Adaptive Pipeline Monitoring Using Unsupervised Anomaly Detection

(Authors Details)
Agim Takon
Novation Ltd., Canada
Email ID: atakon2000@gmail.com

DOI: https://doi.org/10.21590/ijtmh.2020063-408

Abstract

Infrastructure The pipeline infrastructure plays a major role in the transportation of fluids in the industry safely and efficiently. Conventional monitoring techniques are in many cases based on fixed thresholds or monitored models which have the issue of being restricted by the requirement of labeled failure information as well as they are not easily able to adjust to changing operational environments. The paper discusses an adaptive pipeline monitoring scheme based on the unsupervised anomaly detection algorithm and applies the technique to multi-sensor data streams in order to detect the deviation of the normal operating schemes without prior information of fault events. The framework suggested involves adaptive learning, which will enable the framework to adapt to the changing pipeline dynamics and minimize false alarms to achieve real-time detection and strong operational insights. The metrics of evaluation prove the efficiency of the method in detecting the development of bypass on both the subtle and abrupt levels providing a proactive approach to integrity of the pipeline management and risk prevention.

Keywords: Adaptive monitoring, pipeline integrity, unsupervised anomaly detection, sensor data analytics, real-time fault detection, operational resilience

1. Introduction

The pipeline systems form an important part of the industrial infrastructure as they facilitate steady flow of oil, gas, water and other fluids over a distance. Their operation integrity is necessary because leaks, blockages, corrosion, or mechanical failures have dire safety, environmental and economic impacts. Traditional methods of monitoring the pipeline are mostly rule-based thresholds or supervised learning models that are trained on historical fault data. Yet, those are typically not sufficient in practice when the data on labeled anomalies are limited, the conditions under which the system is going to be used change over time, and the failure modes are different and unforeseen.

The recent progress on unsupervised anomaly detection has shown to have a great potential of tracking complex systems based on streaming sensor data without prior knowledge about fault signatures. Unsupervised methods are based on the model of normal system behavior and detect abnormalities that can point to some kind of abnormality or danger. It is the paradigm best applicable to pipeline environments, with rare anomalies, system dynamics caused by operation changes, and the fault events are difficult to label manually. Studies on real-time and streaming anomaly detection have shown that unsupervised approaches can effectively detect abrupt and subtle deviations while maintaining low false alarm rates (Ahmad et al., 2017; Kathareios et al., 2017).

One of the main issues of using the unsupervised anomaly detection of pipelines is adaptivity. Factors which affect the operation conditions of a pipeline include flow demand, change in pressure, environmental impact, and old infrastructure, which cause concept drift in sensor data streams. Such non-stationary conditions tend to worsen the performance of static models. In order to solve this problem, adaptive anomaly detection schemes are suggested, which allows updating the models and changing the parameters according to the changing data distributions (Ibidunmoye et al., 2017; Yu et al., 2019). Adaptive thresholds and online learning plans have also contributed to the detection robustness of large-scale monitoring facilities and IoT-based systems (Wetzig et al., 2019; Ren et al., 2019).

Simultaneously, progress in deep learning and representation learning has broadened the range of unsupervised anomaly detection approaches in time-series and structural monitoring systems. Autoencoders and deep neural architectures have been applied efficiently to identify anomalies in such temporal sensor data on the one hand and detect physical infrastructure defects on the other hand with improved sensitivity to complex nonlinear patterns (Munir et al., 2018; Chow et al., 2020). Also, adaptive clustering and decentralized learning methods have proven to be useful in resilient and scalable monitoring systems especially in distributed and resource-bound systems (Panga and Thanjaivadivel, 2020; Sikdar and Chowdhury, 2019).

In this context, unsupervised anomaly detection based on adaptive pipeline monitoring becomes one of the strong and scalable methods of the early detection of faults and proactive maintenance. Such systems could be improved to increase situational awareness by integrating real time anomaly scoring, multi-sensor data analysis and continuous learning to help minimize dependence on predefined fault models. This work places adaptive unsupervised anomaly detection as a baseline with regard to enhancing the reliability of pipelines, their resilience with regard to operations and risk reduction in the contemporary industrial monitoring systems.

2. Pipeline Monitoring Data Ecosystem

An effective adaptive pipeline monitoring system is fundamentally dependent on the quality, diversity, and structure of the underlying data ecosystem. Pipelines operate under highly dynamic conditions influenced by flow variability, environmental factors, material aging, and operational interventions. As a result, monitoring data exhibit strong temporal dependencies, nonlinearity, noise, and evolving statistical distributions, making conventional static analytics insufficient for reliable anomaly detection.

2.1 Sensor Infrastructure and Data Sources

Pipeline monitoring relies on a heterogeneous network of sensors deployed along transmission and distribution assets. Common sensing modalities include pressure transducers, flow meters, temperature sensors, vibration and acoustic emission sensors, and, in some cases, imaging or fiber-optic sensing systems. These sensors continuously generate multivariate time-series data streams that reflect the operational state of the pipeline. Similar to Internet-of-Things (IoT) and large-scale network monitoring environments, pipeline data are high-velocity and often unlabelled, which motivates the use of unsupervised and adaptive anomaly detection approaches (Ahmad et al., 2017; Wetzig et al., 2019).

2.2 Data Characteristics and Challenges

Pipeline monitoring data share characteristics observed in performance metric streams and network key performance indicators (KPIs), including abrupt shifts, gradual drifts, and seasonal patterns. Abrupt changes may correspond to leaks, blockages, or mechanical failures, whereas gradual distributional changes often arise from operational adjustments or sensor aging. These phenomena resemble concept drift scenarios described in adaptive anomaly detection literature, where static thresholds or fixed models quickly become obsolete (Ibidunmoye et al., 2017; Yu et al., 2019). Additionally, noise, missing values, and asynchronous sampling further complicate anomaly detection in real-world deployments.

2.3 Data Acquisition and Preprocessing

To support reliable anomaly detection, raw pipeline data must undergo preprocessing stages such as synchronization, noise filtering, normalization, and feature extraction. Sliding window segmentation is commonly employed to capture temporal dependencies while maintaining computational efficiency for real-time processing (Munir et al., 2018; Ren et al., 2019). Feature representations may include statistical descriptors, frequency-domain features, or learned latent embeddings generated by unsupervised deep learning models such as autoencoders. These preprocessing steps establish a stable baseline for adaptive learning while preserving sensitivity to subtle deviations.

2.4 Streaming and Real-Time Data Management

Pipeline monitoring systems typically operate in a streaming environment where data are processed continuously at the edge or in centralized control systems. Low-latency processing is essential to ensure timely detection and response to anomalous events. Studies in real-time network and IoT anomaly detection highlight the importance of lightweight models and incremental updates to maintain scalability and minimize false alarms (Kathareios et al., 2017; Wetzig et al., 2019). These principles directly translate to pipeline monitoring, where delayed or excessive alarms can lead to operational inefficiencies or safety risks.

2.5 Representative Data Types in Pipeline Monitoring

Table 1 summarizes the primary data types commonly found in pipeline monitoring ecosystems, their typical sources, and their relevance to unsupervised anomaly detection.

Table 1. Key Data Types in Pipeline Monitoring Ecosystems

Data Type	Sensor Source	Temporal Resolution	Anomaly Indicators	Relevance to Unsupervised Detection
Pressure Data	Pressure transducers	High-frequency	Sudden drops, oscillations	Detects leaks and ruptures via abrupt deviations
Flow Rate Data	Flow meters	High-frequency	Imbalance, unexpected variation	Identifies blockages and unauthorized extraction
Temperature Data	Thermal sensors	Medium-frequency	Gradual or localized shifts	Indicates corrosion or environmental stress
Vibration/Acoustic Data	Accelerometers, acoustic sensors	Very high-frequency	Pattern changes, spikes	Captures mechanical faults and crack propagation
Operational Logs	SCADA systems	Event-driven	Irregular sequences	Contextualizes sensor anomalies

2.6 Implications for Adaptive Anomaly Detection

The complexity and variability of pipeline monitoring data necessitate anomaly detection methods that can learn normal behavior directly from data while continuously adapting to evolving conditions. Unsupervised and training-less approaches, including adaptive thresholds, clustering, and deep representation learning, have demonstrated effectiveness in analogous domains such as network monitoring, IoT systems, and infrastructure inspection (Sikdar & Chowdhury, 2019; Chow et al., 2020). By leveraging these data ecosystem characteristics, adaptive pipeline monitoring systems can achieve higher robustness, reduced false positives, and improved operational resilience.

3. Unsupervised Anomaly Detection Framework

Unsupervised anomaly detection forms the analytical core of adaptive pipeline monitoring, enabling the identification of abnormal operational behavior without reliance on labeled fault data. This is particularly suitable for pipeline systems, where failure events are rare, heterogeneous, and costly to label. The framework focuses on learning normal operational patterns from continuous multi-sensor data streams and flagging statistically or structurally significant deviations as anomalies.

3.1 Rationale for Unsupervised Detection

Pipeline environments exhibit non-stationary behavior due to variations in flow regimes, pressure fluctuations, seasonal demand, and maintenance activities. Supervised models struggle under these conditions because they assume stable data distributions and comprehensive fault labels. Unsupervised methods instead establish baseline representations of normal behavior and continuously adapt as operational conditions evolve, making them well suited for streaming industrial data (Ahmad et al., 2017; Ibidunmoye et al., 2017).

3.2 Core Detection Approaches

The unsupervised framework integrates multiple algorithmic paradigms to capture different anomaly characteristics:

- **Statistical and threshold-based models**, which estimate normal ranges and detect abrupt deviations, are effective for early warning but require adaptive parameter tuning to reduce false positives (Yu et al., 2019; Wetzig et al., 2019).
- **Clustering and density-based methods** identify sparse or isolated data points in feature space, supporting detection of gradual degradation and collective anomalies (Panga &

Thanjaivadivel, 2020).

- **Tree-based and subspace techniques**, such as half-space trees, efficiently handle high-dimensional streaming data and are suitable for edge-level deployment in pipeline monitoring systems (Wetzig et al., 2019; Kathareios et al., 2017).

- **Deep learning–based representations**, particularly autoencoders and convolutional architectures, learn compressed representations of normal behavior and use reconstruction error as an anomaly score, enabling detection of subtle and nonlinear deviations (Munir et al., 2018; Chow et al., 2020).

3.3 Streaming and Online Adaptation

Pipeline monitoring requires real-time or near-real-time analysis. The framework therefore emphasizes online learning and incremental updates, allowing the model to adapt to concept drift without retraining from scratch. Parameter adaptation and sliding-window strategies help distinguish between genuine faults and benign operational changes, maintaining stable detection performance over long-term deployments (Yu et al., 2019; Ren et al., 2019).

3.4 Anomaly Scoring and Alert Generation

Detected deviations are translated into anomaly scores that quantify severity and persistence. Short-lived spikes may indicate transient disturbances, while sustained high scores suggest leaks, blockages, or structural degradation. Adaptive thresholds and ensemble scoring mechanisms are employed to balance sensitivity and false alarm rates, a critical requirement for operator trust and practical deployment (Kathareios et al., 2017; Sikdar & Chowdhury, 2019).

Overall, the unsupervised anomaly detection framework provides a flexible and adaptive foundation for pipeline monitoring, enabling continuous learning, real-time detection, and robust operation under evolving industrial conditions without dependence on labeled fault data.

4. Adaptive Learning Mechanisms

Adaptive learning mechanisms are central to unsupervised anomaly detection in pipeline monitoring systems, as they enable models to remain effective under evolving operational and environmental conditions. Pipeline systems are subject to concept drift caused by changes in flow regimes, pressure profiles, seasonal demand, maintenance activities, and sensor aging. Static models trained on historical data are therefore prone to performance degradation and increased false alarms over time. Adaptive mechanisms address this limitation by continuously updating model parameters and decision boundaries in response to streaming data.

Table 2. Major Unsupervised Anomaly Detection Techniques Relevant to Pipeline Monitoring

Method Category	Representative Techniques	Key Strengths	Limitations	Relevant Studies
Statistical / Threshold-Based	Adaptive thresholds, KPI change detection	Fast, interpretable, low computational cost	Sensitive to noise, limited for complex patterns	Yu et al. (2019); Wetzig et al. (2019)
Clustering & Density-Based	DBSCAN, adaptive DBSCAN	Detects collective and gradual anomalies	Parameter sensitivity, scalability issues	Panga & Thanjaivadivel (2020)
Tree & Subspace Methods	Half-space trees	Efficient for streaming, high-dimensional data	Reduced interpretability	Wetzig et al. (2019); Kathareios et al. (2017)
Deep Learning Models	Autoencoders, convolutional autoencoders	Captures nonlinear and subtle anomalies	Higher computational demand	Munir et al. (2018); Chow et al. (2020)
Online Service-Oriented Systems	Incremental time-series models	Robust to concept drift, production-ready	Complex system integration	Ren et al. (2019)

One core adaptive strategy involves online and incremental learning, where model parameters are updated as new observations arrive, rather than relying on periodic retraining. Techniques such as adaptive statistical modeling and online clustering dynamically recalibrate baseline behavior to reflect current pipeline states, allowing the system to distinguish genuine anomalies from normal operational shifts (Yu et al., 2019; Ibidunmoye et al., 2017). This approach is particularly effective for high-frequency sensor data where abrupt KPI changes may occur without prior labeling.

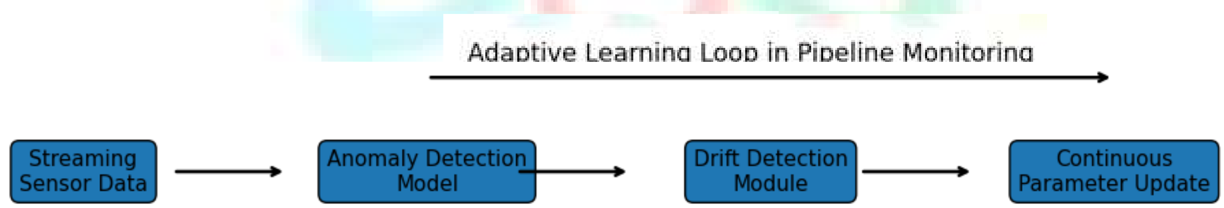
Another important mechanism is adaptive thresholding, which replaces fixed alarm thresholds with data-driven, context-aware limits. Adaptive thresholds are computed based on recent data distributions, anomaly scores, or density estimates, ensuring sensitivity to subtle deviations while controlling false-positive rates (Wetzig et al., 2019; Kathareios et al., 2017). In pipeline monitoring, this is critical for handling gradual pressure changes or transient disturbances that do not indicate structural faults.

Representation learning through adaptive deep models further enhances anomaly detection performance. Autoencoder-based architectures and deep temporal models learn compact representations of normal pipeline behavior and update these representations as system dynamics evolve. Models such as DeepAnT and convolutional autoencoders have demonstrated robustness in capturing non-linear temporal and spatial dependencies, enabling the detection of both localized and system-wide anomalies without explicit retraining on labeled fault data (Munir et al., 2018; Chow et al., 2020).

To support scalability and distributed monitoring, adaptive clustering and federated learning approaches can be employed across pipeline segments and edge devices. These methods allow localized adaptation while preserving global consistency, reducing communication overhead and improving resilience in large-scale infrastructures (Panga & Thanjaivadivel, 2020). Training-less and self-adjusting mechanisms further reduce operational complexity by eliminating manual parameter tuning (Sikdar & Chowdhury, 2019).

Finally, adaptive learning mechanisms must incorporate drift detection and validation logic to prevent model corruption due to persistent anomalies or sensor faults. By separating short-term anomalies from long-term behavioral changes, the system maintains stability while remaining responsive to genuine pipeline degradation (Ahmad et al., 2017; Ren et al., 2019).

Fig 1: This figure illustrates an adaptive learning framework for pipeline monitoring in which streaming sensor data are continuously analyzed for anomalies, monitored for concept drift, and used to update model parameters, ensuring sustained detection accuracy under evolving operational conditions.



Overall, adaptive learning mechanisms enable unsupervised anomaly detection systems to operate reliably in real-world pipeline environments, supporting continuous integrity assessment and proactive risk management without dependence on labeled failure data.

5. Anomaly Scoring and Decision Logic

Anomaly scoring and decision logic form the core operational layer of adaptive pipeline monitoring systems, translating model outputs into actionable insights. In unsupervised anomaly detection, raw deviations identified by learning models must be quantified, contextualized, and evaluated to distinguish genuine pipeline threats from benign operational variability.

5.1 Anomaly Scoring Mechanisms

Anomaly scoring assigns a numerical value representing the degree of deviation between observed pipeline behavior and learned baseline patterns. Common scoring approaches include reconstruction error, distance-based deviation, density estimation, and probabilistic likelihood. For time-series sensor data, reconstruction-based scores widely used in autoencoder and deep learning models measure the discrepancy between observed signals and model-generated reconstructions, with larger errors indicating potential anomalies (Munir et al., 2018; Chow et al., 2020).

Distance-based and clustering-driven scores assess how far new observations deviate from established normal clusters, while density-based approaches assign lower likelihoods to sparse or isolated observations (Ibidunmoye et al., 2017; Sikdar & Chowdhury, 2019). In streaming pipeline environments, anomaly scores are often normalized to accommodate sensor heterogeneity and varying operational scales, ensuring comparability across multiple data streams (Ahmad et al., 2017; Ren et al., 2019).

5.2 Adaptive Thresholding Strategies

Static thresholds are inadequate for pipeline systems subject to fluctuating flow rates, pressure regimes, and environmental conditions. Adaptive thresholding dynamically adjusts decision boundaries based on recent data distributions, historical trends, or model confidence intervals. Techniques such as exponentially weighted moving averages, percentile-based thresholds, and adaptive control limits enable continuous recalibration of anomaly sensitivity (Yu et al., 2019; Wetzig et al., 2019).

Adaptive thresholds reduce false positives during transient operational changes while preserving sensitivity to persistent abnormal patterns. Parameter adaptation mechanisms further refine thresholds by responding to concept drift, ensuring long-term stability in anomaly detection performance (Ibidunmoye et al., 2017; Kathareios et al., 2017).

5.3 Multi-Sensor Score Fusion

Pipeline monitoring typically relies on heterogeneous sensors capturing pressure, flow, temperature, vibration, and acoustic signals. Individual anomaly scores derived from each sensor are aggregated using score fusion strategies to improve detection robustness. Common fusion methods include weighted averaging, voting-based aggregation, and probabilistic combination, where sensor reliability and historical relevance influence final anomaly confidence (Ahmad et al., 2017; Ren et al., 2019).

Fusion-based decision logic mitigates single-sensor noise effects and enhances detection of complex fault scenarios, such as leaks or blockages that manifest across multiple modalities rather than a single parameter.

Table 3: Anomaly Scoring and Decision Logic Techniques in Adaptive Monitoring

Component	Technique	Description	Key References
Anomaly Scoring	Reconstruction Error	Measures deviation between observed and reconstructed signals	Munir et al. (2018); Chow et al. (2020)
Anomaly Scoring	Distance/Density-Based Scores	Identifies deviations from learned normal clusters	Ibidunmoye et al. (2017); Sikdar & Chowdhury (2019)
Thresholding	Adaptive Thresholds	Dynamic adjustment of decision boundaries	Yu et al. (2019); Wetzig et al. (2019)
Decision Logic	Streaming Decision Models	Real-time evaluation of anomaly persistence	Ahmad et al. (2017); Ren et al. (2019)
Score Fusion	Multi-Sensor Aggregation	Combines scores across heterogeneous sensors	Kathareios et al. (2017); Ren et al. (2019)

5.4 Decision Logic and Alert Generation

Decision logic integrates anomaly scores, adaptive thresholds, and temporal persistence rules to determine whether an alert should be triggered. Short-lived spikes are often filtered using temporal smoothing or consecutive anomaly confirmation windows, preventing unnecessary alarms caused by noise or transient disturbances (Kathareios et al., 2017; Wetzig et al., 2019).

Alerts are prioritized based on severity, spatial correlation, and historical risk profiles, enabling operators to focus on high-impact events. In advanced implementations, decision logic supports automated responses such as valve isolation or flow regulation, contributing to proactive pipeline integrity management (Yu et al., 2019; Panga & Thanjaivadivel, 2020).

6. Performance Evaluation Metrics

Evaluating adaptive pipeline monitoring systems based on unsupervised anomaly detection requires metrics that capture detection accuracy, timeliness, robustness, and operational relevance. Since labeled failure data are often unavailable or incomplete in pipeline environments, performance assessment emphasizes indirect and behavior-based evaluation criteria rather than conventional supervised accuracy alone (Ahmad et al., 2017; Yu et al., 2019).

6.1 Detection Accuracy and Reliability

Detection performance is commonly assessed using precision, recall, and F1-score when limited ground truth or expert-labeled anomaly windows are available. Precision reflects the system's ability to minimize false alarms, while recall measures sensitivity to genuine abnormal events such as leaks, blockages, or pressure instabilities. Maintaining a balance between these metrics is critical for operational trust, as excessive false positives can lead to alarm fatigue (Kathareios et al., 2017; Ren et al., 2019).

6.2 False Alarm Rate and Stability

The false positive rate (FPR) is a key metric in continuous pipeline monitoring, particularly under fluctuating flow regimes and seasonal demand variations. Adaptive thresholding and parameter tuning mechanisms are evaluated based on their ability to suppress spurious alerts while preserving anomaly sensitivity (Wetzig et al., 2019; Ibidunmoye et al., 2017). A stable monitoring system should demonstrate low variance in alert frequency during normal operations.

6.3 Detection Latency

Detection latency measures the time elapsed between the onset of an abnormal event and its identification by the monitoring system. Low latency is essential for mitigating safety and environmental risks in pipeline operations. Streaming and online anomaly detection approaches are evaluated based on their responsiveness under real-time constraints, particularly for abrupt KPI shifts or gradual fault evolution (Yu et al., 2019; Ahmad et al., 2017).

6.4 Anomaly Scoring Consistency

Unsupervised systems often produce continuous anomaly scores rather than binary labels. Performance evaluation includes analyzing score separability between normal and abnormal operational states, as well as score consistency across time and sensor modalities. Autoencoder-based and clustering-based approaches are assessed for their ability to generate stable and interpretable anomaly magnitudes (Munir et al., 2018; Chow et al., 2020).

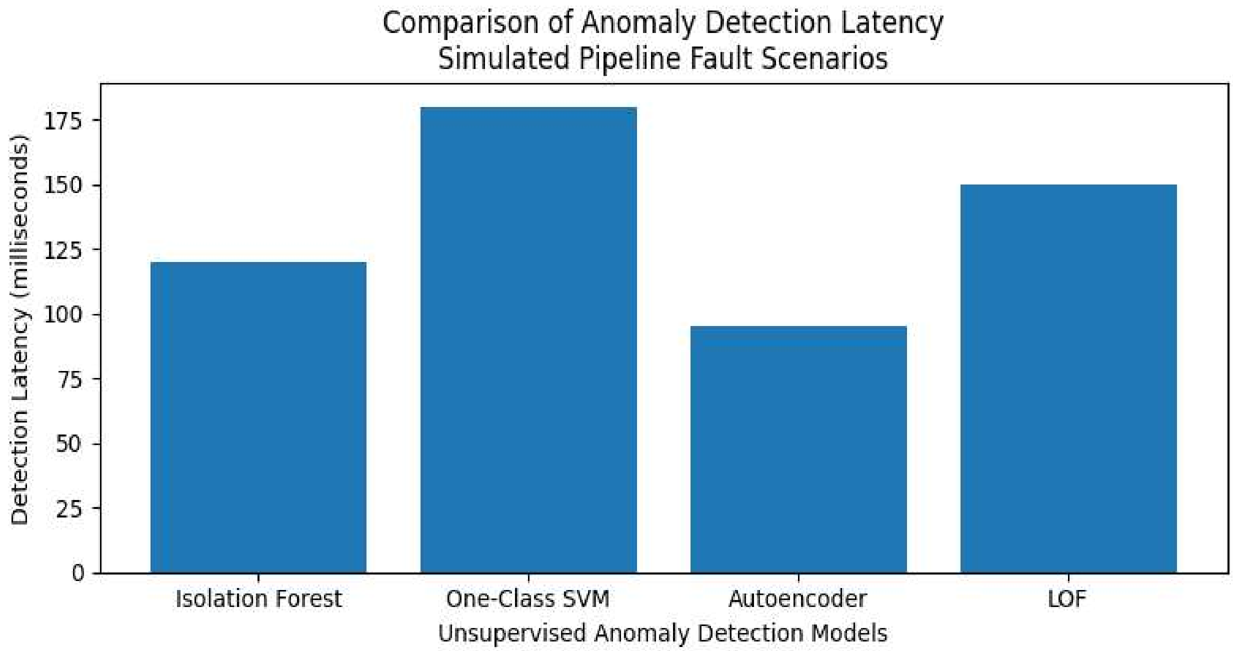


Fig 2: Detection latency values are illustrative and derived from simulated pipeline fault scenarios, highlighting relative responsiveness of unsupervised anomaly detection models rather than absolute performance benchmarks.

6.6 Computational Efficiency and Scalability

Computational cost, memory usage, and scalability are critical metrics for deployment in large-scale pipeline networks. Performance evaluation considers model inference time, adaptability to high-frequency data streams, and feasibility of edge or gateway-level deployment. Lightweight adaptive models are favored for real-time operation in resource-constrained environments (Wetzig et al., 2019; Panga & Thanjaivadivel, 2020).

6.7 Operational Impact Assessment

Beyond algorithmic metrics, evaluation includes operational impact indicators, such as reduction in unplanned downtime, improved maintenance scheduling, and enhanced situational awareness. These metrics link anomaly detection performance to tangible pipeline integrity outcomes, reinforcing the practical value of adaptive unsupervised monitoring systems (Ren et al., 2019).

Conclusion

Adaptive pipeline monitoring using unsupervised anomaly detection provides a robust and scalable approach for ensuring pipeline integrity under dynamic operational conditions. By eliminating dependence on labeled fault data, unsupervised methods enable continuous learning of normal system behavior and support early detection of both abrupt and gradual deviations in pipeline performance. This is particularly critical for large-scale pipeline networks where failure events are rare, heterogeneous, and costly to label accurately.

The incorporation of adaptive learning mechanisms allows monitoring systems to respond effectively to concept drift, seasonal variations, and evolving operational profiles. Prior studies have demonstrated that online parameter adaptation and training-less detection models significantly improve responsiveness while maintaining low false alarm rates in streaming environments (Yu et al., 2019; Ibidunmoye et al., 2017; Kathareios et al., 2017). Techniques such as adaptive thresholding, density-based clustering, and half-space trees further enhance anomaly sensitivity in resource-constrained and distributed monitoring architectures (Wetzig et al., 2019; Panga & Thanjaivadivel, 2020).

Deep learning–based unsupervised approaches, including autoencoders and temporal neural architectures, offer strong capabilities for modeling complex, nonlinear pipeline sensor data and detecting subtle structural or operational anomalies (Munir et al., 2018; Chow et al., 2020). When combined with real-time streaming analytics frameworks, these methods enable low-latency detection and scalable deployment across edge and cloud environments (Ahmad et al., 2017; Ren et al., 2019). Such integration supports proactive maintenance strategies and enhances situational awareness for pipeline operators.

Despite these advantages, practical challenges remain, including interpretability of anomaly alerts, resilience to noise, and secure integration with existing industrial control systems. Addressing these challenges through explainable models and adaptive fusion of multi-sensor data will be essential for broader industrial adoption. Overall, adaptive unsupervised anomaly detection represents a critical advancement in pipeline monitoring, offering a resilient, data-driven foundation for safeguarding critical infrastructure and optimizing operational reliability.

References

1. Yu, G., Cai, Z., Wang, S., Chen, H., Liu, F., & Liu, A. (2019). Unsupervised online anomaly detection with parameter adaptation for KPI abrupt changes. *IEEE Transactions on Network and Service Management*, *17*(3), 1294-1308.
2. Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data. *Neurocomputing*, *262*, 134-147.

3. Ibidunmoye, O., Rezaie, A. R., & Elmroth, E. (2017). Adaptive anomaly detection in performance metric streams. *IEEE Transactions on Network and Service Management*, *15*(1), 217-231.
4. Wetzig, R., Gulenko, A., & Schmidt, F. (2019, October). Unsupervised anomaly alerting for iot-gateway monitoring using adaptive thresholds and half-space trees. In *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 161-168). IEEE.
5. Kathareios, G., Anghel, A., Mate, A., Clauberg, R., & Gusat, M. (2017, December). Catch it if you can: Real-time network anomaly detection with low false alarm rates. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 924-929). IEEE.
6. Munir, M., Siddiqui, S. A., Dengel, A., & Ahmed, S. (2018). DeepAnT: A deep learning approach for unsupervised anomaly detection in time series. *Ieee Access*, *7*, 1991-2005.
7. Chow, J. K., Su, Z., Wu, J., Tan, P. S., Mao, X., & Wang, Y. H. (2020). Anomaly detection of defects on concrete structures with the convolutional autoencoder. *Advanced Engineering Informatics*, *45*, 101105.
8. Panga, N. K. R., & Thanjaivadivel, M. (2020). Adaptive DBSCAN and Federated Learning-Based Anomaly Detection for Resilient Intrusion Detection in Internet of Things Networks. *International Journal of Management Research and Business Strategy*, *10*(4), 39-56.
9. Sikdar, A., & Chowdhury, A. S. (2019). An adaptive training-less system for anomaly detection in crowd scenes. *arXiv preprint arXiv:1906.00705*.
10. Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., ... & Zhang, Q. (2019, July). Time-series anomaly detection service at microsoft. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining* (pp. 3009-3017).
11. Kumar, S. (2007). *Patterns in the daily diary of the 41st president, George Bush* (Doctoral dissertation, Texas A&M University).
12. Uppuluri, V. (2019). The Role of Natural Language Processing (NLP) in Business Intelligence (BI) for Clinical Decision Support. *ISCSITR-INTERNATIONAL JOURNAL OF BUSINESS INTELLIGENCE (ISCSITR-IJBI)*, *1*(2), 1-21.
13. Uppuluri, V. (2020). Integrating behavioral analytics with clinical trial data to inform vaccination strategies in the US retail sector. *J Artif Intell Mach Learn & Data Sci*, *1*(1), 3024-3030.
14. Taorui Guan, "Evidence-Based Patent Damages," 28 Journal of Intellectual Property Law (2020), 1-61.