. AI-enhanced automatic data governance aims to eliminate these threats by enforcing compliance guarantees seamlessly, with negligible overhead. Presenting the approach in a healthcare context highlights its generality and the technical aspects relevant to a broad audience.

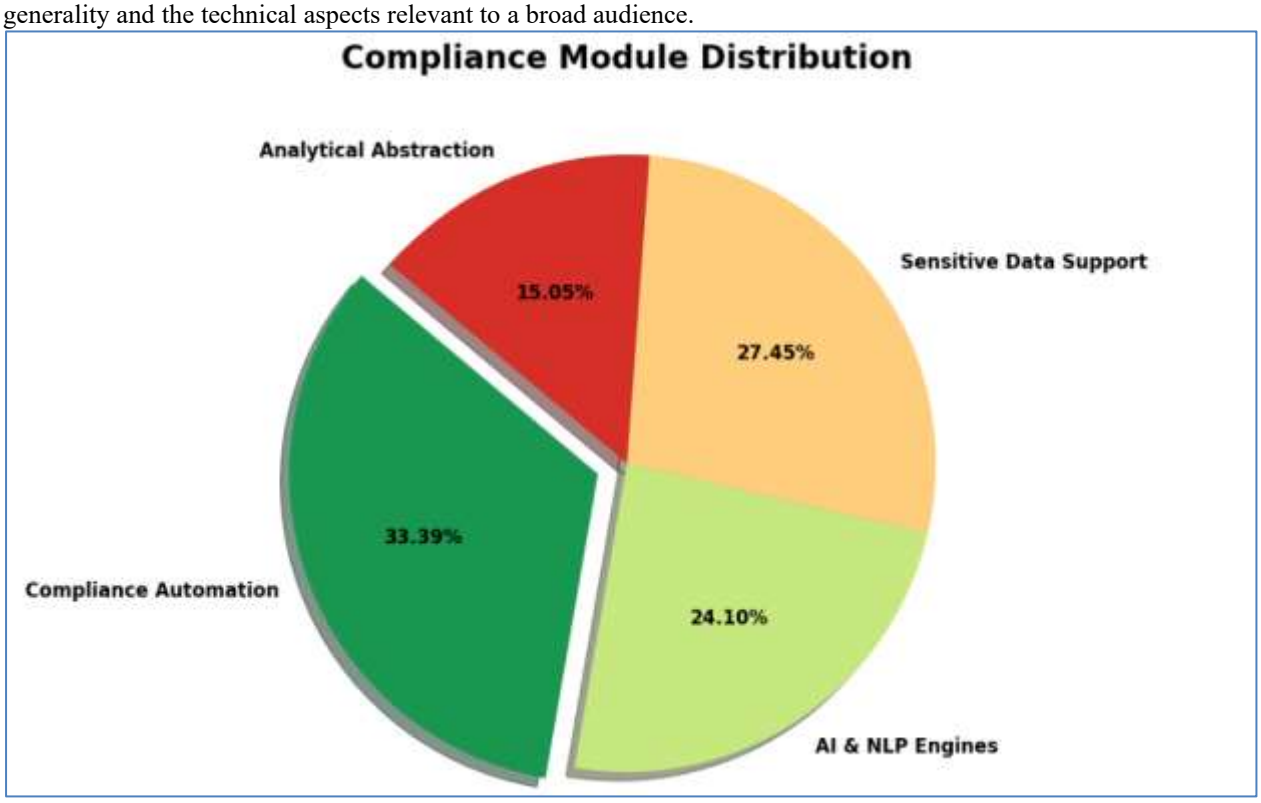


Fig 4: Compliance Module Distribution

7.1. Final Thoughts and Future Directions

Modern healthcare analytics platforms intelligently analyze various healthcare-related data (structured and unstructured, internal and external) to support important decisions that benefit patients and health institutions. However, the sensitive nature of these data makes compliance with regulatory requirements (e.g., HIPAA, HITECH, GDPR) critical. Non-compliance may lead to significant financial penalties. Regulatory data governance (including compliance monitoring and auditing) is crucial for compliance and, therefore, for the acceptance of these platforms in the healthcare environment. Nevertheless, current data governance approaches largely rely on manual processes, which may be insufficient and susceptible to errors. Automating data governance can provide a solution, and a novel architecture with an AI-Enhanced Data Governance layer that supports the automation is proposed.

The AI-Enhanced Data Governance layer utilizes a set of methods for regulatory compliance data monitoring and auditing to support the compliance of intelligent healthcare analytics platforms. The proposed architecture, operationalization of the layer, and technical algorithms have been developed within the context of providing support for significant healthcare-related decisions while meeting regulatory compliance requirements. Future work will explore additional Technical Methods and AlgorithmsTelecom Designers project-specific regulatory requirements and enhance the proposed AI-Enhanced Data Governance Layer and its operationalization with automated data annotation using Natural Language Processing in combination with a Multi-Chatbot framework for semantically annotated and regulated data used by Multi-Chatbot-based Artificial Intelligence Agents.

References

[1] Kshetri, N., & Voas, J. (2022). Blockchain-enabled healthcare data governance. IT Professional, 24(4), 23–29..

[2] Inala, R. AI-Powered Investment Decision Support Systems: Building Smart Data Products with Embedded Governance Controls.

[3] Lasi, H., Fettke, P., Kemper, H. G., et al. (2014). Industry 4.0. Business & Information Systems Engineering, 6(4), 239–242.

[4] Nagabhyru, K. C. (2024). Data Engineering in the Age of Large Language Models: Transforming Data Access, Curation, and Enterprise Interpretation. Computer Fraud and Security.

[5] Kumar, R., Singh, P., & Gupta, A. (2024). AI-driven governance models for healthcare data ecosystems. Information Systems Frontiers, 26(1), 233–248.

[6] Meda, R. (2024). Agentic AI in Multi-Tiered Paint Supply Chains: A Case Study on Efficiency and Responsiveness. Journal of Compu-tational Analysis and Applications (JoCAAA), 33(08), 3994-4015.
[7] Sarker, I. H. (2023). AI-based data science for healthcare decision support systems. SN Computer Science, 4(2), 156.
[8] Varri, D. B. S. (2022). A Framework for Cloud-Integrated Database Hardening in Hybrid AWS-Azure Environments: Security Posture Automation Through Wiz-Driven Insights. International Journal of Scientific Research and Modern Technology, 1(12), 216-226.
[9] Wang, S., Wan, J., Zhang, D., et al. (2016). Towards smart factory for Industry 4.0. International Journal of Distributed Sensor Networks, 12(1), 1–12.
[10] Rongali, S. K. (2024). Federated and Generative AI Models for Secure, Cross-Institutional Healthcare Data Interoperability. Journal of Neonatal Surgery, 13(1), 1683-1694.
[11] Sharma, V., Patel, S., & Shah, M. (2024). Intelligent compliance management for healthcare big data platforms. Future Generation Computer Systems, 150, 112–125.
[12] Nagubandi, A. R. (2023). Advanced Multi-Agent AI Systems for Autonomous Reconciliation Across Enterprise Multi-Counterparty Derivatives, Collateral, and Accounting Platforms. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 653-674.
[13] Zhang, Y., Li, X., & Chen, H. (2024). Automated regulatory compliance monitoring using artificial intelligence in healthcare data platforms. Journal of Biomedical Informatics, 149, 104563.
[14] Vardhan Kumar Bandi, V. D. (2024). Automated Feature Engineering Systems in Large-Scale Healthcare Data Environments. Journal of Neonatal Surgery, 13(1), 2127–2141. Retrieved from https://www.jneonatalsurg.com/index.php/jns/article/view/10004.
[15] Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25, 1097–1105.
[16] Gottimukkala, V. R. R. (2023). Privacy-Preserving Machine Learning Models for Transaction Monitoring in Global Banking Networks. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 633-652.
[17] Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. CVPR Proceedings, 1251–1258.
[18] Davuluri, P. N. Integrating Artificial Intelligence into Event-Driven Financial Crime Compliance Platforms.
[19] Bergmann, P., Fauser, M., Sattlegger, D., & Steger, C. (2019). MVTec AD—A comprehensive real-world dataset for unsupervised anomaly detection. CVPR Proceedings, 9592–9600.
[20] Kushvanth Chowdary Nagabhyru. (2023). Accelerating Digital Transformation with AI Driven Data Engineering: Industry Case Studies from Cloud and IoT Domains. Educational Administration: Theory and Practice, 29(4), 5898–5910. https://doi.org/10.53555/kuey.v29i4.10932
[21] Ruff, L., Vandermeulen, R. A., Görnitz, N., et al. (2018). Deep one-class classification. ICML Proceedings, 4393–4402.
[22] Meda, R. (2023). Intelligent Infrastructure for Real-Time Inventory and Logistics in Retail Supply Chains. Educational Administration: Theory and Practice.
[23] Schlegl, T., Seeböck, P., Waldstein, S. M., et al. (2017). Unsupervised anomaly detection with GANs. Information Processing in Medical Imaging, 146–157.
[24] Amistapuram, K. (2024). Generative AI in Insurance: Automating Claims Documentation and Customer Communication. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 15(3), 461–475. https://doi.org/10.61841/turcomat.v15i3.15474
[25] Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000). LOF: Identifying density-based local outliers. ACM SIGMOD, 93–104.
[26] Rongali, S. K., & Kumar Kakarala, M. R. (2024). Existing challenges in ethical AI: Addressing algorithmic bias, transparency, accountability and regulatory compliance.
[27] Agentic AI in Data Pipelines: Self Optimizing Systems for Continuous Data Quality, Performance and Governance. (2024). American Data Science Journal for Advanced Computations (ADSJAC) ISSN: 3067-4166, 2(1).
[28] Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.
[29] Pandugula, C., Kalisetty, S., & Polineni, T. N. S. (2024). Omni-channel Retail: Leveraging Machine Learning for Personalized Customer Experiences and Transaction Optimization. Utilitas Mathematica, 121, 389-401.
[30] Batini, C., & Scannapieco, M. (2016). Data and information quality. Springer.
[31] Kalisetty, S. (2023). The Role of Circular Supply Chains in Achieving Sustainability Goals: A 2023 Perspective on Recycling, Reuse, and Resource Optimization. Reuse, and Resource Optimization (June 15, 2023).
[32] Sculley, D., Holt, G., Golovin, D., et al. (2015). Hidden technical debt in machine learning systems. Advances in Neural Information Processing Systems, 28, 2503–2511.
[33] Segireddy, A. R. (2024). Machine Learning-Driven Anomaly Detection in CI/CD Pipelines for Financial Applications. Journal of Computational Analysis and Applications, 33(8).
[34] Amershi, S., Begel, A., Bird, C., et al. (2019). Software engineering for machine learning. IEEE Software, 36(5), 56–67.
[35] Varri, D. B. S. (2024). Adaptive and Autonomous Security Frameworks Using Generative AI for Cloud Ecosystems. Available at SSRN 5774785.

[36] Breck, E., Cai, S., Nielsen, E., et al. (2017). The ML test score. IEEE Big Data Proceedings, 1123–1132.
[37] Keerthi Amistapuram. (2024). Federated Learning for Cross-Carrier Insurance Fraud Detection: Secure Multi-Institutional Collaboration. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 6727–6738. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/3934
[38] Zaharia, M., Das, T., Li, H., et al. (2012). Discretized streams: Fault-tolerant streaming computation. USENIX NSDI, 423–438.
[39] Kreps, J., Narkhede, N., & Rao, J. (2011). Kafka: A distributed messaging system. NetDB Workshop.
[40] Inala, R. Revolutionizing Customer Master Data in Insurance Technology Platforms: An AI and MDM Architecture Perspective.
[41] Carbone, P., Katsifodimos, A., Ewen, S., et al. (2015). Apache Flink: Stream and batch processing. IEEE Data Engineering Bulletin, 38(4), 28–38.
[42] Singireddy, J. (2024). AI-Enhanced Tax Preparation and Filing: Automating Complex Regulatory Compliance. European Data Science Journal (EDSJ) p-ISSN 3050-9572 en e-ISSN 3050-9580, 2(1).
[43] van der Aalst, W. M. P. (2016). Process mining: Data science in action (2nd ed.). Springer.
[44] Varri, D. B. S. (2023). Advanced Threat Intelligence Modeling for Proactive Cyber Defense Systems. Available at SSRN 5774926.
[45] Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. Journal of Manufacturing Systems, 48, 157–169.
[46] Paleti, S. (2024). Transforming Financial Risk Management with AI and Data Engineering in the Modern Banking Sector. American Journal of Analytics and Artificial Intelligence (ajaai) with ISSN 3067-283X, 2(1).
[47] Wan, J., Cai, H., & Zhou, K. (2015). Industrie 4.0: Enabling technologies. IEEE Access, 3, 1567–1579.
[48] Kalisetty, S., & Singireddy, J. (2023). Optimizing Tax Preparation and Filing Services: A Comparative Study of Traditional Methods and AI Augmented Tax Compliance Frameworks. Available at SSRN 5206185.
[49] Zhang, C., Yang, J., & Chen, Y. (2023). AI-enabled defect detection in smart factories using hybrid deep learning models. IEEE Access, 11, 94532–94545.
[50] Sheelam, G. K., & Koppolu, H. K. R. (2024). From Transistors to Intelligence: Semiconductor Architectures Empowering Agentic AI in 5G and Beyond. Journal of Computational Analy- sis and Applications(JoCAAA), 33(08), 4518-4537.
[51] Li, X., Sun, Q., & Wang, H. (2024). Real-time industrial anomaly detection with edge-cloud collaborative learning. IEEE Transactions on Industrial Informatics, 20(2), 1324–1336.
[52] Aitha, A. R. (2023). CloudBased Micro services Architecture for Seamless Insurance Policy Administration. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 607-632.
[53] Li, X., Sun, Q., & Wang, H. (2024). Real-time industrial anomaly detection with edge–cloud collaborative learning. IEEE Transactions on Industrial Informatics, 20(2), 1324–1336.
[54] Kolla, S. H. (2024). RETRIEVAL-AUGMENTED GENERATION WITH SMALL LLMS FOR KNOWLEDGE-DRIVEN DECISION AUTOMATION IN ENTERPRISE SERVICE PLATFORMS. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 15(3), 476–486. https://doi.org/10.61841/turcomat.v15i3.15497.
[55] Zhang, C., Yang, J., & Chen, Y. (2023). AI-enabled defect detection in smart factories using hybrid deep learning models. IEEE Access, 11, 94532–94545.
[56] Guntupalli, R. (2024). Enhancing Cloud Security with AI: A Deep Learning Approach to Identify and Prevent Cyberattacks in Multi-Tenant Environments. Available at SSRN 5329132.
[57] Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. Journal of Manufacturing Systems, 48, 157–169.
[58] Kolla, S. K. (2021). Designing Scalable Healthcare Data Pipelines for Multi-Hospital Networks. World Journal of Clinical Medicine Research, 1(1), 1–14. Retrieved from https://www.scipublications.com/journal/index.php/wjcmr/article/view/1376
[59] Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23.
[60] Yandamuri, U. S. AI-Driven Decision Support Systems for Operational Optimization in Hospitality Technology.
[61] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1–10.
[62] Koppolu, H. K. R., & Sheelam, G. K. (2024). Machine Learning-Driven Optimization in 6G Telecommunications: The Role of Intelligent Wireless and Semiconductor Innovation. Global Research Development (GRD) ISSN: 2455-5703, 9(12).
[63] Wan, J., Tang, S., Li, D., et al. (2018). A manufacturing big data solution for active preventive maintenance. IEEE Transactions on Industrial Informatics, 13(4), 2039–2047.
[64] Lahari Pandiri, "AI-Powered Fraud Detection Systems in Professional and Contractors Insurance Claims," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2024.121206.

[65] Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2016). Towards smart factory for Industry 4.0: A self-organized multi-agent system with big data-based feedback and coordination. International Journal of Distributed Sensor Networks, 12(1), 1–12.
[66] Rongali, S. K. (2023). Explainable Artificial Intelligence (XAI) Framework for Transparent Clinical Decision Support Systems. International Journal of Medical Toxicology and Legal Medicine, 26(3), 22-31.
[67] Bergmann, P., Fauser, M., Sattlegger, D., & Steger, C. (2019). MVTec AD—A comprehensive real-world dataset for unsupervised anomaly detection. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 9592–9600.
[68]
[69] Ruff, L., Vandermeulen, R. A., Görnitz, N., et al. (2018). Deep one-class classification. Proceedings of the 35th International Conference on Machine Learning, 4393–4402.
[70] Kolla, S. K. (2021). Architectural Frameworks for Large-Scale Electronic Health Record Data Platforms. Current Research in Public Health, 1(1), 1–19. Retrieved from https://www.scipublications.com/journal/index.php/crph/article/view/1372.
[71] Schlegl, T., Seeböck, P., Waldstein, S. M., Schmidt-Erfurth, U., & Langs, G. (2017). Unsupervised anomaly detection with generative adversarial networks. Information Processing in Medical Imaging, 146–157.
[72] Guntupalli, R. (2024). AI-Powered Infrastructure Management in Cloud Computing: Automating Security Compliance and Performance Monitoring. Available at SSRN 5329147.
[73] Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000). LOF: Identifying density-based local outliers. Proceedings of the ACM SIGMOD International Conference on Management of Data, 93–104.
[74] Uday Surendra Yandamuri. (2023). An Intelligent Analytics Framework Combining Big Data and Machine Learning for Business Forecasting. International Journal Of Finance, 36(6), 682-706. https://doi.org/10.5281/zenodo.18095256
[75] Sculley, D., Holt, G., Golovin, D., et al. (2015). Hidden technical debt in machine learning systems. Advances in Neural Information Processing Systems, 28, 2503–2511.
[76] Garapati, R. S. (2023). Optimizing Energy Consumption in Smart Build-ings Through Web-Integrated AI and Cloud-Driven Control Systems.
[77] Amershi, S., Begel, A., Bird, C., et al. (2019). Software engineering for machine learning: A case study. IEEE Software, 36(5), 56–67.
[78] Kalisetty, S. (2024). Deep learning frameworks for multi-modal data fusion in retail supply chains: enhancing forecast accuracy and agility.
[79] Breck, E., Cai, S., Nielsen, E., Salib, M., & Sculley, D. (2017). The ML test score: A rubric for ML production readiness and technical debt reduction. Proceedings of IEEE Big Data, 1123–1132.
[80] Meda, R. (2024). Agentic AI in Multi-Tiered Paint Supply Chains: A Case Study on Efficiency and Responsiveness. Journal of Compu-tational Analysis and Applications (JoCAAA), 33(08), 3994-4015.
[81] Zaharia, M., Das, T., Li, H., et al. (2012). Discretized streams: Fault-tolerant streaming computation at scale. Proceedings of the USENIX Symposium on Networked Systems Design and Implementation, 423–438.
[82] Aitha, A. R. (2024). Generative AI-Powered Fraud Detection in Workers' Compensation: A DevOps-Based Multi-Cloud Architecture Leveraging, Deep Learning, and Explainable AI. Deep Learning, and Explainable AI (July 26, 2024).
19. Spackman, K. A., Campbell, K. E., & Côté, R. A. (1997). SNOMED RT. JAMIA, 4(6), 640–649.
[83] Carbone, P., Katsifodimos, A., Ewen, S., et al. (2015). Apache Flink: Stream and batch processing in a single engine. IEEE Data Engineering Bulletin, 38(4), 28–38.
[84] Keerthi Amistapuram. (2023). Privacy-Preserving Machine Learning Models for Sensitive Customer Data in Insurance Systems. Educational Administration: Theory and Practice, 29(4), 5950–5958. https://doi.org/10.53555/kuey.v29i4.10965
[85] van der Aalst, W. M. P. (2016). Process mining: Data science in action (2nd ed.). Springer.
[86] Chava, K. (2024). The Role of Cloud Computing in Accelerating AI-Driven Innovations in Healthcare Systems. European Advanced Journal for Emerging Technologies (EAJET)-p-ISSN 3050-9734 en e-ISSN 3050-9742, 2(1).
[87] Rasmy, L., Wu, Y., Wang, N., et al. (2021). Deep learning for healthcare predictive analytics. Journal of Biomedical Informatics, 118, 103779.
[88] Siva Hemanth Kolla. (2023). Deep Learning–Driven Retrieval-Augmented Generation for Enterprise ITSM Automation: A Governance-Aligned Large Language Model Architecture. Journal of Computational Analysis and Applications (JoCAAA), 31(4), 2489–2502. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/4774
[89] Li, Z., Wang, Y., & Zhang, H. (2024). AI-driven visual inspection and quality prediction in Industry 4.0 manufacturing systems. Journal of Manufacturing Systems, 72, 210–224.
[90] Davuluri, P. S. L. N. (2024). AI-Driven Data Governance Frameworks for Automated Regulatory Reporting and Audit Readiness. Metallurgical and Materials Engineering, 30(4), 996–1010. Retrieved from https://metall-mater-eng.com/index.php/home/article/view/1936
[91] Sarker, I. H., Kayes, A., & Watters, P. (2022). Data science and analytics for healthcare governance. Journal of Big Data, 9(1), 34.

[92] Sasi Kumar Kolla. (2023). Big Data–Driven Machine Learning Frameworks for Clinical Risk Prediction. International Journal of Medical Toxicology and Legal Medicine, 26(3 and 4), 44–59. Retrieved from https://ijmtlm.org/index.php/journal/article/view/1456.
[93] Haleem, A., Javaid, M., Singh, R., & Suman, R. (2023). Artificial intelligence applications in healthcare and data governance. Sensors International, 4, 100207.
[94] Bandi, V. D. V. K. (2023). Production-Grade Machine Learning Pipelines For Healthcare Predictive Analytics. South Eastern European Journal of Public Health, 189–205. Retrieved from https://www.seejph.com/index.php/seejph/article/view/7057
[95] Kaur, H., Alam, M. A., Jameel, R., Mourya, A., & Chang, V. (2024). AI-enabled data governance frameworks for secure healthcare analytics. IEEE Access, 12, 22514–22530.
[96] Velangani Divya Vardhan Kumar Bandi. (2024). Intelligent Data Platforms For Personalized Retail Analytics At Scale. Metallurgical and Materials Engineering, 30(4), 1011–1027. Retrieved from https://metall-mater-eng.com/index.php/home/article/view/1011-1027
[97] Patel, V., Shortliffe, E., Stefanelli, M., et al. (2023). The coming of age of artificial intelligence in healthcare governance. NPJ Digital Medicine, 6(1), 45.