International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 6, Nov – Dec 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Enterprise AI Model Drift Detection and Lifecycle Monitoring Architecture

A Comprehensive Enterprise Architecture for Detecting Data, Concept, Performance, Behavioral, and Governance Drift Across the AI Lifecycle

Sanjeeve Kumar Gajadi*
*(HCL Technologies, Bengaluru, Karnataka, India)
Email: sanjeevekumar.g@hcltech.com

****

Abstract:

AI systems can degrade after deployment as data distributions, user behavior, business processes, model providers, prompts, retrieval sources, or external conditions change. Traditional monitoring often focuses on availability and latency while missing semantic and behavioral deterioration. This paper proposes an Enterprise AI Model Drift Detection and Lifecycle Monitoring Architecture that integrates data drift, concept drift, performance drift, prompt drift, retrieval drift, safety drift, fairness drift, security indicators, and business outcomes. The architecture defines baselines, telemetry, thresholds, statistical methods, evaluation datasets, alerts, reassessment triggers, retraining or rollback workflows, and governance evidence. It supports predictive models, Generative AI, RAG, and agentic systems. The proposed design enables organizations to detect degradation earlier, distinguish expected change from harmful drift, and maintain model performance, compliance, and business reliability throughout the lifecycle.

Keywords — Model Drift, AI Monitoring, Data Drift, Concept Drift, Generative AI Monitoring, RAG Monitoring, Agentic AI, Model Lifecycle, Continuous Assurance, MLOps

****

I. INTRODUCTION

AI systems are not static assets. Their operating environment, data, users, providers, and dependencies can change continuously.

Lifecycle monitoring should therefore evaluate whether the assumptions used during approval remain valid in production.

II. DRIFT TAXONOMY

Drift can affect input data, target relationships, output quality, prompts, retrieval sources, user behavior, fairness, safety, security, or business outcomes.

Different drift types require different detection and remediation methods.

III. BASELINE ARCHITECTURE

Approved baselines should capture distributions, quality metrics, model version, prompt version, retrieval configuration, policy settings, and business performance.

Baseline changes should be controlled and auditable.

IV. DATA AND CONCEPT DRIFT

Statistical tests can identify significant changes in feature distributions, classes, missingness, or relationships between inputs and outcomes.

Detection thresholds should consider sample size, seasonality, and business context.

V. GENERATIVE AI AND PROMPT DRIFT

Generative systems require monitoring of factuality, relevance, refusal behavior, harmful output, style, and instruction following.

Prompt and model-provider updates should be treated as lifecycle changes that may alter behavior even when application code is unchanged.

VI. RAG AND KNOWLEDGE DRIFT

RAG monitoring should track source freshness, retrieval relevance, coverage, citation quality, and semantic shifts in the knowledge base.

 ©IJSRED: All Rights are Reserved

Changes in embeddings, chunking, indexing, or source permissions may create silent quality degradation.

VII. AGENTIC BEHAVIOR DRIFT

Agents should be monitored for changing tool sequences, delegation patterns, retries, decision latency, policy denials, and autonomous task completion.

Behavioral drift can indicate model change, environment change, or emerging misuse.

VIII. MONITORING AND ALERTING

Telemetry should combine model, data, application, security, policy, and business signals.

Alerts should use risk-aware thresholds so critical use cases trigger faster investigation and lower-risk systems avoid excessive noise.

IX. REASSESSMENT AND REMEDIATION

Detected drift can trigger evaluation, retraining, prompt revision, retrieval refresh, model rollback, access restriction, or temporary human approval.

The remediation path should depend on root cause and residual risk.

X. LIFECYCLE GOVERNANCE

Model owners should define monitoring obligations, thresholds, review frequency, evidence retention, and retirement criteria.

Material changes should trigger formal reassessment and, for high-risk systems, renewed approval.

XI. PORTFOLIO MONITORING

Portfolio dashboards should show drift exposure, affected models, unresolved alerts, monitoring coverage, recertification status, and recurring causes.

Portfolio insight supports prioritization and helps identify systemic data or provider issues.

XII. CONCLUSION

Enterprise AI Model Drift Detection and Lifecycle Monitoring Architecture provides a structured approach for maintaining trustworthy AI after deployment.

By combining technical drift detection with business and governance monitoring, organizations can detect degradation earlier and preserve lifecycle assurance.

ACKNOWLEDGMENT

The author acknowledges the contributions of enterprise architecture practitioners, AI governance specialists, standards bodies, security professionals, data leaders, and technology researchers whose published work informed the concepts synthesized in this paper.

REFERENCES

[1] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.
[2] National Institute of Standards and Technology, AI RMF Generative Artificial Intelligence Profile, 2024.
[3] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.
[4] ISO 31000:2018, Risk management — Guidelines.
[5] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems.
[6] The Open Group, TOGAF Standard, 10th Edition, 2022.
[7] ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2019.
[8] OWASP Foundation, OWASP Top 10 for Large Language Model Applications.
[9] MITRE, ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems.
[10] OECD, Recommendation of the Council on Artificial Intelligence.
[11] SAP SE, SAP Business Technology Platform Documentation.
[12] SAP SE, SAP Business Data Cloud and SAP Datasphere Documentation.

 ©IJSRED: All Rights are Reserved