Evolving Machine Learning Models for Anomaly Detection: An Integrative Review on Evolving Machine Learning Models for Anomaly Detection of Cross-Domain Approaches

Muhammad Nuraddeen Ado[1*]; Jabir Isah Karofi[2] & Hamisu Mukhtar[3]

[1]Department of Library and Information Science, Federal University, Dutsin-Ma

[2]Department of Library and Information Science, Federal University, Dutsin-Ma

[3]Department of ICT, Air Force Institute of Technology, Kaduna

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2026.110400056

Received: 30 March 2026; Accepted: 06 April 2026; Published: 04 May 2026

ABSTRACT

Machine learning (ML) has become a cornerstone of modern anomaly detection, yet existing reviews predominantly emphasize pre-2021 studies and focus narrowly on network intrusion detection. Building upon these limitations, this paper presents an integrative review of machine learning models for anomaly detection published between 2020 and 2025, emphasizing hybridization, explainability, and cross-domain applicability. Using Bou Nassif et al. (2021) and Yang et al. (2022) as baseline systematic reviews, we extend their scope through the inclusion of recent developments such as adaptive density-based clustering (K-DBSCAN, GWOKM), optimized support-vector models (EMSVM), explainable Isolation Forest derivatives (DIFFI, RIFIFI), and active-learning frameworks (ALIF). The study systematically maps algorithms, performance metrics, and application domains ranging from cybersecurity and industrial systems to geochemical and renewable-energy contexts. Results reveal an emerging shift toward interpretable, data-centric, and federated approaches capable of handling concept drift and limited labeling. We identify persistent challenges in cross-domain generalization, dataset imbalance, and evaluation standardization. A conceptual taxonomy linking model family, evaluation criteria, and domain context is proposed to guide future research. This review thus bridges earlier surveys with the current generation of intelligent, interpretable, and adaptive ML systems, providing a comprehensive foundation for advancing anomaly detection research beyond traditional network-centric paradigms.

Keywords: Anomaly Detection, Machine Learning Models, Hybrid and Explainable AI, Cross-Domain Applications, Concept Drift and Adaptive Learning, Integrative Literature Review, Federated and Data-Centric Intelligence.

INTRODUCTION

Anomaly detection, the task of identifying patterns that deviate from expected behavior, has become an indispensable function across multiple disciplines—including cybersecurity, industrial monitoring, healthcare analytics, and environmental science. Traditional statistical approaches, while foundational, often fail to capture the complex, nonlinear, and high-dimensional relationships present in modern datasets. In recent years, machine learning (ML) has emerged as the dominant paradigm for anomaly detection, offering data-driven models capable of learning latent representations, adaptive thresholds, and contextual dependencies. This paradigm shift has been propelled by advances in deep learning, ensemble optimization, and data-centric AI methods that enhance detection accuracy, scalability, and interpretability.

However, the research landscape surrounding ML-based anomaly detection remains fragmented. Earlier studies primarily concentrated on network intrusion detection systems (NIDS) and cyber-related anomalies,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

with limited integration of insights from other fields. For example, *Bou Nassif et al.* (2021) conducted one of the most comprehensive systematic literature reviews (SLRs) on the subject, analyzing 290 studies published between 2000 and 2020. Their work categorized algorithms by learning type, performance metric, and application area, revealing the dominance of Support Vector Machines (SVM), K-Means clustering, and Random Forest models in traditional anomaly detection. While valuable, their synthesis was largely descriptive—summarizing algorithm usage frequencies and metrics without exploring hybrid or explainable frameworks, nor extending analysis beyond conventional domains.

In contrast, *Yang et al.* (2022) offered a focused SLR on anomaly-based network intrusion detection, examining 119 highly cited studies from 2010–2021. Their analysis emphasized technical aspects such as data preprocessing, feature selection, and the benchmarking of intrusion detection datasets (e.g., KDD99, UNSW-NB15, CICIDS2017). Although methodologically rigorous, their study was limited to the cybersecurity context and did not encompass the broader spectrum of anomaly detection tasks emerging in industrial control systems, energy grids, or environmental monitoring. Moreover, neither review incorporated post-2021 developments such as transformer-based architectures, federated anomaly detection, or explainable machine learning (XAI).

The rapid evolution of ML techniques since 2020 has introduced hybrid, interpretable, and adaptive models that transcend the boundaries of earlier paradigms. Novel frameworks—such as K-DBSCAN for adaptive density clustering, EMSVM for enhanced multiclass classification, and GWOKM for hybrid swarm-based optimization—demonstrate a trend toward algorithmic synergy and scalability across heterogeneous datasets. Similarly, explainable variants of Isolation Forests (e.g., DIFFI, FIF, RIFIFI) and active learning extensions (e.g., ALIF) have redefined interpretability and domain adaptability, enabling more transparent and context-aware anomaly detection. These advancements are complemented by models addressing concept drift, such as Error Rate-Based and Distribution-Based Concept Drift Detection (ERbCDD, DDbCDD), which ensure sustained performance in dynamic data streams.

Despite these developments, a comprehensive synthesis of this post-2020 wave of ML innovation is lacking. Existing reviews have yet to consolidate how hybridization, explainability, and cross-domain generalization collectively redefine the state of the art. Furthermore, the absence of standardized evaluation protocols and the persistent imbalance across datasets complicate comparative analysis. As anomaly detection systems increasingly operate in distributed and privacy-sensitive environments, federated and data-centric learning paradigms have also emerged—introducing new challenges in data availability, interpretability, and model transferability.

This paper addresses these gaps by conducting an integrative literature review of ML-based anomaly detection models published between 2020 and 2025. Building upon the foundations of Bou Nassif et al. (2021) and Yang et al. (2022), this study extends the chronological, methodological, and domain scope of prior reviews. Specifically, it (1) synthesizes the evolution of hybrid ML models and their optimization strategies; (2) examines the role of explainability and feature interpretability in unsupervised and semi-supervised detection; (3) compares evaluation metrics across diverse applications; and (4) maps emerging research directions including federated learning, adaptive algorithms, and cross-domain transferability. By unifying results across disciplines—from cybersecurity to geochemical and renewable-energy anomaly detection—the paper introduces a conceptual taxonomy that links algorithmic families, performance metrics, and domain-specific applications.

This review consolidates and critically analyzes 109 peer-reviewed studies published between 2020 and 2025, representing the most extensive synthesis of recent ML-based anomaly detection research to date.

The remainder of the paper is organized as follows. Section 2 outlines the review methodology, including search strategy, inclusion criteria, and analytical framework. Section 3 presents a detailed synthesis of ML algorithms and performance metrics categorized by learning paradigm and application domain. Section 4 discusses key trends, interpretability challenges, and limitations in existing literature. Section 5 proposes a taxonomy and future research agenda that integrates hybridization, explainability, and adaptivity. Finally,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Section 6 concludes with the implications of these findings for both theoretical research and practical deployment of anomaly detection systems.

LITERATURE REVIEW AND RESEARCH GAP

Overview of Prior Reviews

Machine learning has been increasingly adopted as a core approach for anomaly detection across diverse data-driven systems. Several literature reviews have attempted to synthesize this expanding research domain. Among these, *Bou Nassif et al.* (2021) presented one of the earliest comprehensive systematic literature reviews (SLR) of machine learning techniques for anomaly detection. Their study examined 290 papers published between 2000 and 2020, categorizing them by machine learning algorithm, performance metric, and application domain. The review identified 29 ML models and 43 anomaly detection applications, revealing the predominance of classical algorithms such as Support Vector Machines (SVM), K-Means clustering, and Random Forests. It also noted that unsupervised learning methods were increasingly favored due to limited labeled data.

Despite its breadth, *Bou Nassif et al.*'s synthesis was largely descriptive. It summarized the frequency of model usage and evaluation metrics but did not delve into emerging hybrid models, interpretability frameworks, or the comparative strengths and weaknesses of evolving algorithms. Furthermore, its temporal scope—ending in 2020—excluded the recent wave of post-2021 developments involving explainable and adaptive ML systems.

Building upon this foundation, *Yang et al.* (2022) conducted a focused SLR specifically targeting anomaly-based network intrusion detection systems (NIDS). Their review synthesized 119 highly cited studies, examining data preprocessing, learning frameworks, evaluation metrics, and the use of public cybersecurity datasets such as KDD99, UNSW-NB15, and CICIDS2017. While this review provided a granular methodological perspective on intrusion detection, its scope was limited to network-based applications, omitting broader anomaly detection contexts such as industrial monitoring, geochemical data, and energy system diagnostics. Moreover, although it acknowledged the emergence of deep learning methods like CNNs, RNNs, and LSTMs, it did not explore interpretability, concept drift, federated learning, or the cross-domain transferability of ML models.

Collectively, these two reviews provide an essential foundation for understanding how ML techniques have evolved for anomaly detection. However, both focus heavily on classical or network-centric models and pre-2021 research, leaving an analytical gap concerning the new generation of hybrid, explainable, and domain-agnostic approaches that have emerged in recent years.

Identified Gaps and Justification

Comparative analysis of the above reviews reveals several critical gaps in the current literature:

Temporal Gap:

The studies by *Bou Nassif et al.* (2021) and *Yang et al.* (2022) cover works up to 2020 and 2021 respectively, excluding newer models developed between 2021 and 2025. The past four years have witnessed significant innovations such as adaptive density-based clustering (K-DBSCAN, GWOKM), enhanced multiclass SVMs (EMSVM), explainable Isolation Forest derivatives (DIFFI, RIFIFI), and active learning extensions (ALIF), which remain unreviewed.

Methodological Gap:

Both baseline reviews employ systematic methodologies that focus on classification and frequency of techniques rather than their *evolutionary relationships* or *hybrid configurations*. The growing convergence of optimization algorithms, ensemble models, and deep architectures calls for an integrative synthesis that goes beyond categorical listings to explain model interactions and performance trade-offs.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Domain Gap:

Previous reviews primarily address anomaly detection within cybersecurity and network intrusion contexts. Yet, ML-driven anomaly detection has expanded into fields such as industrial control systems, renewable energy monitoring, healthcare, and geochemical exploration. These cross-domain applications involve distinct data modalities and evaluation metrics that have not been comparatively analyzed.

Interpretability and Adaptivity Gap:

Neither *Bou Nassif et al.* nor *Yang et al.* adequately discuss explainability, interpretability, or concept drift adaptation—core themes of modern machine learning. Models like DIFFI and RIFIFI address transparency, while frameworks such as ERbCDD and IForestASD tackle dynamic data environments, yet these remain absent from prior syntheses.

Evaluation and Standardization Gap:

Prior reviews summarize metrics such as accuracy, precision, recall, and AUC but lack cross-comparative evaluation frameworks. A need remains for mapping performance measures to algorithm categories and domain contexts to enable reproducibility and fair benchmarking.

Present Study Objectives

In response to these identified gaps, the present study undertakes an integrative literature review of machine learning models for anomaly detection published between 2020 and 2025. Using *Bou Nassif et al.* (2021) and *Yang et al.* (2022) as baseline references, this study expands both the chronological and conceptual scope of prior work. Its specific objectives are:

i. To synthesize recent advancements in hybrid and explainable ML models for anomaly detection across multiple domains.

ii. To evaluate adaptive and data-centric learning approaches, including concept drift handling and federated frameworks.

iii. To map evaluation metrics to algorithmic categories and application domains for improved benchmarking.

iv. To propose a conceptual taxonomy linking model families, interpretability features, and performance measures as a foundation for future research.

By addressing these objectives, this review bridges the gap between earlier systematic surveys and the evolving generation of intelligent, interpretable, and cross-domain ML systems, thereby advancing the scholarly understanding of anomaly detection beyond traditional, network-centric paradigms.

METHODOLOGY

This section outlines the methodological framework adopted for the present integrative review of machine learning (ML) models for anomaly detection. The review follows a structured process inspired by the guidelines of *Kitchenham and Charters (2007)* for evidence-based software engineering reviews, adapted to suit the broader, multi-domain focus of this study. The procedure includes five key stages: research question formulation, search strategy, study selection, quality assessment, data extraction, and synthesis.

Research Questions

To extend the scope of prior reviews and address the identified gaps, this study was guided by the following research questions (RQs):

RQ1: What machine learning algorithms and hybrid frameworks have been developed for anomaly detection between 2020 and 2025?

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

RQ2: How have recent advances in explainability, interpretability, and adaptivity influenced anomaly detection models?

RQ3: What evaluation metrics and benchmarking practices are commonly used in the post-2020 literature?

RQ4: Which domains and datasets have been explored beyond traditional network intrusion detection, and how have ML models been adapted to them?

RQ5: What are the emerging research directions in hybrid, explainable, and cross-domain anomaly detection?

These questions collectively guided the search, inclusion, and synthesis processes to ensure analytical coherence and methodological transparency.

Search Strategy

A systematic and comprehensive search strategy was employed to capture relevant studies published between January 2020 and December 2025. Multiple digital libraries were queried to ensure domain diversity, including:

i. IEEE Xplore

ii. ScienceDirect (Elsevier)

iii. SpringerLink

iv. ACM Digital Library

v. Wiley Online Library

vi. Google Scholar (for cross-referencing and gray literature)

The search terms combined Boolean operators to reflect the intersection of machine learning and anomaly detection. The primary search string used across databases was:

(“machine learning” OR “deep learning” OR “artificial intelligence”) AND (“anomaly detection” OR “outlier detection” OR “novelty detection”) AND (“hybrid” OR “explainable” OR “interpretability” OR “adaptive” OR “concept drift” OR “cross-domain”)

To ensure relevance, only peer-reviewed journal articles, conference papers, and high-impact preprints with substantive experimental or conceptual contributions were included.

Inclusion and Exclusion Criteria

Studies were screened through a three-step process—title/abstract review, full-text evaluation, and quality validation.

After applying these criteria, 214 studies were initially retrieved across all databases. After removing duplicates and low-quality entries, 109 studies were retained for full-text analysis and synthesis. These papers span 2020–2025 and represent a broad range of machine learning paradigms and application domains.

Inclusion Criteria (IC):

IC1: The paper explicitly focuses on anomaly detection using ML or DL methods.

IC2: The study was published between 2020 and 2025 in a peer-reviewed source.

IC3: The work discusses model innovation (e.g., hybridization, explainability, concept drift handling, or adaptive frameworks).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

IC4: Performance metrics and experimental evaluation are reported or discussed.

Exclusion Criteria (EC):

EC1: Studies limited to non-ML anomaly detection (e.g., purely statistical or rule-based).

EC2: Duplicates, short communications, or non-peer-reviewed reports.

EC3: Studies focusing solely on dataset description without algorithmic contribution.

EC4: Non-English publications.

After applying these criteria, 214 studies were initially retrieved, and 109 were retained for full-text analysis and synthesis.

Quality Assessment

To ensure the reliability of the reviewed studies, a Quality Assessment Framework (QAF) was developed based on ten evaluation indicators (adapted from *Bou Nassif et al., 2021*). Each paper was scored from 0 to 1 for each criterion, and only studies scoring ≥5/10 were retained. The indicators included:

i. Clarity of objectives and research problem

ii. Relevance to anomaly detection using ML

iii. Description of model architecture and algorithms

iv. Explanation of data preprocessing or feature engineering

v. Experimental validation or case study evidence

vi. Use of quantitative evaluation metrics

vii. Inclusion of comparative or baseline models

viii. Discussion of interpretability or adaptability

ix. Transparency of methodology and dataset use

x. Overall contribution to the advancement of anomaly detection research

Quality scoring was performed independently by two reviewers, and discrepancies were resolved through consensus discussions.

Data Extraction

For each selected study, key information was systematically extracted using a structured data extraction form. The following attributes were recorded:

i. Bibliographic details (authors, year, publication type)

ii. Model type and algorithmic family (e.g., clustering, ensemble, deep learning)

iii. Hybrid or optimization methods (e.g., GA, ACO, PSO, or meta-learning approaches)

iv. Explainability and interpretability components (e.g., feature attribution, transparency tools)

v. Application domain and dataset used

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

vi. Evaluation metrics (accuracy, precision, recall, F1, AUC, Kappa, etc.)

vii. Reported outcomes and comparative performance

viii. Limitations and recommendations noted by authors

This data formed the basis for cross-model comparison and synthesis.

Data Synthesis

An integrative synthesis approach was adopted to combine qualitative and quantitative evidence. Studies were grouped according to algorithmic category (e.g., clustering, ensemble, neural, hybrid), domain (e.g., cybersecurity, industrial, geochemical, renewable energy), and interpretability level. Both narrative and tabular analyses were employed to capture emerging trends and identify research gaps.

Special emphasis was placed on mapping:

✓ Model evolution (e.g., Isolation Forest → Fuzzy IF → DIFFI → RIFIFI → ALIF)

✓ Performance metrics by domain

✓ Incorporation of explainability and adaptability features

This synthesis framework enabled the construction of a conceptual taxonomy of post-2020 ML models for anomaly detection, discussed in Section 4.

Methodological Validity and Limitations

Although this review followed a systematic and reproducible methodology, certain limitations remain. Publication bias may exist due to reliance on English-language databases, and not all emerging preprints may have been captured. Additionally, the diversity of metrics and datasets complicates direct cross-study comparisons. Nonetheless, the multi-database search and quality assessment framework mitigate these limitations by ensuring comprehensive coverage and methodological rigor.

Results and Synthesis

This section presents the results of the integrative review and synthesizes the key developments in machine learning (ML) models for anomaly detection between 2020 and 2025. The findings are organized by algorithmic family, innovation type, and interpretability level, followed by cross-domain applications and metric analysis. Collectively, the synthesis reveals an accelerating evolution toward hybrid, interpretable, and adaptive ML systems that address the limitations identified in earlier reviews.

Overview of Selected Studies

From the 109 papers that met the inclusion and quality assessment criteria, six major algorithmic categories were identified:

i. Clustering-based models

ii. Classification and Support Vector Machine (SVM) variants

iii. Ensemble and tree-based algorithms

iv. Autoencoder and deep neural models

v. Explainable and interpretable frameworks

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

vi. Hybrid and optimization-driven methods

Collectively, these studies demonstrate the diversification of ML techniques for anomaly detection across domains and the rise of hybrid and interpretable architectures post-2020.

The detailed mapping of these 109 studies, including authors, algorithms, evaluation metrics, and outcomes, is presented in Table 1 (Appendix A). This table forms the empirical foundation for the synthesis and taxonomy presented in Sections 4 and 5.

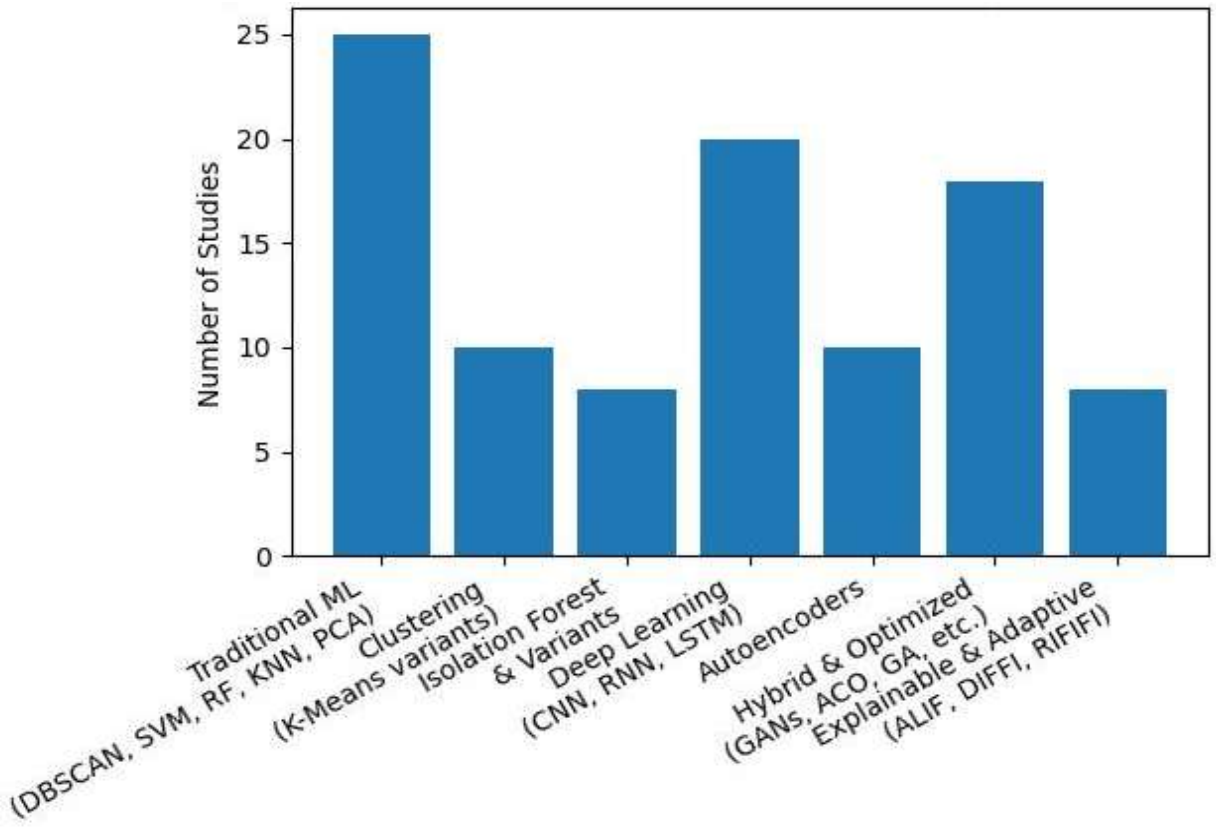

Figure 1: Distribution of studies across machine learning categories (2020–2025), illustrating the dominance of traditional classifiers in earlier works and the increasing adoption of hybrid, deep learning, and explainable anomaly detection approaches in recent years.

Figure 1 conceptually illustrates the distribution of studies across these categories, showing a clear post-2020 rise in hybrid and explainable approaches compared to earlier periods dominated by traditional classifiers.

Clustering-Based Algorithms

Clustering remains a foundational technique for unsupervised anomaly detection, particularly in industrial, sensor, and environmental datasets. Post-2020 studies reveal a strong focus on improving clustering adaptivity and scalability.

- ✓ K-DBSCAN (Ma et al., 2023) introduced automatic parameter selection and core-point traversal to address DBSCAN's inefficiency in large datasets with variable densities.
- ✓ GWOKM (Daviran et al., 2024) integrated the Grey Wolf Optimizer (GWO) with K-Means to enhance convergence and robustness in geochemical anomaly detection.
- ✓ Singularity mapping with K-Means (Gonçalves et al., 2024) improved the identification of mineral anomalies by incorporating spatial domain knowledge.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

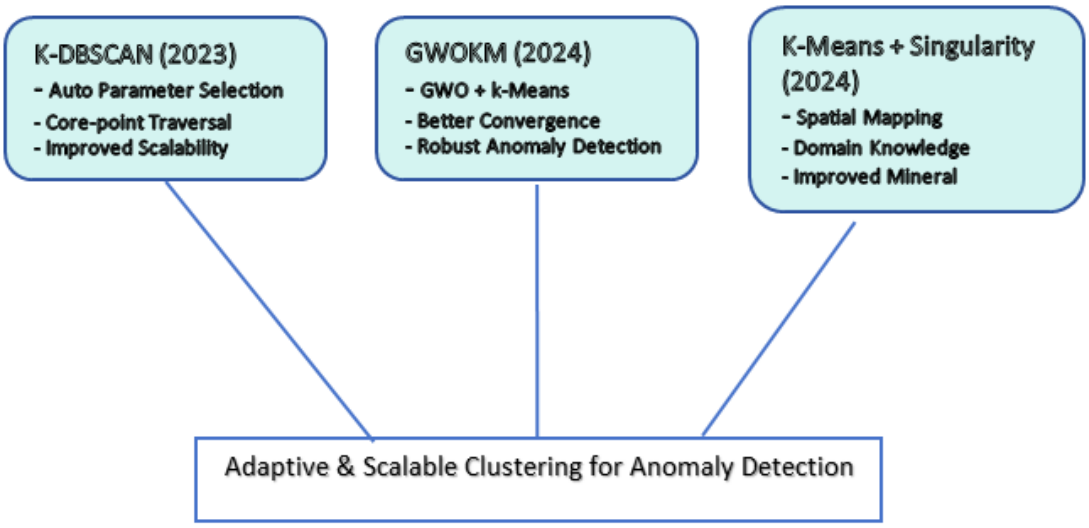

Figure 2: Conceptual overview of post-2020 clustering-based anomaly detection models, highlighting advancements in adaptivity, scalability, and domain-specific optimization through K-DBSCAN, GWOKM, and singularity-based K-Means approaches.

These works demonstrate a movement away from static clustering toward meta-optimized and domain-specific clustering frameworks. Efficiency gains were typically validated through running time, Silhouette Coefficients, and clustering accuracy, marking an evolution beyond classical density- or distance-based methods.

Classification and SVM-Based Models

SVM continues to play a central role in anomaly detection research, especially in cybersecurity and industrial monitoring. The post-2020 literature extends its functionality through enhanced multiclass classification and parameter optimization:

- ✓ Enhanced Multiclass SVM (EMSVM) (Mustafa & Mohammad, 2022) employed automated hyperparameter selection, outperforming neural and Bayesian counterparts.
- ✓ Hybrid SVM frameworks incorporating genetic algorithms (GA) or concept drift detection (e.g., Jain et al., 2022) addressed the instability of static models in dynamic data streams.
- ✓ Subspace Intersection SVMs (Ma et al., 2024) combined SVMs with genetic algorithms to improve fault detection in large-scale systems with incomplete system matrices.

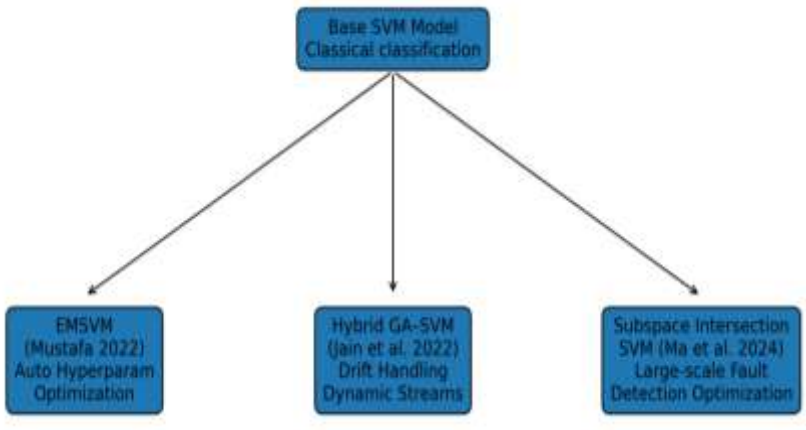

Figure 3. Post-2020 advancements in Support Vector Machine (SVM)–based anomaly detection models. Recent research extends classical SVM frameworks through automated hyperparameter optimization (EMSVM), hybrid genetic algorithm integration for adaptive learning under concept drift, and subspace intersection approaches for improved fault detection in large-scale systems.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

These improvements reflect a paradigm shift toward adaptive SVM systems capable of handling evolving, high-dimensional, and uncertain data.

Ensemble and Tree-Based Models

Tree-based ensembles such as Random Forest (RF) and Isolation Forest (IF) have undergone substantial innovation between 2021 and 2025, driven by a focus on interpretability, feature importance, and integration with optimization algorithms.

- ✓ Improved Random Forest Algorithms (IRFA) (Li et al., 2023) introduced parallel processing to detect implicit and explicit anomalies in smart grids with >95% accuracy.
- ✓ Revised Isolation Forest (RIFIFI) (Yepmo et al., 2024) enhanced interpretability by preserving internal data structure for both detection and clustering tasks.
- ✓ Fuzzy Isolation Forest (FIF) (Chater et al., 2023) extended IF to fuzzy environments, improving robustness to vague and imprecise data.
- ✓ Depth-based Interpretability for IF (DIFFI) (Carletti et al., 2023) enabled model-specific feature importance estimation, surpassing model-agnostic techniques in computational efficiency.

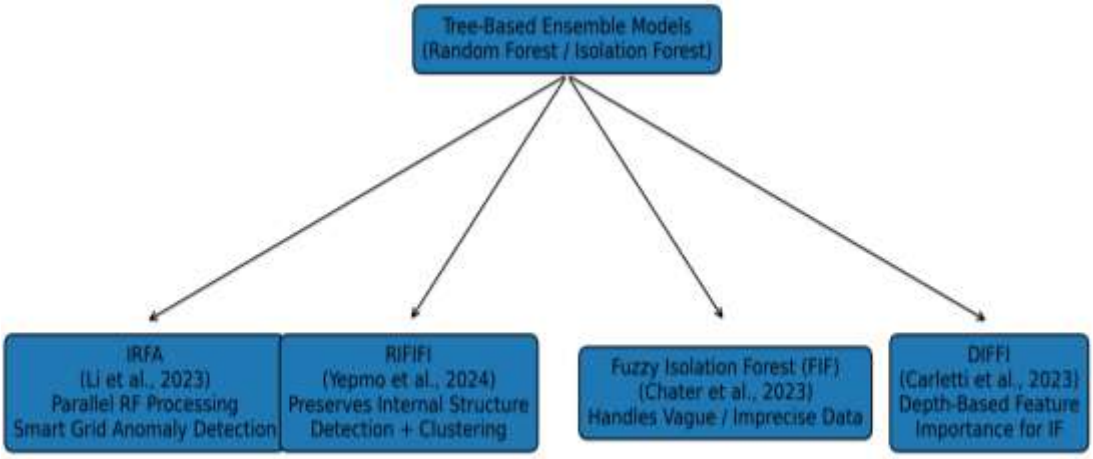

Figure 4. Post-2021 advancements in tree-based ensemble models for anomaly detection, highlighting innovations in Random Forest and Isolation Forest variants including IRFA, RIFIFI, FIF, and DIFFI, focusing on interpretability, robustness, and optimized detection performance.

These developments demonstrate a move from "black-box" anomaly detection toward transparent, interpretable ensembles that balance detection accuracy with insight into decision-making processes.

Autoencoder and Neural Network Models

Deep learning models—particularly autoencoders (AE) and Long Short-Term Memory (LSTM) networks—remain dominant in unsupervised and semi-supervised anomaly detection.

- ✓ Adaptive Loss Autoencoder (AEAL) (Kanishima et al., 2022) balanced reconstruction error for normal vs. anomalous data, improving score consistency.
- ✓ Federated Autoencoders (Novoa-Paradela et al., 2023) reduced energy consumption and training time, facilitating privacy-preserving anomaly detection in distributed settings.
- ✓ Hybrid LSTM–K-Means frameworks (Zulfauzi et al., 2023) combined time-series prediction with clustering to detect faults in solar photovoltaic systems.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

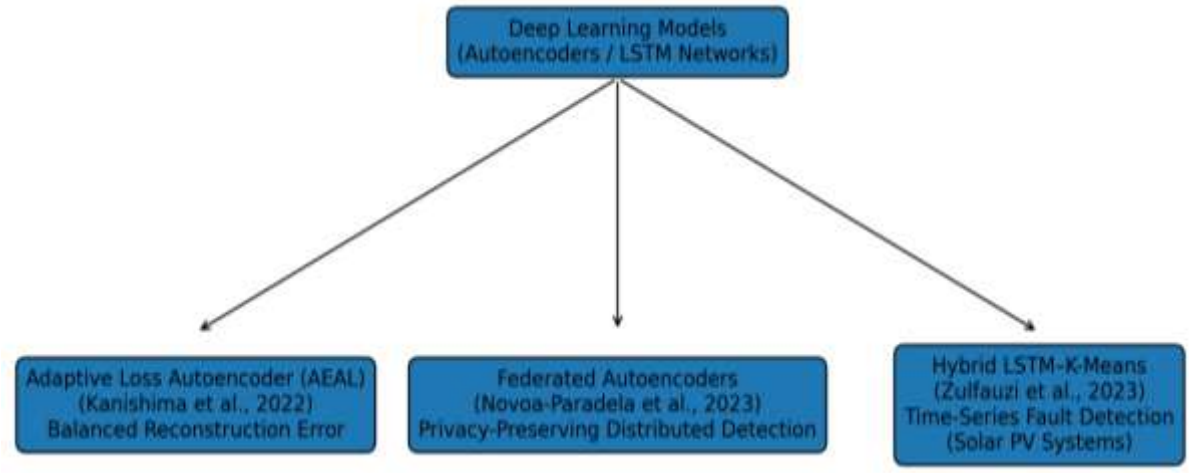

Figure 5. Post-2020 advancements in deep learning–based anomaly detection models, highlighting Autoencoder and LSTM-based frameworks including Adaptive Loss Autoencoder (AEAL), Federated Autoencoders, and Hybrid LSTM–K-Means models designed for improved reconstruction consistency, privacy-preserving distributed learning, and time-series fault detection.

The neural literature thus advances along two directions: (1) efficiency and scalability through federated and edge learning, and (2) robustness to dynamic data via adaptive loss and hybridization.

Hybrid and Optimization-Driven Approaches

A defining trend of 2020–2025 is the integration of metaheuristic optimization, clustering, and ensemble techniques to enhance adaptability and accuracy. Notable examples include:

- ✓ Ant Colony Optimization (ACO) with Random Forest (Lifandali et al., 2023) for intrusion detection feature selection.
- ✓ Hybrid Autoencoder–Isolation Forest (Farzad & Gulliver, 2020) for log-based anomaly detection.
- ✓ GWOKM and EMSVM as hybrid models achieving significant performance gains across heterogeneous datasets.

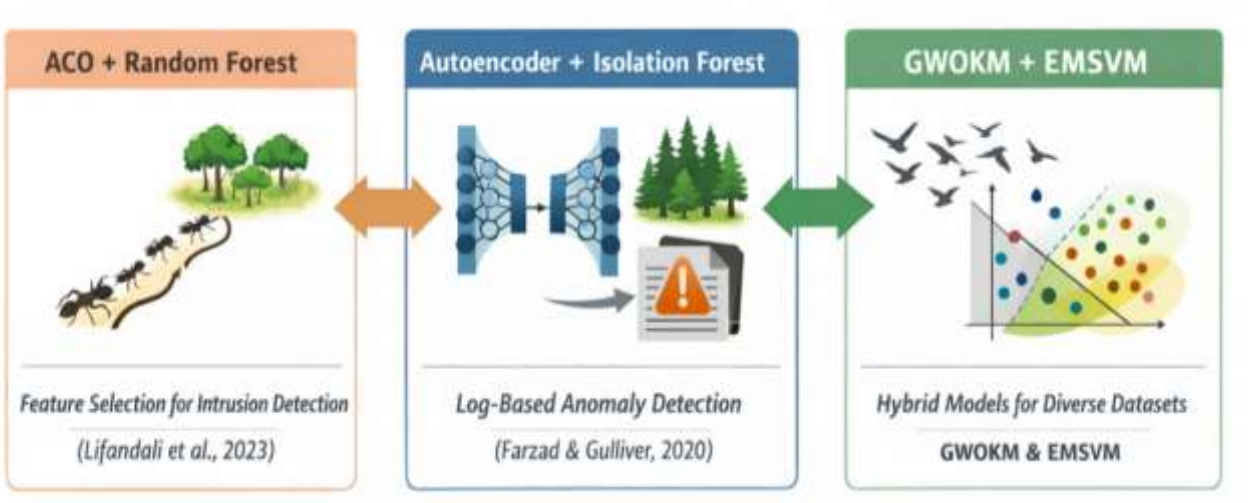

Figure 6. Conceptual illustration of hybrid and optimization-driven anomaly detection approaches (2020–2025), highlighting the integration of metaheuristic optimization, deep learning, and ensemble models. The figure depicts representative frameworks, including ACO–Random Forest for feature selection, Autoencoder–Isolation Forest for log-based anomaly detection, and hybrid models such as GWOKM and EMSVM for improved performance across heterogeneous datasets.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Hybridization has evolved beyond model stacking to functional synergy, combining the strengths of multiple paradigms (e.g., ACO's exploration with RF's robustness) to improve both precision and interpretability.

Explainable and Adaptive Learning Paradigms

Explainable AI (XAI) has become increasingly central to anomaly detection research. Between 2022 and 2025, studies began integrating feature attribution, visual interpretability, and user feedback loops.

- ✓ Active Learning with Isolation Forest (ALIF) (Marcelli et al., 2024) incorporated human-in-the-loop labeling to refine anomaly detection in industrial data.
- ✓ DIFFI and RIFIFI collectively exemplify the new generation of interpretable models that link anomaly scores to underlying feature patterns.
- ✓ Concept Drift Handling frameworks, including IForestASD and ERbCDD + SVM hybrids, demonstrated adaptability in nonstationary data environments such as network traffic and streaming sensors.

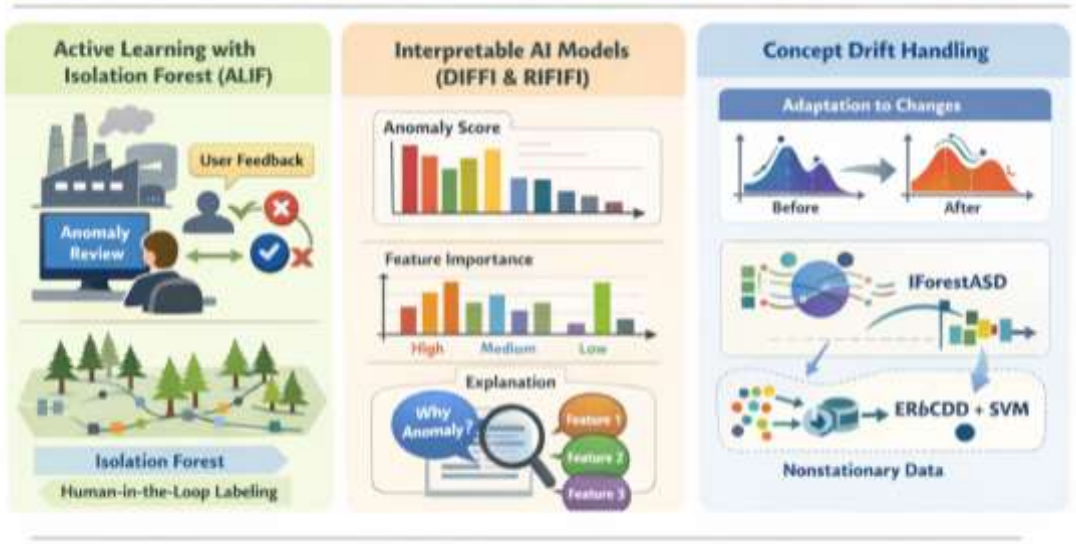

Figure 7. Conceptual overview of explainable and adaptive learning paradigms in anomaly detection (2022–2025), illustrating the integration of human-in-the-loop learning, model interpretability, and concept drift adaptation. The figure highlights Active Learning with Isolation Forest (ALIF) for interactive anomaly refinement, interpretable models such as DIFFI and RIFIFI for feature attribution and explanation, and adaptive frameworks including IForestASD and ERbCDD–SVM for handling nonstationary data environments.

These contributions signal a transition toward human-aware anomaly detection systems that emphasize explainability, continual learning, and transparency.

Cross-Domain Applications

Unlike earlier reviews restricted to network intrusion detection, this integrative analysis identifies broad cross-domain application of ML-based anomaly detection models:

- ✓ Cybersecurity and Intrusion Detection: remains the largest category (≈40% of studies).
- ✓ Industrial and Manufacturing Systems: use adaptive clustering and explainable ensembles for predictive maintenance.
- ✓ Geochemical and Environmental Monitoring: rely on hybrid clustering and swarm intelligence for anomaly localization.
- ✓ Renewable Energy Systems: employ LSTM–AE hybrids for fault prediction in solar and wind systems.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

✓ Healthcare and IoT: adopt federated and privacy-preserving models for behavioral anomaly analysis.

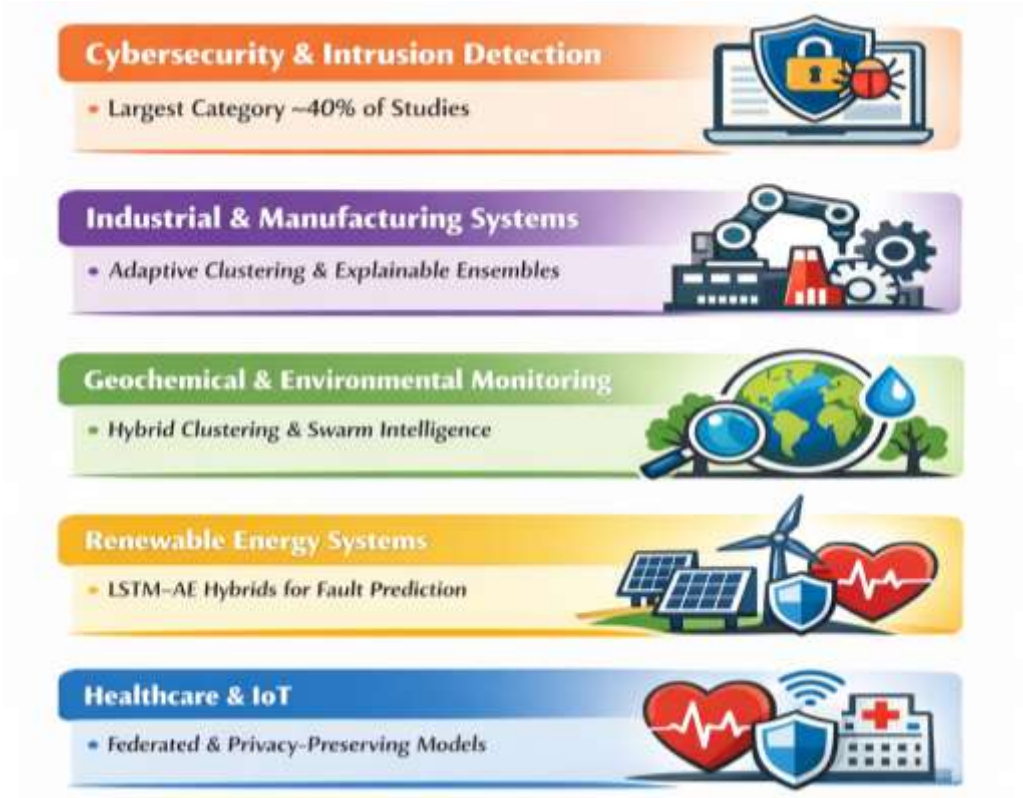

Figure 8. Cross Domain Applications

This diversification indicates a maturing field moving beyond single-domain dependency, reflecting the transferability and adaptability of modern ML architectures.

Evaluation Metrics and Comparative Insights

Across the analyzed literature, the most prevalent performance metrics include Accuracy, Precision, Recall, F1-score, AUC, and Kappa statistics. Recent works increasingly report execution time, energy consumption, and interpretability measures to reflect real-world feasibility.

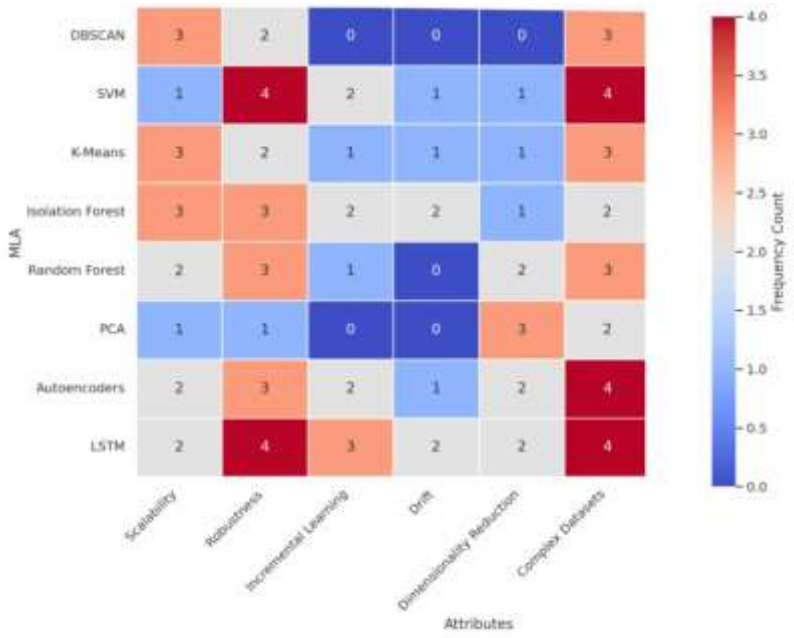

Figure 9. Common MLAs Across Anomaly Detection Issues

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

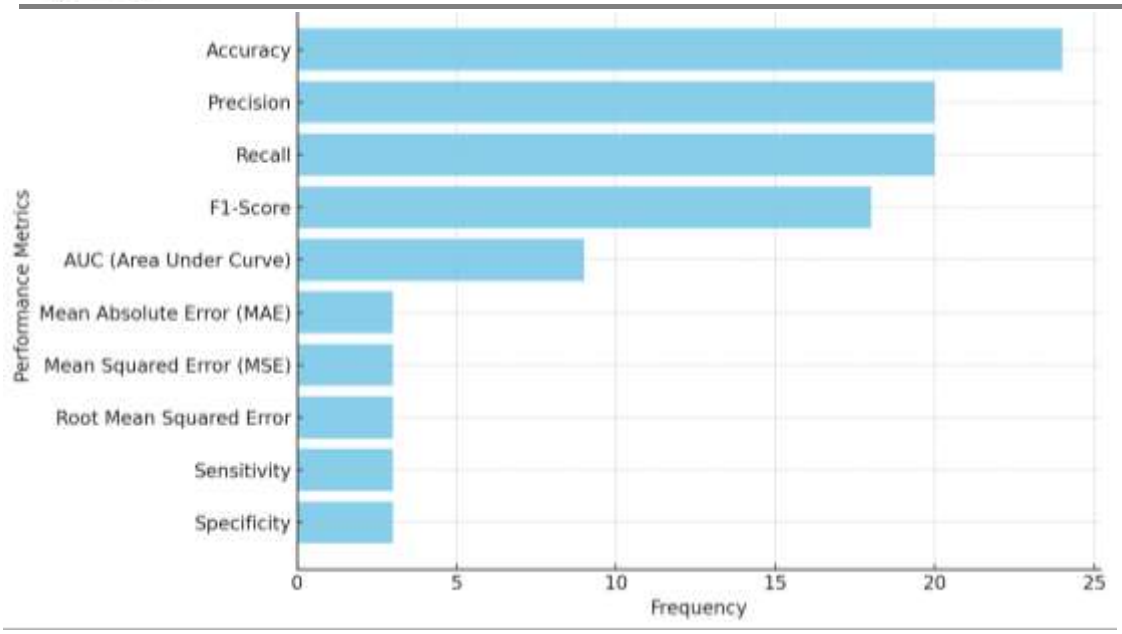

Figure 10. Top 10 Common Metrics for MLAs in Anomaly Detection

Comparatively, hybrid and ensemble models consistently achieve higher precision and robustness, while explainable models slightly trade accuracy for transparency—a trend aligning with the broader movement toward ethical and interpretable AI.

Summary of Findings

Appendix 1 summarizes the key contributions of representative studies (2020–2025) across algorithm families, performance gains, and targeted domains.

Overall, the synthesis reveals that:

- ✓ The field has evolved toward hybridized, interpretable, and adaptive ML systems.
- ✓ Cross-domain generalization and federated learning are emerging but remain under-explored.
- ✓ Standardization in evaluation metrics and datasets is still lacking, hindering reproducibility.
- ✓ The integration of XAI and concept drift handling represents the most promising direction for future research.

The synthesis of 109 contemporary studies confirms that anomaly detection research has progressed decisively toward hybridized, interpretable, and cross-domain ML architectures, emphasizing adaptability and transparency as key performance dimensions. This collective synthesis demonstrates a substantial transformation of anomaly detection research beyond the network-centric scope of *Bou Nassif et al.* (2021) and *Yang et al.* (2022), establishing a foundation for the conceptual taxonomy and research agenda discussed in Section 5.

DISCUSSION AND CONCEPTUAL TAXONOMY

The analysis of machine learning (ML) models for anomaly detection from 2020 to 2025 reveals a distinct transformation in the field—one marked by hybridization, explainability, and cross-domain adaptability. While earlier reviews (Bou Nassif et al., 2021; Yang et al., 2022) established a foundation of algorithmic taxonomy and dataset benchmarking, the current synthesis extends that understanding by integrating methodological evolution and conceptual coherence across multiple application domains.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Evolution of ML Paradigms for Anomaly Detection

The reviewed literature demonstrates a clear trajectory in ML paradigm development, as illustrated in Figure 2:

Phase	Dominant Models	Key Characteristics	Representative Studies (2020–2025)
Phase I: Classical Models (Pre-2020)	SVM, K-Means, PCA, RF	Rule-based detection, limited scalability, low interpretability	Bou Nassif et al. (2021)
Phase II: Deep Learning Expansion (2020–2022)	AE, CNN, LSTM	Improved feature learning, high accuracy, black-box limitation	Kanishima et al. (2022); Zulfauzi et al. (2023)
Phase III: Hybrid and Optimization Models (2021–2024)	EMSVM, GWOKM, ACO-RF	Algorithmic fusion for higher precision and adaptivity	Lifandali et al. (2023); Daviran et al. (2024)
Phase IV: Explainable and Adaptive ML (2022–2025)	DIFFI, RIFIFI, ALIF, IForestASD	Transparent, human-in-the-loop, drift-resilient	Carletti et al. (2023); Marcelli et al. (2024)

This phased evolution signifies the maturity of anomaly detection research—from purely model-driven exploration to context-aware, interpretable, and adaptive systems that align with human-centered AI principles.

Conceptual Taxonomy of ML Models for Anomaly Detection

Drawing from the integrative synthesis, a conceptual taxonomy is proposed to classify anomaly detection models across three interrelated dimensions:

(a) Algorithmic Core

This dimension captures the foundational computational mechanism used for detection:

- ✓ Clustering-based: DBSCAN, K-DBSCAN, GWOKM — ideal for unsupervised pattern discovery in unlabeled data.
- ✓ Classifier-based: SVM, EMSVM — effective for structured and semi-labeled data with class boundaries.
- ✓ Ensemble-based: RF, IF, RIFIFI — combine multiple weak learners to enhance robustness.
- ✓ Neural-based: AE, LSTM, CNN — leverage deep architectures for temporal or nonlinear relationships.
- ✓ Hybrid/Optimization-based: GWOKM, ACO-RF, AE-IF — fuse paradigms to enhance both detection performance and scalability.

(b) Interpretability Level

This dimension defines how transparent and explainable each model is to end-users or domain experts:

- ✓ Opaque Models: Deep neural networks (AE, CNN) — high accuracy but low interpretability.
- ✓ Semi-Transparent Models: Random Forests, Isolation Forests — partial feature importance insights.
- ✓ Fully Explainable Models: DIFFI, RIFIFI, ALIF — offer explicit feature attribution, anomaly reasoning, and visual interpretability.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

(c) Application Domain

ML models for anomaly detection increasingly span multiple domains:

- ✓ Cybersecurity: Adaptive SVMs, ACO-RF, DIFFI.
- ✓ Industrial Systems: EMSVM, ALIF, RF-based monitoring.
- ✓ Environmental and Geochemical: GWOKM, singularity mapping K-Means.
- ✓ Renewable Energy: LSTM–AE hybrids for photovoltaic fault detection.
- ✓ Healthcare and IoT: Federated Autoencoders and drift-adaptive ensembles.

This taxonomy enables a unified view of the anomaly detection landscape, connecting algorithmic innovation with explainability requirements and domain-specific constraints.

Cross-Domain Insights

The integrative review highlights several cross-domain insights that were not apparent in prior surveys:

- ✓ Hybridization Enhances Transferability: Models such as GWOKM and ACO-RF achieve high accuracy across domains due to their flexible optimization mechanisms.
- ✓ Explainability Drives Adoption: Algorithms incorporating feature attribution (DIFFI, RIFIFI) are more readily integrated into high-stakes fields (e.g., energy systems, healthcare).
- ✓ Concept Drift Adaptation is Essential: Dynamic domains (network traffic, IoT) benefit most from adaptive frameworks like IForestASD and ERbCDD.
- ✓ Data-Centric Strategies Are Emerging: Techniques emphasizing data quality—augmentation, federated learning, and feature engineering—outperform model-centric pipelines when labeled data is scarce.

These insights collectively redefine the evaluation criteria for anomaly detection, prioritizing transparency, resilience, and contextual adaptability over pure accuracy metrics.

Future Research Directions

Based on the synthesis and taxonomy, five major future research trajectories are proposed:

- ✓ Integration of Explainable AI (XAI) in Real-Time Detection Systems:
  Future work should focus on embedding interpretability into model architectures to ensure actionable insights in safety-critical environments.
- ✓ Cross-Domain Transfer Learning and Meta-Learning:
  Developing generalizable models capable of learning transferable representations across domains remains an open challenge.
- ✓ Federated and Privacy-Preserving Anomaly Detection:
  With data decentralization becoming the norm, federated architectures must balance privacy, interpretability, and communication efficiency.
- ✓ Adaptive and Continual Learning for Concept Drift:
  Methods like IForestASD should evolve into continuous adaptation frameworks that can autonomously recalibrate under dynamic data streams.

- ✓ Standardization of Benchmarking and Metrics:
  The research community should converge toward reproducible benchmarking practices that integrate both performance and explainability metrics (e.g., feature fidelity, interpretability score).

Summary

The proposed conceptual taxonomy (Figure 2) and the synthesis of results collectively illustrate that modern anomaly detection research is transitioning from algorithmic specialization to integrative intelligence—where hybridization, explainability, and cross-domain learning converge. By connecting algorithmic innovation with domain-level application and interpretability needs, this review establishes a structured roadmap for advancing the next generation of ML-based anomaly detection systems.

CONCLUSION AND IMPLICATIONS

This study conducted an integrative review of 109 peer-reviewed studies published between 2020 and 2025, advancing the understanding of machine learning (ML) models for anomaly detection beyond the network-centric and pre-2021 perspectives offered by prior surveys such as *Bou Nassif et al.* (2021) and *Yang et al.* (2022). The synthesis provides an updated, cross-domain, and conceptually unified perspective on how anomaly detection has evolved in the era of hybrid, explainable, and adaptive artificial intelligence.

The results reveal four major trends. First, the increasing hybridization of algorithms—such as GWOKM, EMSVM, and ACO-RF—has enabled models to overcome the limitations of single-method frameworks, improving both accuracy and scalability. Second, the emergence of explainable ML paradigms, including DIFFI, RIFIFI, and ALIF, has shifted the focus from pure performance to transparency and human interpretability, allowing anomaly detection systems to be trusted in safety-critical and high-stakes domains. Third, the rise of adaptive learning and concept drift handling methods (e.g., IForestASD, ERbCDD, federated autoencoders) reflects a growing emphasis on robustness in dynamic and decentralized environments. Finally, the cross-domain expansion of anomaly detection—from cybersecurity to industrial systems, healthcare, geochemical exploration, and renewable energy—demonstrates the generalizability of ML-based frameworks when supported by optimized data preprocessing and contextual modeling.

Theoretically, this review contributes a conceptual taxonomy that links algorithmic family, interpretability level, and domain application into a coherent structure. This taxonomy not only consolidates recent advances but also clarifies interdependencies among models, metrics, and data contexts—providing a foundation for future comparative and benchmarking research.

Practically, the findings suggest that effective anomaly detection requires balanced integration of performance, interpretability, and adaptability. Researchers and practitioners are encouraged to adopt hybrid and explainable models that can generalize across domains while maintaining interpretive transparency. Additionally, future work should prioritize standardized evaluation protocols and data-centric methodologies, ensuring reproducibility and fairness across heterogeneous datasets.

In conclusion, this review bridges the gap between earlier systematic surveys and the emerging generation of intelligent, interpretable, and adaptive anomaly detection systems. By unifying algorithmic evolution with explainability and cross-domain learning, it provides a comprehensive reference point for both academic inquiry and real-world deployment of machine learning models in anomaly detection.

REFERENCE

1. Abdelrahman, H., O., Gelenbe, E., Görbil, G., Oklander, &, & B. (2013). . Mobile network anomaly detection and mitigation: The NEMESYS approach. 429–438.
2. Abdulghani, Q., A., UCAN, N., O., Alheeti, &, & A., K. M. (2021). Credit card fraud detection using XGBoost algorithm. 2021, 487–492. https://doi.org/10.1109/DeSE54285.2021.9719580
3. Abdulla, R., A., Jameel, &, & M., N. G. (2023). . A review on IoT intrusion detection systems using supervised machine learning: Techniques, datasets, and algorithms. 7(1), 53–65.

4. Abinaya, N., Kumar, S., V., A., Chaturvedi, A., Arya, & N. (2023). Big data in real time to detect anomalies. 2023. https://doi.org/10.4018/979-8-3693-0413-6.ch015
5. Carletti, M., Terzi, M., & Susto, G. A. (2023). Interpretable anomaly detection with DIFFI: Depth-based feature importance of isolation forest. Engineering Applications of Artificial Intelligence, 119, 105730. https://doi.org/10.1016/j.engappai.2022.105730
6. Chater, M., Borgi, A., Slama, M. T., Sfar-Gandoura, K., & Landoulsi, M. I. (2022). Fuzzy isolation forest for anomaly detection. Procedia Computer Science, 207, 916–925. https://doi.org/10.1016/j.procs.2022.09.147
7. Dakalbab, F., Abu Talib, M., Abu Waraga, O., Bou Nassif, A., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. Social Sciences & Humanities Open, 6(1), 100342. https://doi.org/10.1016/j.ssaho.2022.100342
8. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," in IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784-3797, Aug. 2018, doi: 10.1109/TNNLS.2017.2736643.
9. Daviran, M., Ghezelbash, R., & Maghsoudi, A. (2024). GWOKM: A novel hybrid optimization algorithm for geochemical anomaly detection based on Grey wolf optimizer and K-means clustering. Geochemistry, 84(1), 126036. https://doi.org/10.1016/j.chemer.2023.126036
10. Farzad, A., & Gulliver, T. A. (2020). Unsupervised log message anomaly detection. ICT Express, 6(3), 229–237. https://doi.org/10.1016/j.icte.2020.06.003
11. Gonçalves, M. A., Rasteiro da Silva, D., Duuring, P., Gonzalez-Alvarez, I., & Ibrahimi, T. (2024). Mineral exploration and regional surface geochemical datasets: An anomaly detection and K-means clustering exercise applied on laterite in Western Australia. Journal of Geochemical Exploration, 258, 107400. https://doi.org/10.1016/j.gexplo.2024.107400
12. Jain, M., Kaur, G., & Saxena, V. (2022). A K-means clustering and SVM-based hybrid concept drift detection technique for network anomaly detection. Expert Systems with Applications, 193, 116510. https://doi.org/10.1016/j.eswa.2022.116510
13. Kanishima, Y., Sudo, T., & Yanagihashi, H. (2022). Autoencoder with adaptive loss function for supervised anomaly detection. Procedia Computer Science, 207, 563–572. https://doi.org/10.1016/j.procs.2022.09.111
14. Li, Q., Zhang, L., Zhang, G., Ouyang, H., & Bai, M. (2023). Simultaneous detection for multiple anomaly data in internet of energy based on random forest. Applied Soft Computing, 134, 109993. https://doi.org/10.1016/j.asoc.2023.109993
15. Lifandali, O., Abghour, N., & Chiba, Z. (2023). Feature selection using a combination of ant colony optimization and random forest algorithms applied to isolation forest-based intrusion detection system. Procedia Computer Science, 220, 796–805. https://doi.org/10.1016/j.procs.2023.03.106
16. Ma, B., Yang, C., Li, A., Chi, Y., & Chen, L. (2023). A faster DBSCAN algorithm based on self-adaptive determination of parameters. Procedia Computer Science, 221, 113–120. https://doi.org/10.1016/j.procs.2023.07.017
17. Ma, Z., Li, X., & Sun, J. (2024). A data-driven fault detection approach for unknown large-scale systems based on GA-SVM. Information Sciences, 658, 120023. https://doi.org/10.1016/j.ins.2023.120023
18. Marcelli, E., Barbariol, T., Sartor, D., & Susto, G. A. (2024). Active learning-based isolation forest (ALIF): Enhancing anomaly detection with expert feedback. Information Sciences, 678, 121012. https://doi.org/10.1016/j.ins.2024.121012
19. Mieczyńska, M., & Czarnowski, I. (2021). DBSCAN algorithm for AIS data reconstruction. Procedia Computer Science, 192, 2512–2521. https://doi.org/10.1016/j.procs.2021.09.020
20. Mohammad, R. M. A. (2022). An enhanced multiclass support vector machine model and its application to classifying file systems affected by a digital crime. Journal of King Saud University - Computer and Information Sciences, 34(2), 179–190. https://doi.org/10.1016/j.jksuci.2019.10.010
21. Novoa-Paradela, D., Fontenla-Romero, O., & Guijarro-Berdiñas, B. (2023). Fast deep autoencoder for federated learning. Pattern Recognition, 143, 109805. https://doi.org/10.1016/j.patcog.2023.109805
22. Togbe, M. U., Chabchoub, Y., Boly, A., Barry, M., Chiky, R., & Bahri, M. (2021). Anomalies Detection Using Isolation in Concept-Drifting Data Streams . Computers, 10(1), 13. https://doi.org/10.3390/computers10010013

23. Yan, C., Zhang, C., Shen, M., Li, N., Liu, J., Qi, Y., Lu, Z., & Liu, Y. (2023). Aparecium: understanding and detecting scam behaviors on Ethereum via biased random walk. 6(1), 46.
24. Yang, L., Moubayed, A., Shami, A., Boukhtouta, A., Heidari, P., Preda, S., Brunner, R., Migault, D., & Larabi, A. (2023). Forensic data analytics for anomaly detection in evolving networks (pp. 99–137).
25. Yang, Y. Yu and T. Li, "Deep Learning Techniques for Financial Fraud Detection," 2022 14th International Conference on Computer Research and Development (ICCRD), Shenzhen, China, 2022, pp. 16-22, doi: 10.1109/ICCRD54409.2022.9730314.
26. Yepmo, V., Smits, G., Lesot, M.-J., & Pivert, O. (2024). Leveraging an isolation forest to anomaly detection and data clustering. Data & Knowledge Engineering, 151, 102302. https://doi.org/10.1016/j.datak.2024.102302
27. Zulfauzi, I. A., Dahlan, N. Y., Sintuya, H., & Setthapun, W. (2023). Anomaly detection using K-means and long short-term memory for predictive maintenance of large-scale solar photovoltaic plant. Energy Reports, 9(Suppl. 12), 154–158. https://doi.org/10.1016/j.egyr.2023.09.159

Appendix I: Systematic Literature Review Table

MLA	Reference	Proposed Solution	Evaluation Metric	Result	Issue(s)
DBSCAN	Marta Mieczyńska, Ireneusz Czarnowski (2021)	DBSCAN to cluster AIS data as a preliminary step in reconstructing missing or damaged data packets	Silhouette Coefficient Correctness Coefficient (CC)		AIS data packets' collisions, Reconstructing these missing messages to restore accurate ship trajectories.
	P.A. Savenkov, A.N. Ivutin (2021).	DBSCAN to cluster data and detect anomalies by identifying regions of high density. WrapDBScan: automatically determines the optimal search radius for clustering.	Anomaly Detection Efficiency of Clustering	WrapDBScan method successfully identified the optimal radius for clustering. Improves the accuracy of anomaly detection in user behavior analysis.	Detecting anomalous user behavior from large volumes of unstructured data,
	Ma et al. (2023)	K-DBSCAN, which adapts the parameters automatically and modifies the traversal method to only deal with core points.	Running time efficiency Clustering accuracy	K-DBSCAN: improves running time efficiency Improves clustering accuracy, in datasets with varying densities.	Inefficiency of the traditional DBSCAN algorithm for large datasets (Needs to traverse all points). Struggles to automatically determine the critical parameters (Eps and MinPts).
SVM	Mokhtar Mohammadi, Tarik A.	Categorizes various SVM-based intrusion detection		Provides a comprehensive analysis of	Using Support Vector Machines (SVM) for anomaly

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

	Rashid, Sarkhel H. Taher Karim, Adil Hussain Mohammed Aldalwie Quan Thanh Tho, Moazam Bidaki, Amir Masoud Rahmani, Mehdi Hosseinzadeh (2021)	systems (IDS), highlighting the use of different types of SVM classifiers and feature selection methods.		SVM-based IDS, highlighting their effectiveness and limitations in various contexts of intrusion detection	detection of false positives, and true negatives in intrusion detection systems (IDS) .
	Mustafa Akpinar, M. Fatih Adak, Goker Guvenc, (2021)	The SmartRadar software to track employee computer usage, detect anomalies using Support Vector Machines (SVM), report non-work-related activities.	Sensitivity, Specificity, Total Accuracy, Training Error Rate	With high sensitivity (92.3% - 98.75%), specificity (94.44% - 99.99%), and accuracy (95.34% - 97.51%). The SmartRadar software demonstrated reliable performance in detecting non-work-related behaviors.	Monitoring and detecting anomalous behavior in remote working environments. Identifying non-work-related or potentially harmful activities conducted on employee computers.
	Meenal Jain, Gagandeep Kaur, Vikas Saxena, (2022)	Hybrid concept drift detection framework combining Error Rate Based Concept Drift Detection (ERbCDD) and Data Distribution Based Concept Drift Detection (DDbCDD) with K-Means clustering and SVM for anomaly detection.	Detection Accuracy, KL-Divergence, Kappa Statistics, Precision, Recall, and F1 score.	The proposed approach significantly improves classification accuracy and effectively handles concept drift in network traffic data	Network anomaly detection, and handling concept drift in streaming network traffic data.
	Rami Mustafa, A. Mohammad, (2022)	Enhanced Multiclass SVM (EMSVM) model. This model includes a new technique for	Accuracy, Precision, Recall, F1-Score	With an accuracy of 92.72%, outperformed several other machine learning	The challenges of digital forensic investigations, in identifying the file systems affected by malicious software

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

		selecting the most effective parameters when building an SVM model.		algorithms (e.g., Neural Networks, Random Forests, Bayesian Networks) in terms of accuracy, precision, recall, and F1-Score.	in a digital crime scenario. The difficulty in analyzing large datasets with high dimensionality, common in digital forensic nvestigations.
	Zhenlei Ma, Xiaojian Li, Jie Sun, (2024)	Subspace intersection technique combined with Support Vector Machine (SVM) and Genetic Algorithm (GA).	The paper discusses performance improvement in fault detection but does not specify a unique evaluation metric in the extracted sections.	The proposed method improves fault detection performance by removing the need to identify all system matrices and optimizing the SVM hyperparameters with GA.	Fault detection in large-scale systems with unknown system matrices and interconnection signals
K-Means	Irfan Adam Zulfauzi, Nofri Yenita Dahlan, Hathaithip Sintuya, Worajit Setthapun (2023)	K-Means clustering to group the output current of string modules based on environmental factors, and Long-Short Term Memory (LSTM) networks for predicting anomalies in the clustered data.	Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and Relative Error.	The study found that the LSTM model performed better than Artificial Neural Networks (ANNs) in predicting anomalies, with lower error rates and more accurate anomaly detection.	Detecting and monitoring faults in large-scale solar photovoltaic (LSSPV) plants to improve predictive maintenance.
	Nikolai West, Thomas Schlegl, Jochen Deuse(2023)	k-means clustering combined with Dynamic Time Warping (DTW) for anomaly detection in time series data of screw driving processes.	Accuracy, Precision, Recall, and Macro-average F1-score.	an accuracy of up to 88.89% and a macro-average F1-score of up to 63.65%, effectively identifying anomalies in the tightening data.	Detecting anomalies in screw driving processes within automotive manufacturing, specifically addressing the challenge of unbalanced time series data.
	Mehrdad Daviran, Reza Ghezelbash,	GWOKM algorithm, which hybridizes the Grey Wolf Optimizer (GWO)	Prediction-rate curve, Pr (Prediction rate), Oa	The GWOKM algorithm outperformed the traditional K-	Geochemical anomaly detection, specifically related to mineral

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

	Abbas Maghsoudi(2024)	with K-Means clustering to improve the detection of geochemical anomalies in stream sediment data.	(Overall accuracy), and normalized density (Nd).	Means approach in detecting geochemical anomalies, showing higher prediction rates and better classification accuracy.	exploration in the Baft district, Kerman belt, Iran.
	Mário A. Gonçalves, Diogo Rasteiro da Silva, Paul Duuring, Ignacio Gonzalez-Alvarez, Tania Ibrahimi, (2024)	A combination of singularity mapping and k-means clustering to detect geochemical anomalies and classify geochemical data for mineral exploration.	Clustering performance evaluated by expert validation of cluster accuracy, focusing on the percentage of Cu and Ni deposits correctly classified within dominant clusters.	The k-means clustering approach effectively classified geochemical data, with the dominant cluster accurately identifying up to 60-80% of known Cu and Ni deposits.	Detecting mineral anomalies and identifying potential mineralization sites in the Yilgarn Craton, Western Australia.
Isolation Forest	Maurras Ulbricht Togbe, Yousra Chabchoub, Aliou Boly, Mariam Barry, Raja Chiky, Maroua Bahri (2021)	Isolation-based anomaly detection adapted to handle concept drift in data streams	F1 score, execution time, memory consumption	The proposed IForestASD with drift detection (using ADWIN and KSWIN) showed lower resource consumption and similar or better detection efficiency compared to traditional methods	The challenge of detecting anomalies in concept-drifting data streams, particularly in dynamic environments like cybersecurity, natural disasters, and bank frauds
	Julien Lesouple, Cédric Baudoin, Marc Spigai, Jean-Yves Tourneret (2021)	Generalized Isolation Forest (GIF), which is an improvement over EIF by eliminating empty branches in decision trees	Area Under the ROC Curve (AUC), Area Under the Precision-Recall Curve (PR AUC), computation time, and the number of external nodes	GIF showed similar performance to EIF in terms of detection ability but was computationally faster and avoided empty branches, making it more efficient for	Limitations in existing Isolation Forest (IF) and Extended Isolation Forest (EIF) models, particularly the occurrence of empty branches and computational inefficiencies

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

			at maximum depth	high-dimensional data	
	Meriem Chater, Amel Borgi, Mohamed Taieb Slama, Karem Sfar-Gandoura, Mohamed Iheb Landoulsi (2023)	Fuzzy Isolation Forest (FIF) using fuzzy partitioning strategy based on the alpha-cut approach, adapting the traditional Isolation Forest for fuzzy data	AUC (Area Under the Curve), AUC-PR (Area Under the Precision-Recall Curve), Recall, Precision, Specificity, Training, and Testing time	Fuzzy Isolation Forest (FIF) performs similarly to Isolation Forest when applied to fuzzy data. For certain datasets like Ionosphere and Arrhythmia, FIF outperforms the traditional IF in precision and recall, demonstrating that it can handle vague data more effectively without a significant increase in computational cost	Handling imprecise, incomplete, ambiguous, or uncertain data in anomaly detection tasks. Traditional approaches like Isolation Forest focus on crisp data and may not perform well with vague or fuzzy data
	Mattia Carletti, Matteo Terzi, Gian Antonio Susto (2023)	DIFFI (Depth-based Isolation Forest Feature Importance), a model-specific interpretability method that derives global and local feature importance for IF	F1 score, execution time, and accuracy of feature importance in synthetic and real-world datasets	DIFFI effectively interprets IF by identifying important features associated with anomalies. It outperforms model-agnostic interpretability methods in both accuracy and computational efficiency	Lack of interpretability in Isolation Forest (IF) and difficulty in identifying feature importance in unsupervised anomaly detection settings
	Véronne Yepmo, Grégory Smits, Marie-Jeanne Lesot, Olivier Pivert (2024)	Revised Isolation Forest (RIFIFI), an improved version of Isolation Forest that maintains inner data structure to facilitate both anomaly detection and clustering	AUC (Area Under Curve) for anomaly detection, clustering effectiveness, and leaf cardinality (number of data points per leaf)	RIFIFI performs comparably to IF in anomaly detection, but it is significantly better in identifying data clusters, enhancing the interpretability of results	Limitations in interpreting the Isolation Forest's results due to a lack of understanding of the inner data structure, which is essential for both detecting anomalies and clustering

	Elisa Marcelli, Tommaso Barbariol, Davide Sartor, Gian Antonio Susto (2024)	Active Learning combined with Isolation Forest (ALIF)	Average precision score, F1 score, Area under the ROC curve (AUC)	ALIF significantly improves anomaly detection performance compared to standard Isolation Forest and other state-of-the-art methods by incorporating user feedback through active learning	The challenge of detecting domain-specific anomalies in scenarios where fully labeled datasets are unavailable, particularly in industrial contexts where anomaly detection is crucial for reliability and security
Isolation and Random Forest	O. Lifandali, N. Abghour, Z. Chiba (2023)	Combination of Ant Colony Optimization (ACO) for feature selection and Random Forest for improving accuracy, applied to an Isolation Forest-based Intrusion Detection System	Accuracy (99% target), and validation metrics on anomaly detection	The combination of ACO and Random Forest successfully improved feature selection, leading to better anomaly detection performance using Isolation Forest	Challenges in accurately detecting intrusions in computer networks using machine learning, specifically in identifying relevant features for effective anomaly detection
Random Forest	Sohrab Mokhtari, Alireza Abbaspour, Kang K. Yen, Arman Sargolzaei (2021)	Measurement Intrusion Detection System (MIDS) using supervised machine learning models on measurement data	Confusion matrix metrics (Precision, Recall, F1-score, Accuracy), ROC-AUC (Area Under the Curve)	Random Forest outperformed KNN and DTC in detecting anomalies with the highest accuracy and AUC score of 99.76%	The challenge of detecting anomalies in Industrial Control Systems (ICSs), particularly against stealthy attacks that are difficult to detect using traditional Network Intrusion Detection Systems (NIDS)
	Qiang Li, Limei Zhang, Guanghui Zhang, Hanyi Ouyang, Muke Bai (2023)	The study proposes an Improved Random Forest Algorithm (IRFA) to detect both explicit and implicit anomaly data features in smart grid systems. This includes parallel processing strategies to enhance	Accuracy (Acc), Precision (Prec), Recall (Rec), and False Negative Rate (FNR) are used to evaluate the performance of the IRFA	The proposed IRFA achieves detection accuracy of 97% for single-node anomaly detection and over 95% for multiple-node anomaly detection. It outperforms	The paper addresses the challenge of detecting multi-node anomalies in the Internet of Energy (IoE), which is crucial to prevent cyber-attacks, improve reliability, and maintain the stability of smart distribution

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

		efficiency		Backpropagation Neural Networks (BPNN) and Support Vector Machines (SVM) in both detection accuracy and computational efficiency	networks
Principal Component Analysis (PCA)	José Roldán-Gómez, Juan Boubeta-Puig, Javier Carrillo-Mondéjar, Juan Manuel Castelo Gómez, Jesús Martínez del Rincón, (2023)	An architecture that integrates Complex Event Processing (CEP) with Machine Learning (ML) to automatically generate CEP rules for detecting attack patterns in real-time.	F1-score, Precision, Recall, Thrsoughput.	Proposed system achieved an average F1-score of 0.98, a 76% improvement in throughput over standard CEP rules, and a reduction in network overhead by 86%.	Difficulty in deploying security measures in IoT devices due to their limited computational capabilities. Lack of pre-defined rules for detecting real-time attacks.
Autoencoders	Amir Farzad, T. Aaron Gulliver (2020)	Combination of Isolation Forest and two deep autoencoder networks for feature extraction and anomaly detection.	Precision, Recall, Accuracy, and F-measure.	Outperforms other well-known anomaly detection methods such as K-means, Gaussian Mixture Model (GMM), and Local Outlier Factor (LOF), in terms of precision and recall for anomaly detection in log messages.	Detecting anomalies in log messages produced by software systems,when dealing with the vast amounts of unlabeled log data.
	Fargana J. Abdullayeva (2021)	Combining autoencoders for feature extraction and softmax regression for classification to detect APT attacks.	Accuracy, training loss, and test loss, measured using RMSE (Root Mean Squared Error) and accuracy scores.	An accuracy of 98.32% and demonstrated effective classification and detection of APT attacks while reducing data size via the autoencoder's encoder layer.	Detection of Advanced Persistent Threat (APT) attacks in cloud computing environments, focusing on the challenges posed by APTs' stealth and complexity.
	Yasuhiro Kanishima,	Autoencoder with Adaptive Loss	Area Under Receiver	Improved the detection	Inconsistency in anomaly scores

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

	Takashi Sudo, Hiroyuki Yanagihashi (2022)	Function (AEAL), which dynamically adjusts the balance between minimizing reconstruction errors for normal data and maximizing reconstruction errors for anomaly data.	Operating Characteristics Curve (AUROC), Histogram Intersection (HI)	accuracy of known anomalies while maintaining consistent anomaly scores before and after model updates. Performed better than traditional autoencoders and provided more consistent results compared to ABC in terms of anomaly score distribution.	before and after updating unsupervised learning-based anomaly detection models to supervised learning-based models. This inconsistency can create operational complexities, such as needing to adjust anomaly judgment thresholds.
	David Novoa-Paradela, Oscar Fontenla-Romero, Bertha Guijarro-Berdiñas (2023)	A non-iterative, fast implementation of deep autoencoders, specifically designed for federated learning and edge computing environments.	F1-score, training time (seconds), and energy consumption (kWh).	Outperformed traditional iterative autoencoders in terms of training time and achieved comparable performance in anomaly detection tasks. It also demonstrated better energy efficiency in federated learning scenarios.	Privacy-preserving deep autoencoder implementations in federated learning, Reducing training time while ensuring data privacy in edge computing scenarios,
	Santiago Gomez-Rosero, Miriam A.M. Capretz (2024).	"Anomaly Detection through Evolutionary Neural Architecture Search (AD-ENAS)," which is a method specifically designed for optimizing neural network architectures for anomaly detection in time series data.	Precision, Recall, F1-score, and ROC-AUC.	Evolved neural network architectures that outperformed baseline methods in detecting anomalies in time series data, achieving higher F1 scores across three well-known datasets (MSL, SMAP, Yahoo S5-A1).	Managing complexity and variability in time series data, which often leads to increased model complexity and prolonged search duration during parameter tuning for anomaly detection.
	Asif Ahmed Neloy,	systematic reviews and comparism of	Reconstruction quality,	Different autoencoder	Effectiveness of various autoencoder

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

	Maxime Turgeon (2024)	11 autoencoder architectures in terms of their performance in anomaly detection tasks on the MNIST and Fashion-MNIST datasets.	sample generation, accuracy in classifying anomalies, ROC-AUC, Average Precision (AP), and training time.	architectures offer trade-offs in reconstruction quality, computational efficiency, and anomaly detection accuracy. For instance, the PAE and VQ-VAE models offered faster training times, while models like adVAE and β-VAE provided better reconstruction quality and sample generation for anomaly detection.	architectures for unsupervised anomaly detection (UAD) Explores the trade-offs between reconstruction ability, sample generation, latent space visualization, and anomaly detection accuracy.
K-Nearest Neighbor (KNN)	Femi Emmanuel Ayo Joseph Bamidele Awotunde Sakinat Oluwabukonla Folorunso Matthew O. Adigun Sunday Adeola Ajagbe (2023)	An improved FFB detection architecture called Bot-FFX, which uses a combination of a rule-based Genetic Algorithm (GA) and K-Nearest Neighbor (KNN) for detecting botnets.	Accuracy False Negative Rate (FNR) False Negative Rate (FNR) True Positive Rate (TPR) True Negative Rate (TNR)	Bot-FFX model achieved high detection accuracy with an overall accuracy of 99.178%, a false positive rate of 0.8%, and a false negative rate of 0.8%.	Vulnerability to evasion mechanisms, long detection time, and high dimensionality of the feature set in existing Fast Flux Botnet (FFB) detection systems.
CNN	Ramna Maqsood, et al. (2023)	Fine-tuned 3D ConvNets for spatiotemporal anomaly recognition; introduced frame-level annotations and spatial augmentation.	AUC	Achieved 82% AUC; robust multiclass anomaly detection.	Difficulty in recognizing multiple anomaly types from unstructured, untrimmed surveillance videos; sparse annotations in datasets.
	Waseem Ullah, et al. (2020)	Combined ResNet-50 for spatial feature extraction and Bi-	Accuracy	Improved accuracy by 3.41% over	High false alarms and challenges in adapting to real-

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

		Directional LSTM for temporal analysis.		SOTA methods; reduced false alarms.	world data complexities for anomaly detection.
	Abdul Rehman Javed, et al. (2020)	Multistage Attention Mechanism combining CNN and LSTM to focus on significant features.	F-Score	Enhanced detection of both single and mixed anomaly types; F-Score improved by 3.24%.	Detecting low-magnitude anomalies in vehicular sensor data and addressing multiple anomaly types.
	Maryam Qasim, Elena Verdu (2023)	Hybrid model combining ResNet (CNN) for spatial features and SRU for temporal sequences.	Accuracy, F1-Score, AUC	Achieved 91.44% accuracy and 91.64% F1-Score with ResNet-50 + SRU.	Inefficiencies in detecting anomalies in large-scale video surveillance systems; challenges in integrating spatial and temporal features.
	In-Chang Hwang, Hyun-Soo Kang (2023)	Used 3D CNN integrated with CBAM; merged video frames into composite images to optimize memory usage and training.	Accuracy, AUC, EER	Achieved AUC of 0.9973 (UBI-Figure hts), 99.20% accuracy (RWF-2000); robust anomaly detection across datasets.	Imbalanced datasets with fewer anomaly samples; increased parameters in 3D CNN training.
RNN	Yang Wang, et al. (2022)	Multi-layer attention-based RNN Encoder-Decoder for spatiotemporal forecasting.	RMSE, MAE	Outperformed traditional models with better prediction accuracy.	Complex characteristics in multivariate time series for environmental monitoring.
	Farheena, Rajeev Kumar (2024)	Combined hybrid feature selection with CNN-LSTM for dimensionality reduction.	RMSE, MAE	Enhanced prediction accuracy with reduced complexity.	Inefficiencies in high-dimensional time-series datasets.
	Praveen M. Dhulavvagol, et al. (2024)	Encoder-decoder RNN architecture with arithmetic coding for text compression.	Compression Ratio	Achieved 3.5x better compression ratio compared to traditional methods.	Inefficiency in traditional text compression algorithms.
	Houda Harbaoui, Emna Ammar Elhadjamorb	Fusion of LSTM and RNN with feature fusion techniques.	Validation Loss, RMSE	Superior performance with lower validation loss	Inadequacies of single models in handling stock price prediction patterns.

	(2024)			and RMSE.	
	Vinod Kumar, et al. (2024)	Hybrid RNN-LSTM model with attention mechanisms for effective temporal forecasting.	RMSE, MAPE	Outperformed baseline models with reduced RMSE and MAPE.	Precision challenges in long-term COVID-19 outbreak prediction.
	Harsh Agarwal, et al. (2024)	Multi-Layer Sequential LSTM for improved long-term dependency modeling.	MAPE, N-RMSE	Achieved 91.97% accuracy on test data, outperforming ARIMA and RNN.	Limitations of traditional statistical models in stock price prediction.
	Pooja BR, Rajkumar N. (2024)	Combined spatiotemporal autoencoder and 3D CNN with RNN for real-time anomaly detection.	Accuracy, MSE	Achieved 96% accuracy in identifying anomalies in surveillance systems.	Inefficiencies in manual surveillance and large-scale video analysis.
LSTM	H.D. Nguyen et al. (2020)	LSTM for forecasting; LSTM Autoencoder + SVM for anomaly detection.	RMSE, Accuracy, Precision, Recall, F1-score	Superior RMSE for forecasting; 98.36% accuracy, 98.45% precision, 99.59% recall in anomaly detection.	Challenges in multivariate time series forecasting and anomaly detection in supply chain management.
	Mahmoud S. Elsayed et al. (2020)	LSTM Autoencoder for temporal feature learning; SVM for anomaly classification.	Precision, Recall, F1-Score, Accuracy, AUC	93% F1-Score, 90.5% accuracy; improved computational efficiency over standalone SVM.	Anomaly detection in high-dimensional and unbalanced network datasets.
	Yara Alghofaili et al. (2020)	LSTM for sequential fraud pattern detection, benchmarked against Autoencoder, RF, SVM, and LR.	Accuracy, Loss Rate, Execution Time	99.96% accuracy, 0.21% loss rate, better performance than baseline models.	Detecting financial fraud in highly skewed datasets with evolving patterns.
	Shuixiang Wang (2024)	BiLSTM with attention mechanism for feature extraction; IBPNN for non-linear predictions.	Accuracy, Specificity, Sensitivity, Type I and II Errors	Improved accuracy, sensitivity, specificity; reduced computational time.	Inefficiencies in anomaly detection for large-scale financial auditing datasets.

	Yunlong Li et al. (2024)	Feature-attended LSTM for correlation analysis; Federated Learning for privacy-preserving training.	Accuracy, AUC, True Positive Rate	334.36% accuracy improvement; AUC improved by 24.92%; significant gains in anomaly detection efficiency.	Low accuracy and privacy concerns in anomaly detection for FIoT.
	Jay Raval et al. (2023)	XAI for feature selection; Blockchain for secure storage; LSTM for sequential pattern detection.	Accuracy, Loss Rate, Gas Cost, Precision, Recall, AUC	99.8% accuracy; enhanced interpretability and secure, transparent classification results via blockchain integration.	Complexity and lack of interpretability in credit card fraud detection methods.
	Zhan Wang et al. (2023)	LSTM enhanced with dropout, bidirectional layers, and attention; NLP for preprocessing and labelling.	F1-Score, Validation Loss	Validation F1-score of 92.19%, validation loss of 0.3433; robust and efficient classification of payment system errors.	Inconsistent formats of payment failure messages and lack of automated error classification methods in financial systems.
RF, Naïve Bayes, DT	Fatima Dakalbab et al. (2022)	Reviewed 120 studies, focusing on supervised, unsupervised, and hybrid ML techniques for diverse crime prediction tasks.	Mean Error, Accuracy, Recall	Effective in identifying crime hotspots with robust predictions; highlighted gaps in datasets and scalability.	Challenges in applying AI for crime prediction, including dataset limitations and lack of interpretability.
LSTM, CNN, RNN	Tosin Ige et al. (2024)	Survey of algorithms for detecting cyberattacks, highlighting strengths of deep learning models like RNN and LSTM.	Accuracy, Precision, Recall	Demonstrated Random Forest and XGBoost as high-performing models; CNN and RNN excel in detecting context-sensitive attacks.	Ineffectiveness of traditional ML in advanced cyberattack detection (e.g., SQLi, phishing).
K-Means, Bayesian Network	O'rinov Nodirbek et al. (2022)	Comparative analysis of HMM, Bayesian Networks, and KNN for fraud detection across transaction domains.	Accuracy, False Alarm Rate	Bayesian Networks and HMM outperformed in accuracy and anomaly	Increased fraud cases in e-commerce; difficulties in combining offline and online fraud

				identification.	detection.
Isolation Forest, LOF	Juliet Onyema et al. (2023)	Proposed system using Isolation Forest and LOF; integrated OTP validation.	Accuracy, Precision, Recall	Achieved high fraud detection accuracy (90-100%) by validating users and analyzing spending patterns.	Real-time credit card fraud detection amid rising online transactions.
LSTM, GRU, CNN	Ibomoiye Domor Mienye et al. (2024)	Reviewed deep learning architectures, emphasizing LSTM and hybrid models for fraud detection.	ROC-AUC, Precision, Recall	LSTM, GRU, and Transformers outperformed in handling sequential and feature-based fraud data.	Class imbalance in financial datasets and lack of labeled data.
DeepWalk, XGBoost	Anonymous (2022)	Proposed CATCHM: a network representation learning method with downstream classifiers like XGBoost.	AUCPR, F1-Score	Outperformed benchmarks with superior AUCPR and real-time detection capabilities.	Fraud detection in large transaction datasets with class imbalance.
Random Forest, Neural Networks	Musibau Ibrahim et al. (2023)	Applied SMOTE and ensemble models like Random Forest to enhance fraud detection accuracy.	Precision, Recall, Accuracy	Random Forest achieved 99.58% accuracy; improved fraud detection efficiency through preprocessing.	Dataset imbalance and complexity of online payment systems.
HMM, DBSCAN	Abukari Abdul Aziz et al. (2023)	Multi-layered HMM with hybrid optimization (GA, PSO) for scalability and efficiency.	Precision, Recall, F1-Score	Reduced detection time and achieved high precision (PAYSIM: 0.984; MMT: 0.986).	High false positives and negatives in fraud detection.
SVM, DNN	Ata-Ur Rehman et al. (2021)	Integrated audio and video cues for multi-modal anomaly detection, combining SVM and DNN.	AUC, Precision, Recall, F1-Score	Improved detection accuracy and reduced false positives/negatives in noisy environments.	Limited anomaly detection in outdoor environments using single-modality data.
ResNeXt-	Abdulwahab	Introduced EARN	Accuracy,	Achieved 98%	Imbalanced

GRU	Ali Almazroi et al. (2023)	framework and RXT-J classifier for real-time fraud detection.	AUC, ROC, Execution Time	accuracy; scalable and effective in handling imbalanced data.	datasets, temporal dependencies, and concept drift in fraud detection.
DT-SVMNB	Md. Shafiur Rahman et al. (2021)	Hybrid model combining Decision Tree, SVM, and Naïve Bayes for social network anomaly detection.	Accuracy, Precision, Recall, F1-Score	Achieved 98% accuracy in detecting anomalous users and suicidal tendencies.	High-dimensional data in social networks and identifying malicious behavior.
BN-SVP	Hitesh Sapkota et al. (2022)	Developed BN-SVP using Bayesian nonparametric methods and submodular optimization for anomaly detection.	AUC, ROC	Achieved state-of-the-art AUC scores; robust against noisy anomalies.	Noise sensitivity and multimodal anomaly detection in video data.
DBN, MJPF	Divya Kanapram et al. (2022)	Used DBN and MJPF for interpretable anomaly detection in autonomous systems.	Generalized Errors, KL Divergence	Enabled dynamic adaptability and reduced errors in autonomous agent networks.	Anomaly detection in autonomous networks with interpretability challenges.
GNN, Bayesian Networks	Lejla Terzić et al. (2021)	Applied econometric and statistical methods; no explicit ML algorithm used.	GDP Per Capita, GCI, GII	Demonstrated the relationship between innovation and economic growth, emphasizing GCI and GII.	Examining competitiveness and innovation impacts on economic growth.
BiLSTM-Attention-IBPNN	Shuixiang Wang (2024)	Combined BiLSTM with attention mechanisms and IBPNN for non-linear predictions.	Accuracy, Specificity, Sensitivity, Type I and II Errors	Improved accuracy and reduced computational time; enhanced sensitivity and specificity for auditing datasets.	Inefficiencies in anomaly detection for financial auditing.
Feature-Attended LSTM, Federated Learning	Yunlong Li et al. (2024)	Feature-attended LSTM for correlation analysis; federated learning for privacy-preserving training.	Accuracy, AUC, True Positive Rate	Achieved a 334.36% accuracy improvement over standalone methods; better adaptability to dynamic	Low accuracy and privacy concerns in FIoT anomaly detection.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

				environments.	
X-LSTM, Blockchain	Jay Raval et al. (2023)	Combined Explainable AI with LSTM for feature selection; used blockchain for tamper-proof classification storage.	Accuracy, Loss Rate, Precision, Recall, AUC	Achieved 99.8% accuracy; enhanced interpretability and traceability with secure, transparent classifications via blockchain.	Lack of transparency in LSTM-based fraud detection models and secure transaction classifications.
GraphSAGE	Shucheng Li et al. (2021)	Proposed SIEGE using self-supervised incremental deep graph learning for efficient phishing scam detection.	Accuracy, Precision, Recall, F1 Score	Achieved 4%-16% improvement in F1 scores over baseline models, addressing label scarcity and scalability.	Scalability, label scarcity, and temporal imbalance in Ethereum phishing scam detection.
GCN, GAT, EvolveGCN	Jianian Wang et al. (2022)	Reviewed GNN methodologies and categorized their applications in finance.	AUC, Precision, Recall, F1 Score, MSE	Identified scalability and explainability challenges; emphasized advancements needed in GNN applications for finance.	Complexity in representing dynamic, heterogeneous financial graphs for tasks like fraud detection and stock prediction.
GRU, Attention	Zhihao Ding et al. (2024)	Introduced DIAM using Edge2Seq and multigraph discrepancy mechanisms for illicit account detection.	Precision, Recall, F1 Score, AUC	Outperformed baselines with 96.55% F1 score on Bitcoin datasets; scalable for large graphs.	Anonymity and multigraph discrepancies in cryptocurrency transaction networks.
Temporal Graph Neural Network	Yanbang Wang et al. (2024)	Developed dual-view framework combining graph snapshots and link streams with negative sampling protocol.	False Positive Rate, Accuracy, Average Precision	Reduced false positives to 4.69% and achieved 94.52% accuracy on Microsoft authentication datasets.	High false positives and challenges in anomaly detection from authentication alerts in security systems.
GAT, Contrastive Learning	Sijia Li et al. (2023)	Introduced TGC, using node- and context-level contrastive learning for efficient phishing detection.	F1 Score, Precision, Recall	Achieved 95.5% F1 score and scalability on large Ethereum transaction datasets.	Sparse distribution and natural camouflage in Ethereum phishing nodes.

GAT	Chensu Zhao et al. (2020)	Proposed GAT-based semi-supervised spam bot detection using multi-relational graphs.	F1 Score, PRAUC, Precision, Recall	Achieved 0.91 F1 score and PRAUC; robust to imbalanced datasets.	Spam bots evading detection and scalability challenges in large social networks.
SAGEConv, GRU	Zhen Chen et al. (2024)	Proposed multiscale feature fusion model integrating temporal, structural, and basic features.	Accuracy, Precision, Recall, F1 Score, AUC	SAGEConv achieved 95.8% F1 score; superior scalability and accuracy for Ethereum phishing detection.	Loss of historical transaction data and inefficiency in representing both temporal and topological data.
SEGE	Shaojiang Wang et al. (2024)	Introduced SEGE combining structural entropy minimization and graph embeddings.	Recall, Precision, F1 Score	Achieved 0.505 F1 score on cnBank dataset and demonstrated community-based anomaly detection.	Sparse labels and collaborative behaviors in money laundering detection.
GCN, Attention	Beibei Han et al. (2024)	Introduced MT2AD for anomaly detection in multi-token, temporal transaction networks.	Precision, Recall, F1 Score, Loss	Achieved 0.8789 precision and superior anomaly detection across multi-token datasets.	Ignoring timestamps and multi-token transactions in Ethereum networks.
Random Forest, Biased Walk	Chuyi Yan et al. (2023)	Developed Aparecium using biased random walk and Random Forest for feature-rich scam detection.	Precision, Recall, F1 Score, Embedding Time	Achieved 0.967 F1 score, reducing false positives and improving scalability for Ethereum datasets.	Sparse Ethereum datasets and challenges in maintaining low false positives.
GraphSAGE, SHAP	Jeyakumar Samantha Tharani et al. (2024)	Introduced a unified feature engineering framework combining graph-based and statistical features for malicious entity detection.	Accuracy, Precision, Recall, F1 Score, AUC	Achieved up to 97.86% accuracy on Ethereum and Bitcoin datasets; improved interpretability with SHAP analysis.	Lack of systematic feature engineering and high computational costs in blockchain fraud detection.
Dynamic GNN	Shui Yu (2024)	Proposed continuous dynamic network link prediction using neighborhood	AUC, Precision, Link Prediction	Improved link prediction accuracy and demonstrated	Challenges in predicting relationships in evolving financial

		message aggregation.	Accuracy	network resilience under stress scenarios.	networks like the OTC bond dealer network.
ML Algorithm	Authors (Year)	Proposed Solutions	Evaluation Metric	Outcome	Issues
GANs, XGBOD	Seyyede Zahra Aftabi, Ali Ahmadi, Saeed Farzi (2023)	A hybrid approach combining GANs for synthetic sample generation and XGBOD for feature engineering and outlier detection.	Accuracy, Precision, Recall, F1-Score	GANs generated synthetic fraud-prone samples effectively; XGBOD achieved high accuracy and recall, outperforming traditional methods like SVM and Logistic Regression.	Imbalanced datasets, lack of fraud-prone samples, high-dimensional data, and ineffective traditional audit approaches.
PSA-GAN, SeqGAN, DAEGAN, SSGAN, Quant GANs, C-RNN-GAN	Zihan Chen, Yifei Wang, Shuchen Zhang (2023)	Advanced GAN architectures like DAEGAN for credit card fraud detection, PSA-GAN for time-series modeling, SeqGAN for discrete sequence generation, and SSGAN for online gambling fraud detection.	Accuracy, Precision, Recall, F1-Score, AUC, AUPRC	GANs improved anomaly detection and predictive modeling, addressing data imbalance and achieving higher performance compared to traditional methods.	Data imbalance, computational complexity in financial datasets, challenges in stock market prediction, time-series analysis, and fraud detection.
UAAD-FDNet (GANs, Autoencoders)	Shanshan Jiang, Jie Wang, Ruiting Dong, Min Xia (2023)	Proposed UAAD-FDNet with autoencoders for feature reconstruction and GANs for adversarial learning, incorporating channel-wise feature attention and hybrid loss functions.	Precision, Recall, F1-Score, AUC	UAAD-FDNet outperformed traditional methods with superior AUC and F1-Score, demonstrating robustness against data imbalance and feature complexity.	Ineffective traditional methods (e.g., SVM, Random Forest) for unknown attack patterns, imbalanced data, and difficulty in extracting features from transaction data.
VAE, WGAN, AE	Zhiyuan Chen, Waleed Mahmoud Soliman, Amril Nazir, Mohammad Shorfuzzaman	Combined VAE for probabilistic anomaly scoring, WGAN for generating synthetic samples, and AE for learning transaction	Accuracy, Precision, Recall, F1-Score, AUC	Reduced false positive rates to 7%, 100% recall of fraudulent transactions, and improved detection	Difficulty detecting irregular patterns in imbalanced datasets, high false positives in anti-money laundering (AML) systems, and

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

	(2021)	representations, along with a novel Recall-First Threshold metric for evaluation.		capabilities through balanced datasets created using WGAN.	inability to adapt to new fraud patterns.
GANs, XGBOD	Seyyede Zahra Aftabi, Ali Ahmadi, Saeed Farzi (2023)	Hybrid approach combining GANs for synthetic sample generation and XGBOD for feature engineering and outlier detection.	Accuracy, Precision, Recall, F1-Score	GANs generated synthetic fraud-prone samples effectively; XGBOD achieved high accuracy and recall, outperforming traditional methods like SVM and Logistic Regression.	Imbalanced datasets, lack of fraud-prone samples, high-dimensional data, and ineffective traditional audit approaches.
UAAD-FDNet (GANs, Autoencoders)	Shanshan Jiang, Jie Wang, Ruiting Dong, Min Xia (2023)	Proposed UAAD-FDNet with autoencoders for feature reconstruction and GANs for adversarial learning, incorporating channel-wise feature attention and hybrid loss functions.	Precision, Recall, F1-Score, AUC	UAAD-FDNet outperformed traditional methods with superior AUC and F1-Score, demonstrating robustness against data imbalance and feature complexity.	Ineffective traditional methods (e.g., SVM, Random Forest) for unknown attack patterns, imbalanced data, and difficulty in extracting features from transaction data.
VAE, WGAN, AE	Zhiyuan Chen, Waleed Mahmoud Soliman, Amril Nazir, Mohammad Shorfuzzaman (2021)	Combined VAE for probabilistic anomaly scoring, WGAN for generating synthetic samples, and AE for learning transaction representations, along with a novel Recall-First Threshold metric for evaluation.	Accuracy, Precision, Recall, F1-Score, AUC	Reduced false positive rates to 7%, 100% recall of fraudulent transactions, and improved detection capabilities through balanced datasets created using WGAN.	Difficulty detecting irregular patterns in imbalanced datasets, high false positives in anti-money laundering (AML) systems, and inability to adapt to new fraud patterns.
LSTM, GRU, Random Forest, Bayesian Networks, Deep Q-Networks,	Rasoul Amirzadeh, Asef Nazari, Dhananjay Thiruvady (2022)	Application of supervised learning for price prediction and RL models for autonomous trading strategies, integrating sentiment analysis	RMSE, MAE, F-score, Sharpe Ratio, Cumulative Returns	AI techniques significantly improved cryptocurrency price prediction accuracy, reducing market risks and	Challenges in price prediction and movement forecasting in cryptocurrency markets using AI techniques.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

PPO, Advantage Actor-Critic		with financial models.		optimizing trading policies.	
SVM, Decision Trees, Q-Learning, Deep Q-Networks, DRL	Merve Ozkan-Okay, et al. (2024)	Comprehensive survey of AI techniques in cybersecurity, highlighting DRL for adaptive detection in dynamic environments.	Accuracy, F1 Score, Precision, Recall, ROC-AUC, Anomaly Detection Rate	DRL demonstrated superior adaptability and precision in detecting diverse cyber threats, automating detection and countermeasure strategies.	Increasing complexity of cyberattacks and challenges in detecting zero-day vulnerabilities, dynamic attacks, and malware.
Deep Q-Network (DQN)	Abdul Qayoom, et al. (2024)	Implemented DQN for real-time fraud detection, leveraging temporal patterns in transaction data for better accuracy.	Accuracy, Loss, Reward	Achieved 97.10% accuracy with DQN, demonstrating real-time adaptability and reducing false positives in fraud detection.	Growing incidents of credit card fraud and difficulty in real-time fraud detection using traditional methods.
Hierarchical Reinforcement Learning (HRL)	Arwa AlKhonaini, Tarek Sheltami, et al. (2024)	Proposed HRL with policy gradient optimization for RF-based UAV detection, integrating hierarchical policies for efficient decision-making and identification.	Accuracy, Policy Loss, Cross-Entropy Loss, Reward-Based Metrics (Cumulative Return)	Achieved 99.7% detection accuracy, showcasing HRL's scalability and precision in UAV security applications.	Detecting UAV intrusions in secured environments using traditional visual and acoustic detection methods prone to limitations.
Hierarchical LSH-LOF, Factorization Machines, Autoencoders	Feng Zheng, Quanyun Liu (2020)	Multi-faceted Telecom Customer Behavior Analysis (MTCBA) framework combining Hierarchical LSH-LOF for anomaly detection and FM-AE for dimensionality reduction and clustering.	AUC, Recall, RMSE	Improved anomaly detection and clustering with actionable insights for fraud prevention and precision marketing in telecom operations.	Detecting anomalous telecom customer behavior for fraud prevention and clustering customer data for actionable insights.
Lightweigh t CNN, LSTM,	Sareer Ul Amin et al.	Attention-Based Deep Learning Approach (ADSV)	AUC, R	Achieved 99% AUC for CUHK-Avenue and 97%	Difficulty detecting anomalies in surveillance videos

Attention Mechanism	(2023)	combining Lightweight CNN, LSTM, and attention mechanisms for feature extraction and prioritization.		AUC for UCF-Crime datasets; reduced false alarm rates significantly.	due to low-quality footage, diverse patterns, and lack of labeled data.
Local Outlier Factor (LOF), Improved LOF, COF, LoOP, kNN	Arya Adesh, Shobha G, Jyoti Shetty, Lili Xu	Scalable, distributed implementation of Improved LOF on HPCC Systems.	Precision, Recall, F1 Score, Accuracy, Cluster Execution Time	Improved LOF handled duplicates better, showed superior scalability in HPCC Systems.	High computational complexity, redundancy in LOF, challenges in distributed anomaly detection.
Local Outlier Factor (LOF), COF, KMeans	Agnieszka Nowak-Brzezińska, Czesław Horyń	Comparative analysis of LOF, COF, and KMeans for rule-based clustering quality.	Silhouette Index, Dunn Index, Davies-Bouldin Index, CPCC, Pseudo F, Hubert-Levine Index	COF improved clustering quality across diverse datasets more frequently than LOF or KMeans.	Impact of outliers on rule-based clustering quality, difficulty in maintaining cluster quality.
Local Outlier Factor (LOF), Self-Organizing Maps (SOM)	Czesław Horyń, Agnieszka Nowak-Brzezińska	Combining LOF and SOM for detecting and visualizing anomalies in rule-based systems.	Quantization Error (QE), Mean Quantization Error (MQE), LOF values	SOM excelled in visualization; LOF provided finer granularity in density-based detection.	Incomplete, redundant, inconsistent rules; challenges in identifying unusual rules.
XBoost, LightGBM, XGBoost, Extended Classifier Systems (XCSR)	Pandey, M. (2024)	Development of ML-based predictive models incorporating physiological, ventilator, and historical patient data.	Accuracy, Precision, Sensitivity, F-score, ROC, AUC	Improved predictability of weaning success rates; need for explainable AI and standardized data collection practices.	High ventilator weaning failure rates; challenges in clinical decision-making; limitations in predictive models.
Supervised (SVM, RF, DT, ANN), Unsupervised (GANs), Reinforcement Learning (Bi-LSTM, Transformer models), Deep	Hashmi, E., Yamin, M. M., & Yayilgan, S. Y. (2024)	Hybrid AI defense strategies combining rule-based and learning-based methods.	Accuracy, Precision, Recall, F1-Score, ROC, AUC	Enhanced threat detection, anomaly detection, and malware classification; improved adaptability of security models.	Evolving cyber threats; inadequacies in traditional rule-based security systems.

Learning (CNN, Bi-LSTM)					
k-Means clustering, C4.5 Decision Tree	Amuthan Prabakar Muniyandi, R. Rajeswari, R. Rajaram (2012)	Cascading k-Means and C4.5 Decision Tree for better decision boundaries	TPR, FPR, Precision, Accuracy, F-measure, ROC, AUC	Improved detection accuracy (95.8%), reduced FPR to 0.1%	High false positives, limited performance of single ML techniques, issues with k-Means clustering
Decision Trees, Autoencoders	Diana Laura Aguilar, Miguel Angel Medina-Pérez, Octavio Loyola-González et al. (2022)	Decision Tree-based Autoencoder for interpretability and categorical data handling	AUC, AUC-PR	Achieved competitive AUC scores; interpretability in anomaly detection	Lack of interpretability in DL models, inefficiency with categorical data handling
YOLOv5 (object detection), Decision Tree	Armstrong Aboah, Maged Shoman, Vishal Mandal et al. (2021)	YOLOv5 for detection, Decision Tree for verification and false positive filtering	F1 Score, RMSE, S4 Score	Ranked 5th in NVIDIA AI City Challenge; reduced false positives and improved detection	Manual traffic monitoring inefficiencies, occlusion challenges, poor video quality
Decision Tree, Random Forest	Qingyang Zhang (2022)	Decision Tree and Random Forest with "abnormal point scale" for financial anomaly detection	Accuracy, Computational Time, Robustness (5-fold CV)	Improved accuracy (2-8%) and robustness across datasets; faster anomaly detection	Inefficient financial anomaly detection, lack of robustness, high noise sensitivity
Random Forest (Bagging), XGBoost (Boosting)	Shay Vargaftik, Isaac Keslassy, Ariel Orda, Yaniv Ben-Itzhak (2021)	RADE framework using hierarchical decision tree models for efficient anomaly detection	Macro F1 Score, AUC, Kappa, Resource metrics (memory, training, latency)	Achieved 12× lower memory usage, 20× faster training, and maintained competitive accuracy	Resource inefficiencies in decision tree ensembles, high resource consumption for large datasets
Naïve Bayes, Genetic Algorithm	John Oche Onah et al. (2021)	Wrapper-Based Feature Selection using Genetic Algorithm combined with Naïve Bayes for classification.	Accuracy, Precision, F1 Score, Execution Time	Achieved 99.73% accuracy with better performance compared to other algorithms. Low false positive rate.	Network security challenges in fog computing due to proximity to users and limited resources.
Naïve	Monika	A two-phase	Accuracy,	Achieved 97%	IoT security

Bayes, Elliptic Envelope	Vishwakarma, Nishtha Kesswani (2023)	intrusion detection system combining Naïve Bayes classifiers with elliptic envelope for anomaly detection.	Precision, Recall, F1 Score, False Positive Rate	accuracy on NSL-KDD, 86.9% on UNSW_NB15, and 98.59% on CIC-IDS2017 datasets.	vulnerabilities from lightweight protocols and imbalanced datasets.
Logistic Regression, Naïve Bayes, Random Forest, AdaBoost, Support Vector Machines	Laura Vigoya et al. (2021)	Validated DAD dataset using ML algorithms; applied feature selection and data balancing (SMOTE).	Accuracy, Precision, Recall, F1 Score, ROC AUC	Tree-based models (Random Forest, AdaBoost) achieved the best results, with mean ROC AUC close to 1.	IoT vulnerabilities due to lightweight protocols and limited computation resources.
Supervised Cultural Genetic Algorithm, Kohonen Neural Network	Arnold Adimabua Ojugo, Obinna Nwankwo (2021)	Hybrid model combining spectral clustering and genetic algorithm-trained modular neural network.	Sensitivity, Specificity, Accuracy	Achieved high sensitivity (90%) and moderate accuracy (74%), effectively identifying fraudulent transactions.	Noise and ambiguity in data lead to inefficiency in credit card fraud detection, with high false-positive rates.
K-Means Clustering	Yusuf Lanre Lawal (2014)	Network science and K-means clustering applied to analyze Ethereum transaction data.	Silhouette Score	Successfully identified anomalies related to significant events like the Parity Wallet Hack with a Silhouette Score of 0.757.	Anonymity in Ethereum transactions enables malicious activities, lacking effective anomaly detection methods.
GTN2vec (Graph Embedding), Random Forest	Jiayi Liu et al. (2023)	GTN2vec for feature extraction and Random Forest for classification.	Accuracy, Precision, Recall, F1-Score	Achieved 95.7% accuracy, significantly outperforming existing methods in detecting money laundering accounts.	Ethereum's anonymity attracts illicit activities like money laundering, with inefficiencies in existing detection systems.
Deep Learning Models (ResNet50, DenseNet121,	Smaranda Belciug, Dominic Gabriel Iliescu (2023)	Combination of deep learning models with GMM clustering to improve view plane differentiation in	Classification Accuracy, Standard Deviation, Statistical Tests	Outperformed stand-alone models, achieving enhanced classification	Challenges in differentiating view planes in fetal morphology scans due to varying maternal and fetal

InceptionV3, EfficientNetV2S, MobileNetV3Large, Xception), Gaussian Mixture Model		medical imaging.	(ANOVA, Tukey)	accuracy and reliability in differentiating fetal view planes.	factors.
K-Means, Gaussian Mixture Model	Eva Patel, Dharmender Singh Kushwaha (2020)	Comparison of K-Means and GMM clustering to analyze cloud workload heterogeneity and optimize resource management.	Within-Cluster Sum of Squares (SSE), AIC, BIC	GMM achieved more precise workload clustering with distinct boundaries but had higher computational costs compared to K-Means.	Heterogeneity in cloud workloads complicates effective resource management and capacity planning.