

Isolation Forest-Based Anomaly Detection for Cloud-Native Banking IT Infrastructure: A Simulation-Oriented Study

Standalone study derived from the Isolation Forest component of the supplied main research paper

Dakshta Jain, Awanit Kumar, Sandeep Saxena
Career Point University

Abstract - Cloud-native banking platforms generate heterogeneous operational telemetry from applications, infrastructure components, distributed services, and observability pipelines. Detecting unusual behavior in such environments is difficult because operational anomalies may be sparse, diverse, and insufficiently labeled for conventional supervised learning. This paper isolates the Isolation Forest component described in a larger study of self-adaptive banking IT infrastructure and develops it as a standalone anomaly-detection research study. The proposed approach uses Isolation Forest as an unsupervised detector over incoming telemetry, where observations that can be separated from the majority with relatively short random-partition paths receive higher anomaly scores. The source study describes a controlled synthetic environment representing 30 days of banking activity across five service clusters and containing application and infrastructure logs, time-series metrics, distributed traces, injected faults, and simulated attack scenarios. That environment is used here as the experimental context, while the analysis deliberately excludes the source study's LSTM Autoencoder and other agentic components. A critical attribution issue is identified: the source paper reports its principal anomaly-detection metrics for a hybrid Isolation Forest plus LSTM Autoencoder pipeline. Consequently, its reported 96.3% precision, 94.8% recall, 95.5% F1-score, 97.1% accuracy, 2.7% false-positive rate, and 0.98 AUC-ROC cannot legitimately be presented as Isolation Forest-only results. The paper therefore provides a reproducible evaluation framework for standalone Isolation Forest and treats the hybrid measurements only as contextual evidence. The contribution is a focused methodology, an explicit validity boundary, and a simulation-oriented protocol for determining the independent value of Isolation Forest in banking IT anomaly detection.

Keywords - Isolation Forest, anomaly detection, cloud-native banking, AIOps, operational telemetry, unsupervised learning, IT infrastructure

1. INTRODUCTION

1.1 Background

Modern banking services increasingly depend on distributed applications, microservices, containerized components, cloud resources, and interconnected digital interfaces. These environments create operational visibility at a scale that is difficult to manage through manual observation alone. The source study describes a contemporary banking IT setting in which logs, metrics, traces, ... Anomaly detection therefore becomes an important analytical capability for identifying unusual system behavior early.

1.2 Cloud-Native Banking IT Infrastructure

The main study frames banking infrastructure around five service areas: core banking, payments, card switching, risk and compliance, and customer-facing APIs. The experimental environment is cloud-native and Kubernetes-based, with Prometheus and Grafana used for metrics, the ELK stack used for observability data, and OpenTelemetry used for distributed tracing. ... context is source-supported, whereas any claim about production deployment would go beyond the evidence.

1.3 Anomaly Detection Problem

An anomaly is an observation or operational state that differs materially from the behavior represented by the surrounding data. In IT operations, such deviations can correspond to unusual resource behavior, service failures, configuration problems, traffic abnormalities, or other operational events. A conventional rule-based monitor can detect conditions that ... it can identify unusual observations without requiring every abnormal pattern to be specified beforehand.

1.4 Motivation for Isolation Forest

Isolation Forest is especially relevant to the focused problem because it approaches anomaly detection through isolation rather than through an explicit model of normal behavior. The original method constructs random partitioning trees and exploits the observation that unusual points tend to be isolated with fewer partitions than ordinary ... before the broader hybrid anomaly pipeline is applied. This paper retains only that component.

1.5 Problem Statement

The focused research problem is the design of a standalone, source-grounded Isolation Forest anomaly-detection workflow for cloud-native banking IT telemetry. The challenge is not merely to describe the algorithm, but to define how the algorithm can be positioned within the telemetry environment reported by the source paper and ... belong to a hybrid pipeline, so direct attribution to Isolation Forest is not valid.

1.6 Research Objectives

The study has five objectives: (1) formulate a standalone Isolation Forest detector using the telemetry context available in the source paper; (2) explain the construction of random isolation trees, path-length scoring, and threshold-based identification; (3) define a simulation-oriented evaluation procedure using the source-supported banking workload and telemetry corpus; ... evaluation; and (5) identify practical limitations and future experiments for banking IT anomaly detection.

1.7 Research Questions

RQ1: How can Isolation Forest be formulated as a standalone anomaly detector for cloud-native banking IT telemetry? RQ2: Which telemetry streams and simulated scenarios described in the source paper can support its evaluation? RQ3: Which detection and responsiveness measures are appropriate for evaluating the detector? RQ4: What conclusions ... be drawn from the source study, and which conclusions require a new ablation experiment?

1.8 Contributions of the Study

The main contribution is methodological separation. Rather than treating the entire agentic architecture as the subject of analysis, the paper extracts one algorithmic component and develops a self-contained detection workflow around it. A second contribution is evidence

discipline: the paper explicitly identifies the source measurements that are hybrid ... a focused research study without claiming experimental evidence that the source does not provide.

2. RELATED WORK

2.1 Anomaly Detection in IT Infrastructure

IT operations generate continuous observations from applications, infrastructure, networks, and service dependencies. The source literature review describes the movement from conventional IT operations toward AIOps, where machine learning, analytics, automation, and observability are combined to improve operational decision-making. Anomaly detection is one of the central capabilities in this ... not by themselves establish the independent performance of the Isolation Forest component considered here.

2.2 Machine Learning-Based Anomaly Detection

Machine-learning anomaly detection can be organized around different assumptions about the data and the type of supervision available. Some approaches require labeled examples, while others model regular behavior or identify observations that are structurally unusual. The source paper situates its observability function within this broader AIOps setting and ... of every failure mode are relatively limited. This motivates examination of an unsupervised method.

2.3 Unsupervised Anomaly Detection

Unsupervised detection does not depend on assigning a class label to every training observation. Instead, the detector searches for observations that differ from the dominant structure of the available data. This is useful when the abnormal behavior is not fully enumerated in advance. It is also consistent with ... to determine whether those alerts correspond to known injected faults or other target events.

2.4 Isolation Forest

Liu, Ting, and Zhou introduced Isolation Forest as a method that explicitly isolates anomalies instead of first constructing a detailed profile of normal instances. The method relies on the observation that anomalies are relatively few and different, making them more susceptible to early isolation in randomly partitioned trees. ... work also emphasizes sub-sampling, computational efficiency, and applicability to large or high-dimensional data. Ncited0turn0search0Öturn0search24Ö

2.5 Research Gap

The source paper's observability methodology combines Isolation Forest with an LSTM Autoencoder. The Isolation Forest signal is intended to identify point-level outliers, while the second model captures temporal deviations through reconstruction error; the two are subsequently fused into a composite score. The source reports the performance of this ... Isolation Forest component independently and specify the experiment required to quantify its standalone behavior.

3. PROPOSED METHODOLOGY

3.1 Research Framework

The proposed study treats anomaly detection as a single-stage unsupervised classification-by-score problem. Operational telemetry is transformed into observations, the observations are presented to an ensemble of isolation trees, and each observation receives an anomaly score. A threshold derived from validation data is then used to convert the continuous ... reinforcement-learning policy, resource controller, or autonomous remediation mechanism is part of the proposed detector.

3.2 Isolation Forest-Based Detection Approach

Isolation Forest constructs multiple randomized binary trees. At each internal partition, an attribute is selected and a split value is chosen within the observed range of that attribute. Recursive partitioning continues until observations become isolated or a stopping condition is reached. The central intuition is that an unusual ... while a long path indicates that the observation remains embedded among many similar observations.

3.3 Input Telemetry

The source paper provides three directly relevant telemetry categories: application and infrastructure logs, time-series metrics, and distributed traces. It reports 2.4 million log entries, 850,000 metric data points, and 120,000 distributed traces in the simulation corpus. The paper does not specify the exact feature schema extracted from each ... the source: telemetry samples are converted into numerical observations suitable for Isolation Forest scoring.

3.4 Data Preprocessing

The source paper does not provide a detailed standalone preprocessing recipe for the Isolation Forest input. It does state that the detector computes a score for each incoming metric window and that the anomaly score is compared with a validation-tuned threshold. It also states that parameters were tuned ... that the standalone result can be reproduced and separated from the hybrid source experiment.

3.5 Feature Representation

For Isolation Forest, each telemetry observation must be represented as a feature vector. The source supports the use of metric-window observations and broader telemetry streams but does not specify a complete feature dictionary. A defensible implementation should therefore preserve the semantics of the source data while documenting the ... an implementation choice from being mistaken for a fact reported by the original study.

3.6 Isolation Forest Construction

Let X denote the collection of telemetry observations and let ψ denote the subsample size used to construct an isolation tree. An isolation tree recursively partitions a subsample using randomly selected attributes and split points. A forest is formed by repeating this process across multiple independently randomized trees. ... are expected to be isolated quickly, unusually short paths produce higher evidence of anomalousness.

3.7 Anomaly Score Calculation

The source paper gives the following normalized Isolation Forest score, adapted from Liu, Ting, and Zhou:

$$s(x, n) = 2^{-(\lceil -E[h(x)] / c(n) \rceil)}$$

where $E[h(x)]$ is the mean path length of observation x across the trees and $c(n)$ is the expected path length used to normalize the result for the relevant subsample size. The source explains that this normalization places the score in the interval $[0,1]$. A score closer to the ... paths. This formulation is the only algorithmic scoring equation retained from the source methodology.

3.8 Threshold-Based Anomaly Identification

The source states that the detector flags a telemetry window as a candidate anomaly when its Isolation Forest score exceeds a validation-tuned threshold. This is important because an anomaly score is not, by itself, a final binary decision. The threshold determines how sensitive the detector is to unusual ... source does not specify the numerical threshold, so this paper does not invent one.

3.9 Detection Workflow

The focused workflow contains seven conceptual stages: telemetry acquisition; observation construction; Isolation Forest training on the available baseline data; score generation; threshold application; event-to-label alignment for evaluation; and metric calculation. The source paper's broader environment provides the telemetry and controlled fault/attack events, while the proposed standalone workflow stops ... not pass the result to another agent or use the alert to trigger remediation.

3.10 Computational Considerations

Isolation Forest was selected in the source as a lightweight, unsupervised screening mechanism. The original Isolation Forest literature emphasizes that the method can use sub-sampling and achieve favorable computational characteristics compared with several distance- and density-based alternatives. This property is relevant to operational telemetry because the detector may ... standalone experiment, while recognizing that these measurements are not provided by the source paper.



Fig. 1. Conceptual Isolation Forest anomaly-detection workflow proposed for the focused study.

4. DATASET AND EXPERIMENTAL CONTEXT

4.1 Synthetic Banking Workload

The source study uses a synthetic workload generator because production banking telemetry is not available for open experimentation. The generator emulates 30 days of continuous operation across five service clusters and incorporates realistic transaction volumes, seasonal traffic patterns, and controlled fault and attack scenarios. This makes the corpus ... that the paper does not reinterpret the synthetic workload as real banking production data.

4.2 Telemetry Sources

The reported corpus contains 2.4 million application and infrastructure log entries, 850,000 metric data points, and 120,000 distributed traces. The source associates these streams with the ELK stack, Prometheus/Grafana time-series exporters, and OpenTelemetry instrumentation, respectively. These values are directly reported in the source and can be used to ... directly used by Isolation Forest, because the source does not specify such a mapping.

4.3 Service Environment

Five service clusters are represented: core banking, payments, card switch, risk and compliance, and customer API. This distribution is useful for an anomaly-detection study because operational behavior can differ between transaction-processing services, switching infrastructure, compliance functions, and customer-facing interfaces. The service names are used here only to describe ... context, not to imply that Isolation Forest was independently validated for each service category.

4.4 Fault and Anomaly Scenarios

The source reports 3,200 injected fault scenarios generated through a chaos-engineering fault injector and 1,150 simulated attack scenarios produced by an adversarial traffic and credential-abuse generator. The experimental setup also identifies node failures, service crashes, configuration drift, traffic spikes, and dependency outages as controlled fault conditions. These events ... breakdown by scenario, so no such breakdown is presented as an existing result here.

4.5 Simulation Environment

The broader testbed was deployed on Kubernetes with autoscaling enabled and instrumented with Prometheus, Grafana, the ELK stack, and OpenTelemetry. Chaos engineering was used to reproduce controlled failure conditions. The original study repeated each experiment across five independent runs of the 30-day simulated window and reported mean results. ... replacement is a proposed experimental separation, not a result already performed in the source.

4.6 Experimental Procedure

A valid standalone experiment should preserve identical workload instances across the detector and comparison conditions so that the only methodological difference is the anomaly-detection component. The baseline training portion should contain the source-supported normal operational period, the Isolation Forest should be trained without anomaly labels, and a held-out ... those values must be established and reported in a new experiment rather than inferred.

5. EVALUATION FRAMEWORK

5.1 Evaluation Metrics

The source paper groups detection-quality measures into precision, recall, F1-score, accuracy, false-positive rate, and AUC-ROC, and it also defines mean time to detect for operational responsiveness. These measures are suitable for the focused study because anomaly detection has two competing risks: missing abnormal events and generating excessive false alarms. A useful detector must balance both.

5.2 Precision

Precision measures the proportion of detected anomaly events that correspond to true anomaly events. With TP representing true positives and FP representing false positives, precision is $P = TP/(TP+FP)$. High precision is operationally valuable because each unnecessary alert can consume analyst attention and reduce confidence in the monitoring ... banking operations, where alert volumes may be high, controlling false alarms is particularly important.

5.3 Recall

Recall measures the proportion of relevant anomaly events that are detected. With FN representing false negatives, recall is $R = TP/(TP+FN)$. A low recall means that important abnormal events are missed. For infrastructure monitoring, recall is therefore necessary to determine whether a detector identifies the fault scenarios that are actually present in the evaluation corpus.

5.4 F1-Score

F1-score combines precision and recall through their harmonic mean: $F1 = 2PR/(P+R)$. It is useful when the evaluation requires a single summary of the trade-off between false alarms and missed events. However, the focused paper emphasizes that any F1 value must be calculated from Isolation Forest-only predictions if it is to be described as an Isolation Forest result.

5.5 Accuracy

Accuracy is the proportion of all observations that are correctly classified: $Acc = (TP+TN)/(TP+TN+FP+FN)$. It is easy to interpret, but anomaly datasets may contain many more normal observations than abnormal ones. Consequently, accuracy should not be reported in isolation. Precision, recall, F1-score, and false-positive rate provide additional information about the behavior of the detector on the minority anomaly class.

5.6 False Positive Rate

False-positive rate is $FPR = FP/(FP+TN)$. It quantifies the proportion of normal observations that are incorrectly flagged. This metric is particularly relevant for an unsupervised detector because the decision threshold controls alert sensitivity. A threshold that is too permissive can increase recall while producing an operationally impractical number of false alarms.

5.7 AUC-ROC

AUC-ROC summarizes discrimination across a range of decision thresholds by measuring the relationship between true-positive and false-positive rates. It is useful when the final alert threshold has not yet been fixed or when alternative sensitivity settings need to be compared. The source paper reports AUC-ROC as part of ... belongs to the hybrid anomaly-detection pipeline and is not a standalone Isolation Forest measurement.

5.8 Detection Time

The source defines mean time to detect as the average interval between event onset and detection. For N incidents, MTTD can be represented as $MTTD = (1/N) \sum (t_{detect,i} - t_{onset,i})$. In an Isolation Forest study, this measure connects statistical detection quality with operational usefulness. A detector that identifies ... but only after a long delay may have limited value for time-sensitive infrastructure incidents.

6. RESULTS AND ANALYSIS

6.1 What the Source Study Actually Reports

The original paper reports anomaly-detection performance for the Observability Agent's hybrid Isolation Forest and LSTM Autoencoder pipeline. The reported table gives 96.3% precision, 94.8% recall, 95.5% F1-score, 97.1% accuracy, 2.7% false-positive rate, and 0.98 AUC-ROC for the proposed ecosystem condition. The source explicitly states that the Observability Agent ... detector, but they are not valid evidence for the standalone performance of Isolation Forest.

6.2 Attribution Boundary

The distinction between component-level and pipeline-level evidence is central to this paper. If two detectors contribute to a final decision, the performance of that decision reflects their combined behavior. Removing one component can change the score distribution, threshold, false-positive behavior, and detection coverage. It is therefore methodologically incorrect ... the LSTM Autoencoder is removed. The independent contribution of Isolation Forest consequently remains unresolved.

6.3 Contextual Interpretation of the Hybrid Results

The hybrid results nevertheless establish that an Isolation Forest signal was successfully incorporated into an operational anomaly-detection pipeline in the controlled simulation. The source reports that the Isolation Forest component was used for lightweight, unsupervised outlier screening and that its score was fused with the LSTM reconstruction signal. ... a standalone experiment, but it should not be presented as an Isolation Forest benchmark.

6.4 Results Required for Standalone Evaluation

To establish Isolation Forest-only performance, the experiment must repeat the same relevant workload and evaluation conditions while removing the LSTM Autoencoder and composite-score fusion. The detector would produce $s(x,n)$ directly, apply its independently selected validation threshold, and generate anomaly decisions. Those decisions could then be compared against the ... pipeline would reveal the incremental value of the temporal model without misattributing its contribution.

6.5 Non-Results and Reporting Discipline

No numerical Isolation Forest-only result is reported in this paper because none is available in the source. In particular, the manuscript does not claim that Isolation Forest achieved 95.5% F1-score, 96.3% precision, 94.8% recall, 97.1% accuracy, 2.7% false-positive rate, or 0.98 AUC-ROC. Those values belong to the hybrid ... essential for maintaining a valid academic distinction between source evidence and proposed future experimentation.

7. DISCUSSION

7.1 Interpretation

Isolation Forest is a natural candidate for an initial anomaly-screening layer because its decision principle does not require a complete catalog of abnormal patterns. In the source environment, where telemetry arrives from multiple service clusters and controlled events can be injected, the method can provide a score that ... makes it easier to separate the detection mechanism from later response or orchestration functions.

7.2 Advantages of Isolation Forest

The principal advantages relevant to this setting are unsupervised operation, a tree-based isolation mechanism, use of sub-sampling, and relatively favorable computational characteristics reported in the original algorithm literature. Isolation Forest does not depend on distance or density calculations in the same manner as several alternative outlier methods. Its ... operational telemetry streams, although actual performance depends on feature representation and workload characteristics.

7.3 Suitability for Banking IT Telemetry

Banking infrastructure produces a mixture of normal operational states and comparatively infrequent unusual events. This setting is compatible with the basic isolation assumption that anomalies are uncommon and distinguishable from the majority. However, banking telemetry also contains legitimate workload changes, seasonal effects, and service-specific behavior. A naive global ... A future standalone study should examine threshold sensitivity across service types and workload periods.

7.4 Computational Efficiency

The original Isolation Forest literature emphasizes low computational overhead, linear-time behavior under its formulation, and the benefits of sub-sampling. These properties are attractive for operational monitoring, where the detector may need to score large telemetry volumes. The source simulation contains millions of logs and hundreds of thousands of ... not provide an isolated benchmark. Such a measurement should be included in future experimentation.

7.5 Practical Deployment Considerations

A practical deployment would need a carefully defined observation window, feature construction policy, threshold-management procedure, and mechanism for correlating anomaly alerts with operational events. These details should be documented because they can materially affect detector behavior. The source paper's validation-tuned threshold provides a methodological starting point, but the ... an autonomous remediation mechanism; response actions are outside the scope of this focused study.

7.6 Comparison with Conventional Monitoring

The source paper compares its broader observability pipeline with rule-based monitoring and a standalone AIOps configuration. For the focused Isolation Forest study, the appropriate comparison is narrower: a rule-based anomaly monitor versus Isolation Forest under identical workloads and event labels. Such a comparison would determine whether unsupervised isolation ... this comparison for Isolation Forest alone, no new numerical superiority claim is made here.

7.7 Limitations

The first limitation is source attribution: the available anomaly results are hybrid. The second is the synthetic nature of the workload. The third is the incomplete specification of feature engineering and threshold values for a standalone detector. The fourth is that the source paper's architecture contains other components ... rare legitimate events may be flagged if they are sufficiently isolated in feature space.

8. THREATS TO VALIDITY

8.1 Synthetic-Data Threat

The simulation is intentionally controlled and cannot reproduce every property of production banking telemetry. The source itself cautions that production environments contain regulatory, concurrency, and adversarial conditions that a testbed can only approximate. Results from the simulation should therefore be interpreted as evidence about a controlled experimental setting rather than direct evidence of production performance.

8.2 Attribution Threat

The largest internal-validity threat is that the source's anomaly results come from a fused Isolation Forest plus LSTM Autoencoder pipeline. Any attempt to treat those results as an Isolation Forest-only benchmark would confound two methodological contributions. This paper addresses the threat by refusing to make standalone numerical claims and by specifying the ablation experiment required for valid attribution.

8.3 Generalization Threat

The five simulated service clusters provide useful diversity, but they do not represent every banking platform, workload profile, or operational environment. The same detector could behave differently when feature distributions change, when services have different baselines, or when anomalies are subtle rather than strongly isolated. Cross-environment validation is therefore required before generalizing the method.

8.4 Measurement and Labeling Threat

Anomaly metrics require a definition of what counts as a positive event. The source provides injected faults and attack scenarios, but it does not publish a complete Isolation Forest-specific labeling protocol. Event-window alignment, duplicate alerts, and duration of anomaly conditions can affect precision, recall, and detection time. A standalone experiment should document these decisions before evaluation.

9. CONCLUSION AND FUTURE WORK

9.1 Conclusion

This paper has separated the Isolation Forest component from a larger study of self-adaptive banking IT infrastructure and developed it as a standalone anomaly-detection methodology. The approach uses random isolation trees, average path length, normalized anomaly scoring, and a validation-tuned threshold to identify unusual telemetry observations. The source ... activity across five service clusters, with logs, metrics, traces, injected faults, and simulated attacks.

The most important conclusion is methodological rather than numerical. The source study demonstrates a hybrid anomaly-detection pipeline, not a standalone Isolation Forest benchmark. Its reported detection values therefore cannot be assigned exclusively to Isolation

Forest. A scientifically valid standalone result requires removing the LSTM Autoencoder, generating decisions from ... for that experiment while preserving a clear boundary between evidence and proposed future work.

9.2 Future Work

Future work should conduct an explicit Isolation Forest ablation using the source simulation corpus, publish the exact feature representation and threshold-selection procedure, and report per-service and per-scenario performance. Additional experiments could compare the standalone detector with the hybrid pipeline, evaluate threshold stability under changing workloads, measure throughput and ... detector or is best used as one component of a more comprehensive anomaly-detection system.

REFERENCES

- [1] Dakhsta Jain Research Paper Update 1(1), "Intelligent Agentic AI Ecosystem for Self-Adaptive Banking IT Infrastructure: Autonomous Observability, Predictive Security, Dynamic Resource Orchestration, and Continuous Resilience Engineering," supplied main research paper, 2026.
- [2] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proc. 2008 Eighth IEEE International Conference on Data Mining, 2008, pp. 413–422, doi: 10.1109/ICDM.2008.17.
- [3] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," ACM Transactions on Knowledge Discovery from Data, vol. 6, no. 1, 2012, Art. no. 3.
- [4] M. Joy, S. Venkataramanan, M. Ahmed, M. Mark, L. Gudala, M. Shaik, A. K. Pamidi Venkata, and V. K. R. Vangoor, "AIOps in Action: Streamlining IT Operations through Artificial Intelligence," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 23s, 2024, pp. 2175–2185.
- [5] D. K. D. Pal, V. R. R. Alluri, S. Thota, V. S. M. Bonam, S. Chitta, and M. Shaik, "AIOps: Integrating AI and Machine Learning into IT Operations," Australian Journal of Machine Learning Research & Applications, vol. 4, no. 1, 2024, pp. 288–311.
- [6] N. Y. Mulongo, "Key performance indicators of artificial intelligence for IT operations (AIOps)," in 2024 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2024, pp. 1–8.
- [7] B. Gregg, Systems Performance: Enterprise and the Cloud. Pearson Education, 2014.
- [8] D. Gairola, "Autonomous AIOps Framework for Predictive Incident Management in Large-Scale Enterprise Systems," International Journal of Artificial Intelligence and Machine Learning, vol. 6, no. 5s, 2026, pp. 103–116.
- [9] M. A. R. Banu, "Autonomous Cloud Operations: Integrating AI for Reliability and Scalable System Performance," International Journal of Technology, Management and Humanities, vol. 12, no. 01, 2026, pp. 92–99.

SOURCE-CONTROLLED TABLES

Table 1. Simulation context reported by the source paper

Data category	Volume	Source / generation
Logs	2.4 million	ELK stack
Metrics	850,000	Prometheus/Grafana
Traces	120,000	OpenTelemetry
Injected faults	3,200	Chaos-engineering injector
Simulated attacks	1,150	Adversarial traffic / credential-abuse generator
Service clusters	5	Core banking; payments; card switch; risk & compliance; customer API

Table 2. Detection results and attribution boundary

Measure	Source reports	Standalone IF
Precision	96.3% (hybrid)	Not available
Recall	94.8% (hybrid)	Not available
F1-score	95.5% (hybrid)	Not available
Accuracy	97.1% (hybrid)	Not available
FPR	2.7% (hybrid)	Not available
AUC-ROC	0.98 (hybrid)	Not available