AN EMPIRICAL ANALYSIS OF ANOMALY DETECTION MODEL PARADIGMS UNDER HETEROGENEOUS IOMT ATTACK TRAFFIC

Visvakaanth Kamalakannan Thamaraiselvi
Department of Computer Science
R.M.K. Engineering College
Chennai, India
Email: 230566.cs@rmkec.ac.in
ORCID: 0009-0002-1231-2506

ABSTRACT

Background: Hospitals increasingly rely on heterogeneous Internet of Medical Things (IoMT) devices, which generate highly diverse network traffic.This discrepancy between traffic heterogeneity and joint anomaly modeling is an important question regarding how different anomaly detection paradigms understand abnormal behavior.

Methods: This paper describes an empirical study of three unsupervised anomaly detection model paradigms Isolation Forest (tree-based), One-Class Support Vector Machine (boundary-based), and Local Outlier Factor (density-based) using the CICIoMT2024 dataset, which contains traffic from multiple IoMT devices. We synthetically engineer malicious network flow scenarios from this dataset to evaluate how each model responds to anomalous behavior when exposed to the same attack inputs.

Results: Rather than focusing entirely on binary detection outcomes this study emphasizes differences in anomaly score behavior and detection sensitivity across different models. The results highlight that model responses vary significantly depending on how abnormality is defined.

Keywords— Internet of Medical Things (IoMT), anomaly detection, intrusion detection system, Isolation Forest, One-ClassSVM, Local Outlier Factor, heterogeneous IoMT traffic, empirical analysis.

I. INTRODUCTION

Healthcare environments utilize diverse medical equipment that are used to carry sensitive information. These devices are described as Internet of Medical Things (IoMT) devices. These IoMT devices are distinct in the way they operate, some send packets faster than the others, some are idle and then are active for a short time before going idle again, some use different ports and protocols while some transmit different information. Since these devices carry such important information the security of these IoMT devices poses a critical security risk.

Although hospitals often segment IoMT devices across VLANs or network subnets, traffic is typically aggregated at a central server for security monitoring. Centralized anomaly detection models deployed at these aggregation points must therefore evaluate traffic from multiple device types simultaneously. In such settings, the underlying modeling assumptions strongly influence detection performance and reliability.

Existing research on IoMT security largely focuses on designing new models or optimizing specific anomaly detection algorithms. While many studies report accuracy metrics, only a few provide detailed empirical comparisons of how different anomaly detection paradigms—such as tree-based, boundary-based, and density-based models—behave when exposed to heterogeneous IoMT traffic. In particular, the impact of modeling assumptions on anomaly score distributions and detection sensitivity across diverse attack patterns remains underexplored.

This work addresses this gap by conducting a comprehensive empirical analysis of three unsupervised anomaly detection paradigms—Isolation Forest, One-Class Support Vector Machine, and Local Outlier Factor—using the CICIoMT2024 dataset. Our contributions are threefold:

- Synthetically engineering malicious network flow scenarios from heterogeneous IoMT traffic for controlled evaluation

- Comparing model responses not only in terms of detection accuracy but also in anomaly score behavior and sensitivity to different attack patterns.

- Providing practical insights for deploying centralized anomaly detection systems in heterogeneous healthcare networks.

II. RELATED WORK

The security of IoMT devices has attracted significant attention due to its critical nature in healthcare operations and the sensitivity of the information it carries. IoMT devices are majorly heterogeneous that includes wearables, infusion pumps, imaging systems, and monitoring sensors, each generating distinct traffic patterns. This heterogeneous pattern combined with its different communication protocols and resources utilized, makes IoMT systems vulnerable to cyber attacks such as data breaches, unauthorized access, and denial-of-service attacks.

Prior work has explored various approaches regarding the security of IoMT devices. Signature-based intrusion detection systems depends on known attack patterns, which limit their ability to detect zero day threats. Supervised machine learning approaches have been applied to IoMT traffic to classify normal and anomalous behavior, using models such as Random Forests, Support Vector Machines, and deep learning architectures. These approaches, however, require labeled datasets and often struggle to generalize unseen attack types.

Various studies have analyzed unsupervised anomaly detection methods such as Isolation Forest, One-Class Support Vector Machine, and Local Outlier Factor. While these methods demonstrate promising detection performance, prior work often focuses on single-model evaluation or aggregate accuracy metrics, without examining how different paradigms respond to the same heterogeneous traffic or attack patterns.

Recent studies provide a broader perspective on ML applications in IoMT security. For example, (Himanshu Sharma et al., 2026) discuss machine learning frameworks to detect anomalies, safeguard distributed networks, and preserve data privacy in heterogeneous IoMT systems. While comprehensive, this work is primarily theoretical and does not perform an empirical comparison of multiple anomaly detection paradigms. Similarly, (Prathamesh Chandekar et al., 2025) employ ensemble AI models on the CICIoMT2024 dataset to detect anomalous behavior. Although it demonstrates high predictive performance, this study focuses on model-specific optimization rather than a comparative analysis of the various unsupervised model paradigms.

In contrast, the present study addresses this gap by conducting a comprehensive empirical evaluation of three unsupervised anomaly detection paradigms — Isolation Forest, One-Class Support Vector Machine, and Local Outlier Factor — using the CICIoMT2024 dataset. Our analysis examines not only detection accuracy but also anomaly score behavior and sensitivity across diverse IoMT attack flows, providing practical insights into how different paradigms interpret abnormality in heterogeneous healthcare networks.

III. METHODOLOGY

A.Dataset Description

The experiments in this work utilize the CICIoMT2024 (Dadkhah et al., 2024) dataset, which contains network traffic collected from a variety of Internet of Medical Things (IoMT) devices commonly found in hospital environments. Each network flow is represented by numerical features such as packet timing, size, and protocol used [Pre-Encoded]. Device identities in the dataset are anonymized, however, the traffic remains heterogeneous, reflecting diverse communication behaviors across different IoMT device categories. Some traffic streams portray continuous activity, while others show irregular or burst-like transmission patterns. This heterogeneity mirrors real-world hospital network conditions and motivates the evaluation of anomaly detection models trained on aggregated and partitioned traffic representations.

B. Feature Representation and Preprocessing

The CICIoMT2024 dataset provides flow-level statistical features extracted from heterogeneous IoMT network traffic. These features describe multiple aspects of communication behavior, including:

a) Packet header characteristics (e.g., header length, protocol type, time-to-live)

b) Transport-level flag statistics (e.g., SYN, ACK, FIN, RST flag counts and ratios)

c) Protocol usage indicators (e.g., TCP, UDP, HTTP, HTTPS, DNS, MQTT-related traffic)

d) Traffic volume metrics (e.g., total packet count, total size, rate)

e) Packet size statistics (minimum, maximum, average, standard deviation, and variance)

f) Temporal behavior (inter-arrival time and flow timing characteristics)

Since the selected anomaly detection models are distance- and density-based, feature scaling is necessary to prevent attributes with larger numeric ranges from dominating the learning process. Therefore, all features were standardized prior to model training.

No feature selection was applied, as the goal of this study is to evaluate model behavior under realistic heterogeneous traffic conditions rather than optimize detection performance for a specific feature subset.

All models were trained using only benign IoMT traffic to simulate an unsupervised anomaly detection deployment scenario.

C. Anomaly Detection Models

This study focuses on three different unsupervised anomaly detection models, Isolation Forest, One-Class Support Vector Machine and Local Outlier Factor. All models are trained solely on benign traffic from the CICIoMT2024 dataset and then tested on the five constructed attack scenarios.

1) Isolation Forest:
Isolation Forest is a tree-based model that identifies anomalies by recursively splitting the feature space (Liu et al., 2008). Observations that require fewer splits to isolate are considered more anomalous. This method works well for high-dimensional IoMT traffic and can efficiently detect outliers without assuming a specific data distribution. The model was configured with 50 estimators and a contamination parameter set to “auto.”

2) One-Class Support Vector Machine:
OC-SVM is a boundary-based anomaly detection model that learns a decision function to separate the majority of the data from the origin in feature space (Schölkopf et al., 2001). Points lying outside this learned boundary are classified as anomalies. OC-SVM is effective for modeling heterogeneous traffic with distinct normal patterns. Radial basis function (RBF) kernel was used with the “nu” parameter set to 0.05.

3) Local Outlier Factor:
LOF is a density-based anomaly detection model that measures the local deviation of a sample compared to its neighbors (Breunig et al., 2000). Samples with relatively lower density than their neighbors are labeled as anomalies. This approach captures local structure in heterogeneous IoMT traffic, allowing detection of context-dependent deviations. The number of neighbors (n_neighbors) for the model was set to 20.

All models output an anomaly score for each network flow which indicates the degree of abnormality. This score is used to compare model sensitivity across different attack scenarios, in addition to binary anomaly detection outcomes.

D. Attack Scenario Construction

To evaluate how different anomaly detection paradigms respond to heterogeneous malicious behaviors, five representative IoMT attack scenarios were synthetically engineered by modifying benign network flows from the CICIoMT2024 dataset. Each scenario reflects a realistic stage in a network intrusion lifecycle, while preserving statistical plausibility within IoMT traffic characteristics.

1) Slow TCP Port Scan:

This scenario simulates a low-rate reconnaissance scan designed to avoid detection. The flow exhibits moderate packet rates, increased inter-arrival times, and a predominance of SYN and RST activity with limited ACK responses. Traffic volume remains relatively small, mimicking a stealthy probing strategy that attempts to *remain within normal traffic variability.*

2) Aggressive TCP Port Scan:

In contrast to the slow scan, this scenario represents a high-intensity port scan characterized by extremely high packet rates, near-zero inter-arrival times, and a dominant SYN flag distribution. Large packet counts and rapid transmission emulate burst scanning behavior commonly used for fast reconnaissance.

3) Evasive (Stealth) Scan:

This scenario represents a scan designed to blend with legitimate traffic. Instead of excessive SYN activity, the flow includes a high proportion of ACK and PSH flags, moderate packet rates, and greater packet size variability. This creates a profile that resembles normal application communication while still performing reconnaissance.

4) HTTPS Vulnerability Scan:

After reconnaissance, attackers often probe identified services for vulnerabilities. This scenario simulates targeted probing of HTTPS services, reflected by increased HTTPS feature representation, moderate traffic rates, and high packet size variability. The flow structure resembles application-layer interaction rather than simple port probing.

5) MQTT Denial-of-Service (DoS):

The final scenario represents a service disruption attack targeting MQTT-based IoMT communication. This flow is characterized by very high transmission rates, extremely low inter-arrival times, and sustained TCP activity, consistent with flooding behavior aimed at overwhelming IoMT messaging services.

A representative benign network flow was selected as a template to ensure that unmodified features (like Protocol Type or LLC) retained statistically plausible values for a medical device environment.

All unmodified features retained their original benign values to ensure that each attack scenario deviates only in behaviorally meaningful dimensions rather than becoming statistically unrealistic.

Attack Scenario	**Key Feature Modifications**	**Adversarial Behavior**
Slow TCP Port Scan	High Syn_flag_number (0.84), moderate IAT (0.45s)	Mimics stealthy reconnaissance that avoids rate-limiting alerts.
Aggressive Scan	Extremely high Rate (18,500), near-zero IAT (0.00004)	Represents high-speed "noise" scanning for rapid discovery.
Evasive Scan	High ack_flag_number(0.92) and psh_flag_number (0.40)	Blends with legitimate data exchange to bypass simple SYN filters.
MQTT DoS	High Rate (7,363), low IAT (0.000136), high flag variability	Simulates service exhaustion targeting messaging protocols.

E. Evaluation Strategy

This study evaluates model behavior using a score-based comparative analysis rather than relying solely on binary classification accuracy. Each anomaly detection model produces a continuous anomaly score which indicates the degree of deviation of that malicious network flow from learned normal IoMT traffic patterns.

After training on benign traffic, the five constructed attack scenarios were individually introduced to each model. For every scenario, the following aspects were analyzed:

Anomaly Score Magnitude:

The raw anomaly score assigned by each model was examined to determine how strongly the model perceived the attack flow as abnormal.

Relative Sensitivity Across Attack Types:

Score differences were compared across the five attack scenarios to observe how each model responds to varying attack behaviors, including slow scans, aggressive scans, evasive scans, vulnerability probing, and denial-of-service activity.

Paradigm-Based Detection Behavior:

Differences in scoring trends were interpreted in the context of each model's underlying principle — isolation (Isolation Forest), boundary deviation (One-Class SVM), and local density variation (Local Outlier Factor).

Although binary anomaly labels were recorded, the primary focus of this study is on how anomaly scores vary across models and attack types which reveals differences in detection sensitivity that are not visible through accuracy metrics alone.

IV. RESULTS

1. Global Performance Metrics:

The performance of the three unsupervised anomaly detection paradigms was evaluated using the malicious test subsets of the CICIoMT2024 dataset. Four key metrics were observed for this evaluation: Precision, Recall, F1-Score, and ROC-AUC. These metrics show the model's ability to differentiate between benign medical device traffic and malicious attack flows. The comparative results for Port Scan, Vulnerability Scan, and MQTT DoS attacks are presented in table 1.

Table 1. Global Performance Metrics

Attack Type	Model	Precision	Recall	F1-Score	ROC-AUC
Port Scan	OC-SVM	0.988	1.000	0.994	0.999
	IF	0.978	0.995	0.986	0.929
	LOF	0.967	1.000	0.983	0.998
Vulnerability	OC-SVM	0.797	1.000	0.887	0.999
	LOF	0.573	1.000	0.729	0.999
	IF	0.604	0.750	0.669	0.917
MQTT DoS	OC-SVM	0.922	1.000	0.960	0.999
	IF	0.860	0.999	0.925	0.983
	LOF	0.803	1.000	0.891	1.000

Based on the metrics in Table 1, the One-Class SVM (OC-SVM) emerged as the most robust model for IoMT anomaly detection. While all three models had high recall indicating that almost no attacks were missed, the OC-SVM provided relatively better precision. This is particularly evident in the Vulnerability Scan results, where OC-SVM achieved an F1-score of 0.8868, significantly higher than the other two models. This suggests that the boundary-based models provide relatively better metrics compared to Tree-based or density-based models.

2. Targeted Attack Sensitivity:

A. Isolation Forest

The Isolation Forest model successfully detected the Slow Scan, Aggressive Scan, and MQTT DoS scenarios with strong anomaly scores, indicating that these attacks produce feature values sufficiently distinct from benign IoMT traffic. The Evasive Scan was detected with a much weaker anomaly signal, suggesting that stealthy attacks blending with normal traffic may partially evade detection. Notably, the Vulnerability Scan scenario was classified as normal; the combination of features in this attack did not isolate the flow points quickly enough in the IF model's partitioning space to be considered anomalous, reflecting a limitation of feature-based isolation for subtle application-layer attacks. Table 2 shows the anomaly score and the binary classification.

Table 2. Isolation Forest Metrics

Attack Scenario	**Prediction**	**Anomaly Score**
Slow Scan	Anomaly	-0.114
Aggressive Scan	Anomaly	-0.101
Evasive Scan	Anomaly	-0.018
Vulnerability Scan	Normal	0.021
MQTT DoS	Anomaly	-0.100

Sensitivity Analysis (Isolation Forest)

High sensitivity:

a) Slow Scan (-0.114)

b) Aggressive Scan (-0.101)

c) MQTT DoS (-0.100)

The model reacts strongly even to subtle port scanning (Slow Scan), showing that IF is sensitive to deviations in low-level flow features such as SYN/RST counts and inter-arrival times.

Moderate sensitivity:

a) Evasive Scan (-0.018)

Isolation Forest can detect stealthy scanning, but the weak signal indicates that subtle deviations are harder to pick up.

Low sensitivity:

a) Vulnerability Scan (0.021)

Isolation Forest fails to isolate flows with subtle application-layer changes, demonstrating a limitation in detecting post-reconnaissance attacks.

B. One-Class Support Vector Machine (OC-SVM)

The OC-SVM model successfully detected all five attack scenarios as anomalous, demonstrating its robustness in identifying deviations from benign IoMT traffic. However, the anomaly scores for most attacks (Slow Scan, Aggressive Scan, MQTT DoS, Vulnerability Scan) are nearly identical, indicating score saturation once flows cross the model's boundary. The Evasive Scan receives a slightly lower score (-4.660), but it is still clearly flagged as anomalous.

This behavior reflects the boundary-based nature of OC-SVM, where points far outside the learned support are assigned maximum deviation scores, reducing differentiation between attack types. Table 3 shows the binary classification and the anomaly score of OC-SVM.

Table 3. OC-SVM Metrics

Attack Scenario	**Prediction**	**Anomaly Score**

Attack Scenario	**Prediction**	**Anomaly Score**
Slow Scan	Anomaly	-5.049
Aggressive Scan	Anomaly	-5.049
Evasive Scan	Anomaly	-4.660
Vulnerability Scan	Anomaly	-5.044
MQTT DoS	Anomaly	-5.049

Sensitivity Analysis (OC-SVM)

High sensitivity:

a) Slow Scan, Aggressive Scan, MQTT DoS → strongly flagged with saturated scores (-5.049)

These attacks clearly cross the model's boundary and are reliably detected. However ,they are saturated and do not represent the actual anomaly score of each attack.

Moderate sensitivity:

a) Vulnerability Scan (-5.044)

Score saturation hides the relative strength of the anomaly; OC-SVM still detects it but cannot distinguish it from other high-severity attacks.

Low differentiation *:*

b) Evasive Scan (-4.660)

Slightly lower score, but boundary-based saturation limits the model's ability to rank the severity of attacks, reducing its usefulness for incident triaging.

C. Local Outlier Factor (LOF)

The Local Outlier Factor model exhibits highly variable anomaly score behavior across attack scenarios due to its density-based nature. The Aggressive Scan is assigned an extremely large negative anomaly score (-72.915), indicating that this flow lies in a region of exceptionally low local density compared to its neighbors. The Slow Scan (-6.687) and MQTT DoS (-1.732) are also detected as anomalous, but with progressively weaker anomaly strength. In contrast, both the Evasive Scan and Vulnerability Scan are classified as normal, with positive scores indicating that their local densities are comparable to surrounding benign flows. This suggests that when malicious traffic closely resembles normal IoMT communication patterns in local feature space, LOF may fail to identify it as anomalous. Table 4 shows the anomaly score and the binary classification of LOF.

Table 4. LOF Metrics

Attack Scenario	**Prediction**	**Anomaly Score**
Slow Scan	Anomaly	-6.687
Aggressive Scan	Anomaly	-72.915
Evasive Scan	Normal	0.430

Attack Scenario	Prediction	Anomaly Score
Vulnerability Scan	Normal	0.435
MQTT DoS	Anomaly	-1.732

Sensitivity Analysis (LOF)

Very high sensitivity (extreme density deviation):

a) Aggressive Scan → very strong anomaly score (-72.915)

LOF reacts strongly when a flow's local density is drastically lower than that of neighboring benign flows, resulting in an extreme outlier score.

Moderate sensitivity:

a) Slow Scan (-6.687)

b) MQTT DoS (-1.732)

These attacks deviate from normal traffic but still retain partial similarity to nearby benign points, producing weaker anomaly signals. The difference between the Slow Scan and MQTT DoS scores suggests that LOF's anomaly strength is highly dependent on how the training data shapes local density regions in feature space.

Low sensitivity:

a) Evasive Scan (0.430)

b) Vulnerability Scan (0.435)

These flows maintain local density characteristics similar to benign IoMT traffic, causing LOF to misclassify them as normal. This highlights LOF's limitation when malicious behavior remains locally consistent with normal communication patterns.

V. DISCUSSION

This study presents an empirical analysis of three unsupervised anomaly detection models — Isolation Forest (IF), One-Class SVM (OC-SVM), and Local Outlier Factor (LOF) — across multiple IoMT attack scenarios to understand how different anomaly detection paradigms interpret malicious network behavior.

Model Behavior Differences

The results demonstrate that anomaly detection performance strongly depends on how each model defines "abnormality."

Isolation Forest (IF) isolates anomalies based on how quickly feature values can be separated in random partitions. This made IF particularly effective at detecting reconnaissance-based attacks such as slow and aggressive port scans, where deviations appear in low-level traffic features like flag counts, packet timing, and connection statistics. However, IF failed to detect the Vulnerability Scan, suggesting that attacks which closely resemble legitimate application-layer communication may not be isolated efficiently in tree-based partitioning.

One-Class SVM (OC-SVM) models a boundary around normal traffic in high-dimensional space. It successfully classified all attack scenarios as anomalous, indicating strong sensitivity. However, the anomaly scores were highly similar across different attacks, demonstrating score saturation once samples lie far outside the learned boundary. This limits OC-SVM's usefulness for incident prioritization, as it cannot clearly distinguish between moderately suspicious and highly disruptive attacks.

Local Outlier Factor (LOF) evaluates anomalies based on local density deviation of a feature. It produced the most extreme score for the Aggressive Scan, indicating that this attack significantly disrupted local density structure. However, LOF misclassified both Evasive Scan and Vulnerability Scan as normal because their feature patterns remained locally consistent with benign traffic. This shows that LOF is effective at detecting high-contrast traffic deviations but struggles with stealthy or protocol-compliant malicious behavior.

No single model performed best across all categories:

Attack Type	**IF**	**OC-SVM**	**LOF**	**Key Insight**
Slow Scan	Strong	Strong	Moderate	Feature deviation detectable globally and locally
Aggressive Scan	Strong	Strong	Very Strong	Large structural deviation in traffic
Evasive Scan	Weak	Strong	Missed	Stealthy behavior evades density-based detection
Vulnerability Scan	Missed	Strong	Missed	Protocol-compliant malicious behavior is hard to isolate
MQTT DoS	Strong	Strong	Moderate	Volume-based attacks detectable by most models

This highlights that model diversity is necessary in IoMT environments, where attacks vary from subtle reconnaissance to volumetric disruption.

Operational Implications for IoMT Security:

From a healthcare network perspective:

a) Isolation Forest is well-suited for early-stage reconnaissance detection, helping identify probing before exploitation.

b) OC-SVM is useful as a broad anomaly alarm system, but not ideal for ranking incident severity.

c) LOF can highlight extreme traffic disruptions, making it valuable for detecting aggressive or high-impact attacks.

However, all models struggled with stealthy application-layer attacks, suggesting that flow-level statistical features alone may be insufficient. Integrating protocol-aware features or deep packet inspection could improve detection of vulnerability exploitation attempt.

VI. CONCLUSION

This work evaluated how different unsupervised anomaly detection models respond to diverse IoMT attack behaviors using the CICIoMT2024 dataset. The results indicate that detection performance highly depends on the type of abnormality found in the network flow and model assumptions. Isolation Forest was most effective at identifying reconnaissance-style traffic, One-Class SVM showed high overall sensitivity but limited score interpretability, and Local Outlier Factor excelled at detecting highly disruptive traffic while missing stealthier activity.

These findings show that a single anomaly detection technique cannot reliably detect all forms of malicious behavior in heterogeneous IoMT environments. Subtle application-layer attacks that closely resemble normal communication remain particularly challenging for flow-based models.

Future research should focus on hybrid detection strategies and richer behavioral features to improve coverage of stealthy post-reconnaissance attacks in healthcare networks.

Editing Assistance**:** The author used language editing tools to improve grammar and readability. All experiments were conducted by the author and the author takes full responsibility.

Declarations:

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable. This study utilized the publicly available CICIoMT2024 benchmark dataset. The research did not involve human participants or animal subjects, and all data was anonymized by the original creators to ensure privacy.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used in this study (CICIoMT2024) are publicly available through the Canadian Institute for Cybersecurity. The specific synthetic attack mappings and code developed for this analysis are available at https://github.com/Visvakaanth123/An-Empirical-analysis-of-anomaly-detection-model-paradigms-under-heterogeneous-iomt-attack-traffic.

Conflicts of Interest: The author declares no conflicts of interest.

REFERENCES

Sharma, H., Kumar, P., Shrivastava, G., Sharma, K., & Bhola, A. (2026). Using machine learning for protecting the security and privacy of Internet of Medical Things (IoMT) systems. *In* Integrating Cloud, Fog, and Edge Computing in Healthcare: Federated Learning and Blockchain Approaches. https://doi.org/10.1007/978-3-031-96265-3_9

Chandekar, P., Mehta, M., & Chandan, S. (2025). Enhanced anomaly detection in IoMT networks using ensemble AI models on the CICIoMT2024 dataset. *arXiv*. https://doi.org/10.48550/arXiv.2502.11854

Dadkhah, S., Neto, E. C. P., Arcoverde Neto, E. N., Ferreira, R., Molokwu, R. C., Sadeghi, S., Ghorbani, A. A., & Ghorbani, A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. *Internet of Things, 28,* 101351. https://doi.org/10.1016/j.iot.2024.101351

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. *2008 Eighth IEEE International Conference on Data Mining,* 413–422. https://doi.org/10.1109/ICDM.2008.17

Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the support of a high-dimensional distribution. *Neural Computation, 13*(7), 1443–1471. https://doi.org/10.1162/089976601750264965

Breunig, M. M., Kriegel, H.-P., Ng, R. T., & Sander, J. (2000). LOF: Identifying Density-Based Local Outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (pp. 93–104). ACM. https://doi.org/10.1145/335191.335388