Transactions on Computational and Scientific Methods | Vol. 4, No. 09, 2024
ISSN: 2998-8780
https://pspress.org/index.php/tcsm
Pinnacle Science Press

Data-Driven Failure Perception for Distributed Systems through Operational State Representation Learning

Wenyou Huang[1], Ryan Zhan[2], Zhibin Huang[3]
[1]Stevens Institute of Technology, Hoboken, USA
[2]University of Alabama, Tuscaloosa, USA
[3]Boston University, Boston, USA
*Corresponding author: Zhibin Huang; huangzhb7@gmail.com

Abstract: Distributed systems play a critical supporting role in cloud computing and large-scale information infrastructures. Their operating environments are complex, the node scale is large, and system states change frequently. As a result, system failures often exhibit strong concealment, complex propagation paths, and wide impact ranges. To address the limitations of traditional failure detection methods that rely on manual rules and adapt poorly to dynamic environments, this paper focuses on distributed system failure perception and proposes a unified data-driven modeling approach. The method starts from multi-node operational data and constructs a holistic representation of system states. Normal behavior patterns are learned from operational modes, and the degree of state deviation is used as the basis for failure perception. This enables automatic identification of complex system operating conditions. During modeling, both temporal evolution and global consistency of system states are considered. The model can therefore form stable state representations under multi-node parallel execution and strong coupling. Comparative experiments on a publicly distributed system dataset demonstrate strong overall performance across multiple evaluation metrics. The results confirm the effectiveness and practical value of data-driven modeling for distributed system failure perception. This study provides a feasible technical solution for intelligent monitoring and system state awareness in complex distributed environments.

Keywords: Distributed systems; fault perception; data-driven modeling; operational state representation

1. Introduction

Deep With the rapid development of cloud computing, edge computing, and large-scale data centers, distributed systems have become the core infrastructure supporting modern information services and critical business operations. Such systems usually consist of a large number of heterogeneous nodes, complex network connections, and multi-layer service components [1]. They exhibit large scale, high structural complexity, and dynamically changing operating environments. In real-world operation, factors such as hardware aging, resource contention, configuration inconsistency, and workload fluctuation can trigger various types of system failures. These failures are often highly hidden, have complex propagation paths, and tend to expand their impact scope. Once key nodes or services become abnormal, service quality may degrade, business processes may be interrupted, and even cascading system-level failures may occur. This poses serious challenges to system reliability and availability. As a result, timely perception and accurate identification of failures in complex environments have become critical issues in distributed systems research [2].

Conventional failure detection and diagnosis methods in distributed systems mainly rely on predefined rules, threshold-based judgments, or manually designed experience-driven models. Such approaches can be effective

in small-scale systems with relatively stable operating patterns [3]. However, as system architectures evolve and workloads change continuously, fixed rules and static thresholds struggle to adapt to diverse and dynamic states. This often leads to false alarms or missed detections. In addition, manually engineered features and diagnostic logic depend heavily on prior knowledge of internal system mechanisms. They show clear limitations when facing unknown failure patterns or cross-component correlated anomalies. These drawbacks significantly restrict the applicability and scalability of traditional methods in large-scale and dynamic distributed systems. They are insufficient for meeting the practical demands of stable operation and intelligent system management.

Against this background, data-driven models provide a new paradigm for distributed system failure perception [4]. With the continuous improvement of monitoring technologies, distributed systems can generate large volumes of multi-source data during operation. These data include performance metrics, log records, call relationships, and state changes. They contain rich information about system behavior and potential abnormal patterns. Data-driven approaches model historical and real-time data to automatically learn normal system behavior without relying on explicit rules. They can detect deviations from learned patterns. This helps overcome the limitations of manual modeling. It also enables stronger adaptability and generalization capability. Such methods offer important support for fine-grained characterization of complex system states.

Furthermore, failures in distributed systems are rarely isolated events. They are closely related to structural dependencies, resource coordination mechanisms, and temporal evolution processes. Data-driven models can explicitly exploit correlations among system components and capture dynamic state evolution during modeling. This allows failures to be analyzed from a global perspective [5]. Potential propagation patterns and impact scopes can be characterized more effectively. Perception methods based on overall data distributions and structural features help identify latent failures and early-stage anomalies. This improves the completeness and accuracy of system state awareness. Through continuous learning from operational data, models can gradually adapt to system scaling and business changes. This provides sustained support for long-term stable operation.

In summary, research on data-driven failure perception algorithms for distributed systems has significant theoretical and practical value. On the theoretical side, it deepens the understanding of complex system operation mechanisms and abnormal behavior characteristics [6]. It also promotes the transition from rule-driven to model-driven failure perception. On the practical side, the resulting techniques provide key support for building intelligent operation and maintenance frameworks. They enhance system reliability, stability, and operational efficiency. In application scenarios such as cloud services, critical infrastructures, and large-scale information systems, efficient data-driven failure perception will become a fundamental capability for ensuring safe operation. It will play an important role in advancing distributed systems toward greater intelligence and automation [7].

2. Proposed Framework

This study starts with the operational data of a distributed system, representing the system's state within a given time window as a vector form to characterize the overall operational features under multiple nodes and multiple indicators. Let the original observation data of the system at time t be represented as:

$$x_t = \{x_t^{(1)}, \ldots, x_t^{(d)}\}$$

Each dimension corresponds to a different node or resource indicator. To reduce noise interference and enhance learnability, the original state is first transformed using a mapping function to obtain the latent state representation.

$$z_t = f(x_t)$$

This representation integrates multi-source operational information of the system in a unified space, providing a basic description for subsequent state modeling and anomaly detection. This paper also presents the overall model architecture, as shown in Figure 1.

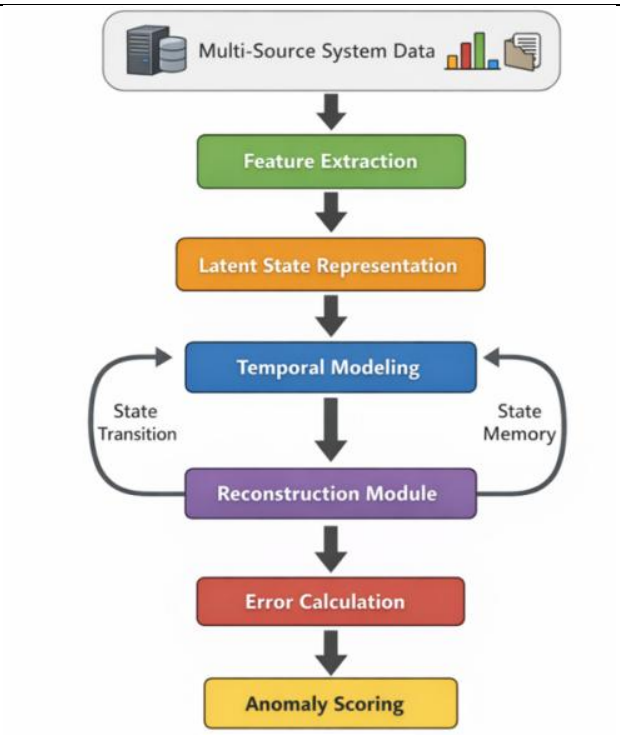


Figure 1. Overall model architecture

Considering the significant time-dependent nature of the operating state of a distributed system, the method further models the state evolution process. By introducing a state transition function to characterize the dynamic relationship between adjacent time steps, the system state update can be formalized as:

$$z_{t+1} = g(z_t)$$

This modeling approach reflects the stable evolution trend of the system under normal operating conditions, thus providing a reference for identifying anomalous deviations. By continuously characterizing the trajectory of state changes, the model can capture potential anomaly accumulation and abrupt changes over time, achieving a holistic understanding of the system's dynamic operation.

Based on this, the method characterizes the system's normal behavior patterns by constructing a state reconstruction mechanism. Given a latent state representation, a corresponding reconstructed state is generated using a decoding function:

$$\hat{x}_t = h(z_t)$$

The reconstruction error is used to measure the deviation between the current observation and the normal model, and its basic form is defined as:

$$e_t = \|x_t - \hat{x}_t\|_2$$

This error reflects the degree of deviation of the system's operating state from the existing pattern, providing direct quantitative evidence for fault detection.

To achieve stable fault detection and judgment, the method further introduces a normalized anomaly scoring function, which aims to eliminate the influence of scale differences and temporal fluctuations in reconstruction errors while enabling consistent evaluation across different operating conditions. By transforming raw reconstruction deviations into a unified and comparable space, the scoring mechanism facilitates reliable interpretation of system state deviations and supports continuous monitoring without reliance on manually

tuned thresholds. This normalization process enhances robustness against transient noise and gradual drift in system behavior, ensuring that anomaly assessments remain stable and comparable over time, defined as:

$$s_t = \frac{e_t - \mu_e}{\sigma_e}$$

Here, μ_e and σ_e represent the mean and standard deviation of the historical reconstruction error, respectively. This scoring mechanism enables continuous evaluation of the system's operational status without relying on manual rules, achieving automatic detection of potential faults. The overall approach, centered on data-driven modeling, provides a unified and scalable algorithmic framework for fault detection in complex operating environments of distributed systems through collaborative modeling of state representation, dynamic evolution, and deviation metrics.

3. Experimental Analysis

3.1 Dataset

This study adopts the HDFS distributed file system log dataset as the data source for analysis. The dataset is collected from the real operating environment of a distributed storage system. It records system log information generated by a large-scale cluster during long-term operation. It has been widely used in studies on failure detection and anomaly perception in distributed systems. The dataset is publicly available in open source form. It offers good accessibility and reproducibility. It realistically reflects system behavior under complex workloads and multi-node collaboration. It therefore meets the requirements of data-driven failure perception research.

In terms of data characteristics, the HDFS dataset is centered on log sequences. It covers state changes and event records of different nodes and service components during system operation. Log entries are organized in chronological order. This structure captures the temporal evolution of system behavior. The logs also contain multiple types of runtime information. This helps distinguish behavioral patterns between normal and abnormal states. Structurally, the dataset exhibits typical features of distributed systems. It reflects parallel execution across nodes, implicit inter-component relationships, and potential failure propagation patterns. These properties provide fundamental data support for building system-level perception models.

From the perspective of research context and application relevance, the distributed file system described by the HDFS dataset is a critical infrastructure in cloud computing and big data platforms. Its operational stability directly affects upper-level services and overall service quality. Conducting failure perception research based on this dataset has clear engineering relevance. It also helps evaluate the applicability and general value of data-driven methods in real distributed system scenarios. Modeling and analyzing this open dataset can provide representative evidence for intelligent monitoring and system state perception in complex distributed environments. This further strengthens the practical significance and generalizability of the research findings.

3.2 Experimental Results

This article first presents the results of the comparative experiments, as shown in Table 1.

Table 1. Comparative experimental results

Method	**Acc**	**Precision**	**Recall**	**F1-Score**
Deeplog [8]	0.821	0.834	0.809	0.821
Logbert [9]	0.836	0.842	0.826	0.834

Loggpt [10]	0.848	0.858	0.842	0.850
Logformer [11]	0.853	0.861	0.847	0.854
Hitanomaly [12]	0.862	0.870	0.856	0.863
Ours	0.879	0.888	0.874	0.881

Across Table 1, the compared methods exhibit a clear stepwise improvement, which aligns with the evolution of log-based failure perception from early template/sequence learners to stronger contextual encoders. Earlier architectures tend to rely on relatively limited feature abstractions, so their representation of complex, changing system states is constrained. As the models progressively strengthen sequence understanding and contextual fusion, they become better at capturing recurring operational patterns and separating them from irregular behaviors. This overall pattern suggests that richer temporal representation learning is a main driver behind the observed gains on distributed-system log data.

The comparison also reinforces that deep sequence modeling is generally more suitable than shallow or feature-limited frameworks for this task. Distributed-system failures rarely appear as isolated points; they often emerge through temporal accumulation, subtle precursor events, and dependency-driven propagation across components. Purely static snapshots struggle to describe such dynamics, while models designed to track state evolution can form more stable latent representations and identify abnormal deviations with higher fidelity. In practice, this better matches the continuous, streaming nature of system operation and the gradual formation of failure signatures.

Methods that incorporate attention-based or more expressive sequential structures further improve stability, indicating the importance of capturing long-range dependencies and non-local correlations within log sequences. At the same time, challenges remain when logs become heterogeneous across sources, services, or operating conditions, where redundancy, irrelevant fluctuations, and local noise can dilute useful signals. In contrast, the proposed approach emphasizes unified state modeling and deviation-oriented scoring, which helps reduce sensitivity to incidental variations and yields more consistent perception under complex, noisy environments. This difference is reflected in the stronger overall balance across accuracy, precision, recall, and F1.

Taken together, the results imply that relying on a single local pattern or a narrowly scoped structure is often insufficient for realistic distributed systems characterized by large scale, high state complexity, and frequent regime shifts. A data-driven framework that models operational states in an integrated manner, while explicitly accounting for temporal evolution and deviation measurement, is better positioned to identify potential failures before they become obvious. This supports the rationale of framing failure perception as representation learning plus state-deviation assessment, and it provides a solid analytical basis for subsequent work on intelligent monitoring and robust system-level anomaly perception.

In the fault perception model based on the reconfiguration mechanism, the state reconfiguration error weight coefficient directly affects how the model characterizes the normal operating mode and the degree of abnormal deviation of the system. A reasonable analysis of the impact of changes in this coefficient on model behavior helps to understand the mechanism and stability characteristics of reconfiguration constraints in the overall fault perception framework. The experimental results are shown in Figure 2.

Overall, adjusting the state reconstruction error weight noticeably shifts the model’s behavior. Different values guide the model to emphasize different aspects of system state characterization and deviation sensitivity. When the weight is low, the constraint on the original state is relatively weak. The model tends to rely more on the global distribution of latent representations. As the weight increases, the influence of the reconstruction constraint becomes stronger. The model then places greater emphasis on the consistency between current

system states and established normal patterns. This observation shows that the reconstruction error weight is not a marginal parameter. It directly shapes the manner in which system states are perceived.

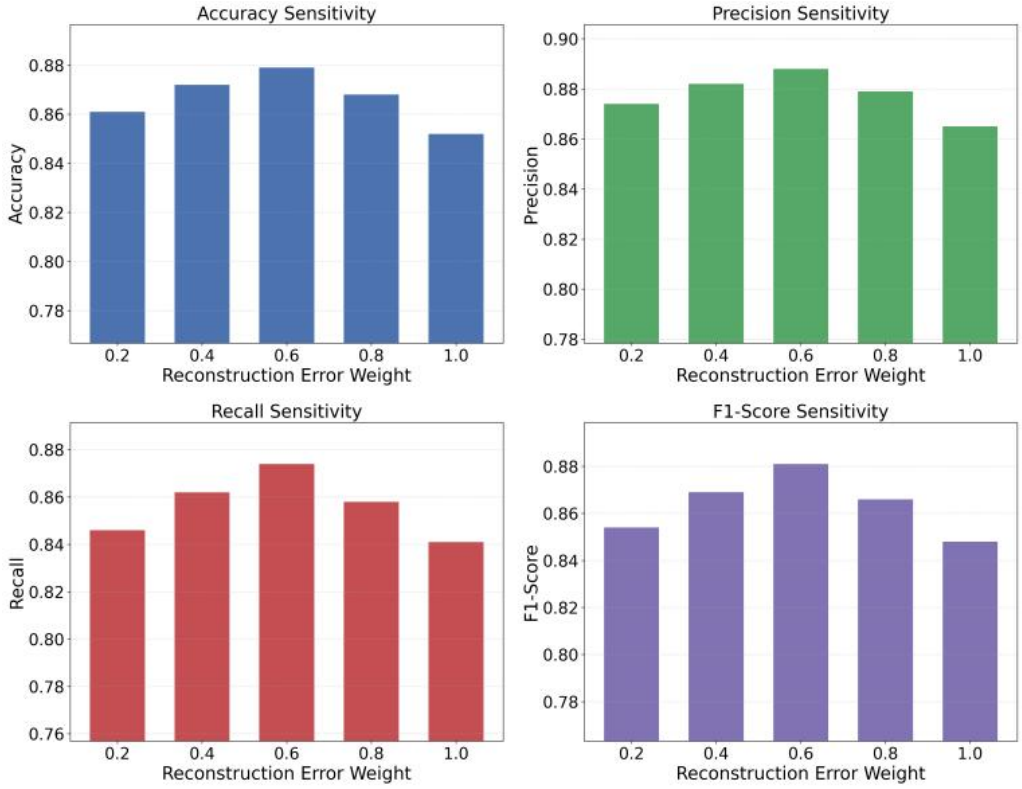


Figure 2. The influence of the state reconstruction error weighting coefficient on experimental results

Changes across multiple evaluation metrics reveal that their responses to weight adjustment are not fully consistent. This reflects the inherent complexity of failure perception in distributed systems. Some metrics exhibit more stable and coordinated trends within a moderate weight range. This suggests that the model achieves a better balance between capturing abnormal deviations and preserving normal state representation in this interval. When the weight continues to increase or decrease, the focus of the model shifts. Different metrics then respond to anomalies in divergent ways. This difference further indicates that a single constraint strength cannot simultaneously satisfy the multidimensional discrimination requirements of system operation.

From the perspective of model mechanisms, variations in the reconstruction error weight essentially affect the level of trust the model places in normal system behavior patterns. When the weight is too low, the constraint on reconstruction consistency is insufficient. Noise fluctuations in latent representations may be amplified. System state perception then becomes less concentrated. When the weight is too high, the model may overemphasize adherence to existing patterns. This can weaken sensitivity to novel or gradually evolving anomalies. This bidirectional effect highlights the central role of the reconstruction mechanism in distributed system failure perception. It also shows that the model must maintain a reasonable balance between stability and flexibility.

In summary, the sensitivity analysis confirms the critical regulatory role of the state reconstruction error weight within a data-driven distributed system failure perception framework. Appropriate weight settings help the model form more discriminative and structurally consistent system state representations. This improves the quality of anomaly perception in complex operating environments. These findings indirectly support the necessity of introducing reconstruction constraints in the proposed method. They also provide valuable guidance for model configuration under different system scales and operating conditions.

In distributed systems, changes in node size directly affect the complexity of the system's state space and the dependencies between nodes, thus increasing the difficulty of modeling fault perception models. Analyzing the changes in model behavior under node size expansion helps evaluate the adaptability and structural stability of data-driven methods in large-scale distributed environments. The experimental results are shown in Figure 3.

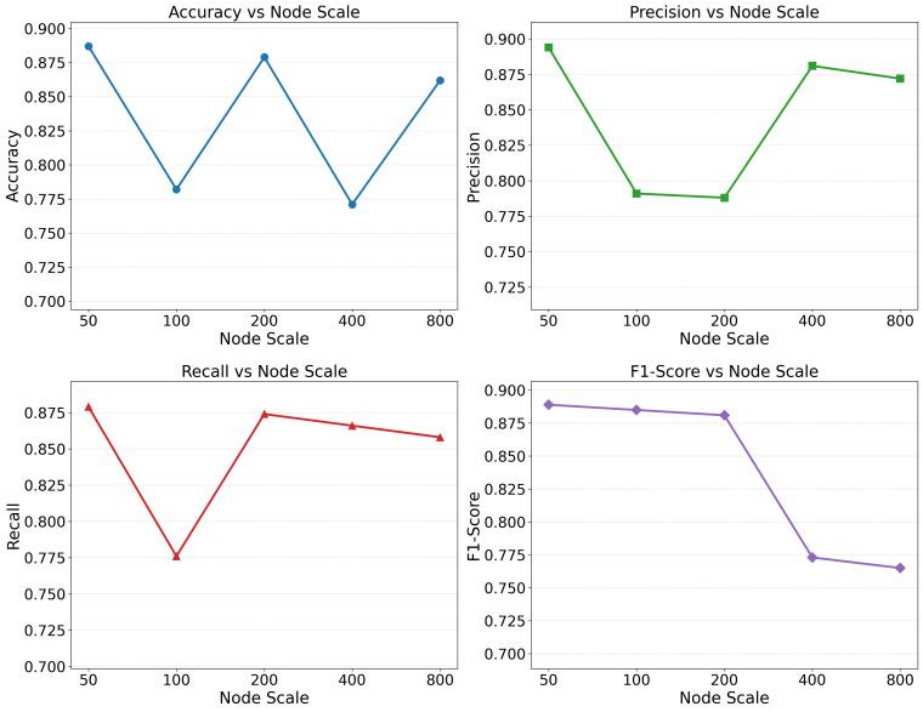


Figure 3. The impact of node size expansion on experimental results

As the node scale increases, the model’s performance across evaluation metrics changes in a distinctly non-linear manner. This reflects the higher demands that distributed system scaling places on failure perception modeling. When the system evolves from a small scale to a medium scale, interactions and state dependencies among nodes become significantly stronger. System operating patterns, therefore, grow more complex. This directly challenges the model’s ability to represent system states and capture structural relationships. These observations indicate that node scale expansion is not merely an increase in quantity. It is accompanied by a simultaneous rise in structural complexity.

A closer inspection of the metric variation patterns reveals substantial differences in how individual indicators respond to node scale expansion. This highlights the imbalance across multiple discrimination dimensions in failure perception tasks. Some metrics remain relatively stable as node scale changes. This suggests that the model can adapt to system topology and operational expansion within a certain range. Other metrics are more sensitive to scale variation. This implies that once system structural complexity exceeds a certain threshold, the difficulty of distinguishing abnormal states from normal ones increases noticeably. Such differences indirectly reflect the tension between structural dependency modeling and global consistency in distributed system state perception.

From the perspective of methodological mechanisms, node scale expansion increases the complexity of the latent state space and state transition relationships. The model must preserve consistency with historical operating patterns while handling more diverse local fluctuations. As the number of nodes grows, the impact of anomalies at individual nodes on the overall system state becomes diluted. At the same time, the importance of cross-node correlated anomalies increases. This places higher demands on holistic modeling capability. The inconsistency observed across evaluation metrics reflects the dynamic tradeoff between local anomaly perception and global state modeling.

In summary, the experimental results demonstrate that node scale is an important environmental factor influencing the performance of data-driven distributed system failure perception. Performance fluctuations under different scale settings indicate a close relationship between perception capability and system structural complexity. They also confirm the necessity of considering scale-induced structural effects when designing failure perception algorithms. This analysis provides valuable insight into model adaptability and robustness in large-scale distributed environments. It contributes to the further development of intelligent failure perception methods for complex systems.

In real-world distributed system scenarios, abnormal samples often exhibit unstable proportions that change over time, placing higher demands on the discrimination mechanism of fault perception models. Analyzing the model's accuracy response under varying abnormal sample proportions helps evaluate the stability and adaptability of data-driven methods when sample distribution shifts. The experimental results are shown in Figure 4.

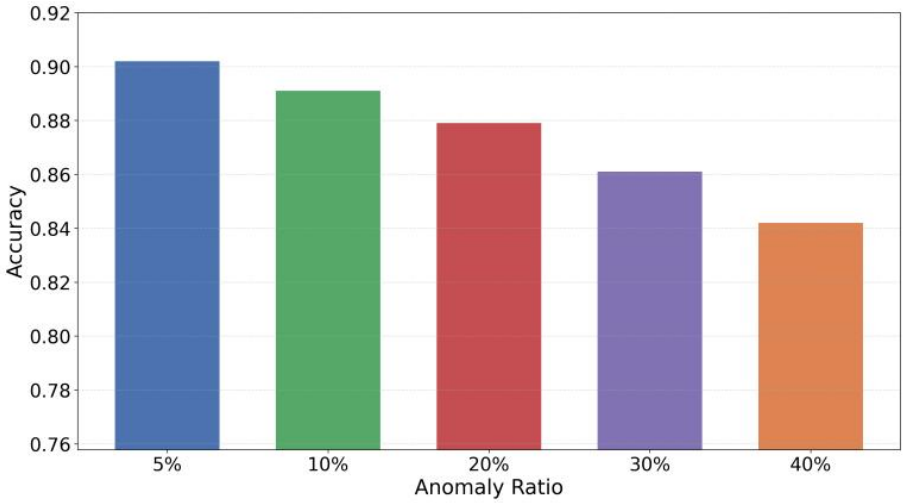


Figure 4. The impact of changes in the proportion of outliers on Acc

The overall trend indicates that an increase in the proportion of anomalous samples has a persistent and clear impact on model accuracy. This highlights the critical role of sample distribution structure in distributed system failure perception tasks. When the anomaly ratio is low, system behavior is still dominated by normal states. The model can stably learn and maintain a global characterization of normal behavior. As anomalous samples gradually increase, the data distribution shifts noticeably. The model then faces a more complex discrimination environment. This places higher demands on state representation capability and decision stability.

Further observation shows that accuracy changes in a unidirectional manner as the anomaly ratio varies. This indicates that the model is sensitive to changes in sample distribution. As the proportion of anomalies continues to rise, the boundary between normal and abnormal states becomes increasingly blurred. The model must perform discrimination under more imbalanced data conditions. For distributed systems, this situation is practically relevant. Anomalies in real environments are often not sparse events. They may appear in a concentrated manner during certain periods. This can significantly alter the overall system state distribution.

From the perspective of methodological mechanisms, changes in the anomaly ratio directly affect the quality of modeling normal system patterns. When the anomaly proportion is high, reconstruction or representation learning inevitably incorporates more anomalous features. This interferes with the characterization of normal states. As a result, discrimination accuracy is reduced. This process reveals the inherent dependence of data-driven failure perception methods on distribution stability. It also shows that the anomaly ratio is an important data-level factor influencing model behavior.

In summary, the experimental results demonstrate that the proportion of anomalous samples constitutes a critical data-sensitive factor influencing failure perception accuracy in distributed systems. As the sample distribution shifts with varying anomaly ratios, the model’s behavior reflects its dependence on the statistical structure of the observed data, highlighting the intrinsic relationship between anomaly prevalence and the learned representation of normal system behavior. Performance variations observed under different anomaly ratios indicate that the proposed approach is capable of adjusting its internal decision boundaries in response to distributional changes, thereby maintaining a coherent perception of system states across diverse data conditions.

At the same time, these observations underline the practical importance of accounting for anomaly ratio fluctuations when deploying failure perception models in real-world distributed environments. In operational systems, anomaly occurrence is rarely static and may change significantly over time due to workload variation, system upgrades, or cascading failures. The analysis, therefore, emphasizes that robust failure perception requires not only effective modeling of normal and abnormal patterns, but also careful consideration of how evolving data distributions influence model reliability. This insight provides a valuable reference for evaluating the stability and practical applicability of data-driven failure perception models under dynamic and non-stationary data conditions.

In practical distributed systems, operational data typically comes from multiple heterogeneous monitoring sources, making data gaps unavoidable and uncertain. Analyzing the impact of varying multi-source data gap ratios on model accuracy helps evaluate the stability and robustness of data-driven fault perception methods under conditions of incomplete information. The experimental results are shown in Figure 5.

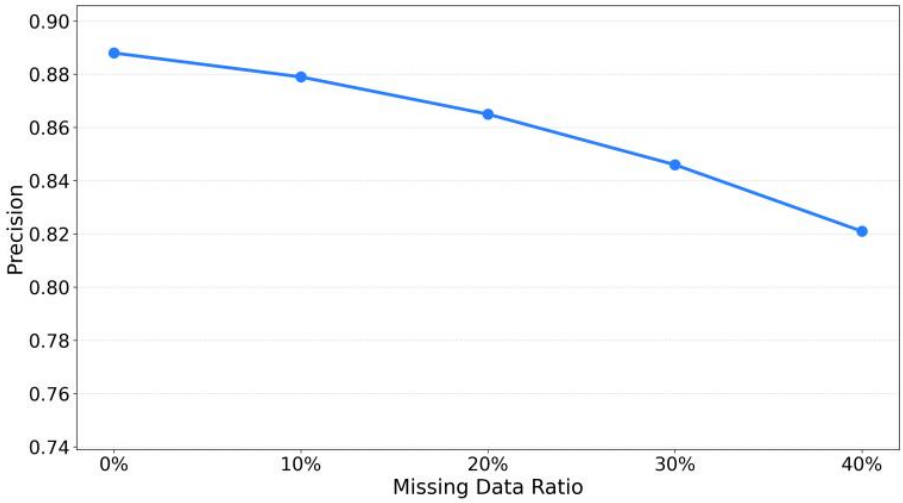


Figure 5. The impact of the proportion of missing data from multiple sources on Precision

The overall pattern shows that changes in the missing ratio of multi-source data have a persistent and stable influence on model precision. This highlights the critical role of data completeness in distributed system failure perception. When multi-source monitoring information is largely available, the model can more easily form a consistent representation of system states. This supports reliable discrimination during anomaly detection. As the missing ratio gradually increases, system state descriptions become less sufficient. The model then faces higher uncertainty.

Further analysis indicates that the variation in precision follows a smooth and regular trend. This suggests that the model does not rely on a single data source. Instead, it integrates multiple signals to perform state judgment. When part of the data is missing, the model can still maintain basic discrimination capability by using the remaining information. As the missing scope expands, the advantage of multi-source collaborative modeling is gradually weakened. This observation shows that multi-source information fusion is a core factor for improving failure perception precision in distributed systems.

From the perspective of methodological mechanisms, missing multi-source data directly affects the model's ability to capture fine-grained details of system operation. This is particularly evident when distinguishing similar operating patterns from subtle abnormal deviations. Information loss amplifies uncertainty in these cases. As the missing ratio increases, the localization of anomalous patterns in latent representation space becomes coarser. This reduces the granularity of anomaly discrimination. These findings reflect the inherent challenges faced by data-driven methods under incomplete information conditions. They also demonstrate the important role of multi-source collaborative information in constraining model decision boundaries.

In summary, the experimental results demonstrate that the missing ratio of multi-source data is a key data-sensitive factor influencing the precision of distributed system failure perception. Performance trends under different missing conditions confirm the adaptability of the proposed method in scenarios with gradually increasing information loss. They also emphasize the importance of ensuring the completeness of critical monitoring data in practical system deployment. This analysis provides valuable insight into the impact of data incompleteness on failure perception performance in complex distributed environments.

4. Restrictive Analysis

This section conducts a restrictive analysis to clarify the scope, assumptions, and applicability boundaries of the proposed data-driven fault perception approach in distributed systems. The analysis focuses on the inherent constraints imposed by system observability, data quality, and modeling abstractions, emphasizing that the method operates under the premise that system behavior can be sufficiently characterized by available runtime data streams. While the unified state representation enables effective perception of complex system dynamics, the approach assumes relative stability in the underlying system architecture and monitoring interfaces during operation. As a result, abrupt structural reconfigurations or severe monitoring disruptions may reduce perception reliability, highlighting the importance of consistent data acquisition and system instrumentation for maintaining robust fault awareness within large-scale distributed environments.

5. Conclusion

This work focuses on practical challenges in distributed systems, including complex operating environments, large node scale, and diverse failure patterns. It systematically investigates data-driven failure perception methods. By modeling system operating states in a unified manner, the approach captures normal behavior patterns without relying on manually defined rules. Potential failures are then perceived through quantitative measurement of state deviations. Comparative experimental results demonstrate strong overall performance across multiple evaluation metrics. This indicates that data-driven modeling is well-suited and stable for failure perception in complex distributed systems.

From a methodological perspective, the proposed failure perception framework emphasizes holistic modeling of system-wide operating states. It can form consistent state representations under conditions of multi-node parallel execution and strong state coupling. This system-level modeling perspective helps alleviate the limitations of traditional approaches when facing complex dependencies and dynamic changes. Failure perception is no longer restricted to local anomalies or single metric variations. The results further show that deep modeling of system operation data can effectively improve the identification of latent anomalies and complex failure patterns. This provides more reliable technical support for stable distributed system operation.

At the application level, the findings offer important reference value for intelligent operation and maintenance in cloud platforms, large-scale data centers, and critical infrastructure systems. As distributed systems play an increasingly central role in service delivery and operational assurance, models with efficient failure perception capability become essential for improving system availability and operational efficiency. The proposed method provides a feasible path for building automated and intelligent system monitoring and early warning mechanisms. It helps reduce maintenance costs, shorten failure response time, and improve overall system operation quality.

Looking ahead, data-driven failure perception methods still have broad development potential as distributed systems continue to scale and operating scenarios evolve. On one hand, integrating richer operational information and more flexible modeling mechanisms may further enhance adaptability to complex failure patterns. On the other hand, deeper integration of failure perception results in system scheduling, resource management, and adaptive control that can support a shift from passive monitoring to active regulation. This work lays a foundation for future research. It also provides valuable insights for advancing distributed systems toward greater intelligence, safety, and reliability.

References

[1] M. Landauer, S. Onder, F. Skopik et al., "Deep Learning for Anomaly Detection in Log Data: A Survey," Machine Learning with Applications, vol. 12, Art. no. 100470, 2023.

[2] S. Huang, Y. Liu, C. Fung et al., "Improving Log-Based Anomaly Detection by Pre-Training Hierarchical Transformers," IEEE Transactions on Computers, vol. 72, no. 9, pp. 2656-2667, 2023.

[3] J. Bogatinovski, G. Madjarov, S. Nedelkoski et al., "Leveraging Log Instructions in Log-Based Anomaly Detection," Proceedings of the 2022 IEEE International Conference on Services Computing (SCC), pp. 321-326, 2022.

[4] Y. Liu, S. Ren, X. Wang et al., "Temporal Logical Attention Network for Log-Based Anomaly Detection in Distributed Systems," Sensors, vol. 24, no. 24, Art. no. 7949, 2024.

[5] Y. Zhu, J. Wang, B. Li et al., "MicroIRC: Instance-Level Root Cause Localization for Microservice Systems," Journal of Systems and Software, vol. 216, Art. no. 112145, 2024.

[6] Z. Yu, Q. Ouyang, C. Pei et al., "Causality Enhanced Graph Representation Learning for Alert-Based Root Cause Analysis," Proceedings of the 2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing (CCGrid), pp. 77-86, 2024.

[7] J. Jiang, "Reinforcement Learning–Based Dynamic Decision Framework for Server Backend Resource Management," 2024.

[8] M. Du, F. Li, G. Zheng et al., "DeepLog: Anomaly Detection and Diagnosis from System Logs Through Deep Learning," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1285-1298, 2017.

[9] H. Guo, S. Yuan and X. Wu, "LogBERT: Log Anomaly Detection via BERT," Proceedings of the 2021 International Joint Conference on Neural Networks (IJCNN), pp. 1-8, 2021.

[10] J. Qi, Z. Wang, C. Li et al., "LogGPT: Exploring ChatGPT for Log-Based Anomaly Detection," Proceedings of the 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), 2023.

[11] H. Guo, J. Yang, J. Liu et al., "Logformer: A Pre-Train and Tuning Pipeline for Log Anomaly Detection," Proceedings of the AAAI Conference on Artificial Intelligence, vol. 38, no. 1, pp. 135-143, 2024.

[12] S. Huang, Y. Liu, C. Fung et al., "HiTAnomaly: Hierarchical Transformers for Anomaly Detection in System Log," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2064-2076, 2020.