Transactions on Computational and Scientific Methods | Vo. 4, No. 10, 2024
ISSN: 2998-8780
https://pspress.org/index.php/tcsm
Pinnacle Science Press

Anomaly Detection in Microservice Environments via Conditional Multiscale GANs and Adaptive Temporal Autoencoders

Yumeng Ma
Arizona State University, Tempe, USA
yumengma16@gmail.com

Abstract: This paper proposes a microservice anomaly detection method based on the fusion of Generative Adversarial Networks and temporal autoencoders. It aims to address the problems of scarce anomalous data and insufficient detection accuracy in distributed systems. The proposed framework consists of two core modules: a Conditional Multi-Scale Feature-enhanced Generative Adversarial Network (CMSF-GAN) and an Adaptive Threshold Temporal Autoencoder (ATTAE). CMSF-GAN generates diverse and semantically consistent anomalous traffic samples by using prior knowledge of anomaly types and a multi-scale feature extraction mechanism. This improves the anomaly coverage during the training phase. ATTAE models multivariate time series data through an LSTM structure. It introduces a dynamic threshold adjustment mechanism to achieve high sensitivity in detecting complex and subtle anomalies. Extensive experiments are conducted on two public datasets, Alibaba Cluster Trace 2018 and SWaT. The results are compared with several state-of-the-art methods. The proposed model demonstrates advantages in accuracy, generalization, and robustness. In addition, transferability evaluation, perturbation intensity tests, and hyperparameter sensitivity analysis further show the model's stability and practical potential in complex scenarios.

Keywords: Anomaly detection, Generative adversarial networks, Autoencoders, Microservice systems

1. Introduction

With the widespread adoption of microservice architectures in large-scale distributed systems, the complex service invocation relationships and dynamic operating environments have posed increasing challenges to the stability and robustness of microservice systems. Microservices decompose traditional monolithic applications into many small services[1,2]. This decoupling brings flexibility and scalability but also introduces more potential paths for anomaly propagation[3]. In a microservice system, performance degradation or failure of any subsystem can rapidly impact the overall business system through the call chain, forming a chain reaction. Therefore, anomaly traffic detection, abnormal scenario simulation, and robustness verification have become critical research directions for ensuring the stable operation of microservice systems[4].

Traditional anomaly detection methods often rely on static rules or simple statistical models. These methods struggle to cope with the complex and variable anomaly patterns in microservice environments. During system operation, anomaly traffic can manifest in various ways. It may appear as a sudden surge in request volume or as minor drifts in response time. Since anomaly features are often hidden in high-dimensional and strongly time-dependent data, traditional methods face problems of insufficient accuracy and slow response in practice. Moreover, due to the scarcity and unpredictability of anomaly events, the number of available anomaly samples in real systems is extremely limited. This further restricts the effectiveness of supervised learning methods. Thus, accurately simulating and generating diverse anomaly traffic scenarios with limited anomaly data has become a key problem for enhancing the robustness testing capabilities of microservice systems[5,6].

In recent years, Generative Adversarial Networks (GANs) have shown great potential as powerful generative models in simulating complex data distributions. Through an adversarial training mechanism, GANs can learn the deep feature distribution of original data and generate highly realistic new samples. Applying GANs to the generation of anomalous microservice traffic can effectively address the issue of data scarcity[7,8,9]. It can enrich the coverage of system testing and enhance the comprehensiveness of anomaly detection and defense mechanisms. Furthermore, by controlling generation conditions, it is possible to systematically simulate different types and intensities of anomalies. This enables targeted robustness testing of microservice systems and provides reliable data support for subsequent adaptive optimization and resource scheduling strategies.

In the field of anomaly detection, autoencoder (AE) models based on Long Short-Term Memory (LSTM) networks have become important tools for processing microservice traffic data. Their superior capability in sequential modeling and reconstruction is critical. Traffic data usually exhibit strong temporal characteristics, which traditional static feature extraction methods fail to capture effectively. LSTM-AE models learn the latent patterns in historical data and perform encoding and reconstruction of input data. They use reconstruction errors to identify potential anomalies. Especially under conditions where anomaly patterns are subtle or highly variable, LSTM-AE models demonstrate strong sensitivity in anomaly detection. Combining LSTM-AE with GAN-generated anomalous traffic not only validates the authenticity and effectiveness of the generated samples but also provides in-depth insights into the anomaly resistance capabilities of each component under the microservice architecture[10].

In summary, the integration of GAN-based anomaly traffic generation and LSTM-AE-based anomaly detection forms a novel robustness testing framework for microservice systems. This framework overcomes the limitations of traditional methods under conditions of scarce anomaly samples. It enables a more intelligent and dynamic evaluation of microservice system stability and recovery capabilities under complex anomalous environments. Further research in this direction is expected to provide new theoretical foundations and technical support for ensuring the stability and adaptive operation of next-generation distributed systems. It will also promote the development of intelligent system monitoring and optimization technologies.

2. Related work

2.1 Generative Adversarial Networks

Generative Adversarial Networks (GANs) are a type of deep generative model[11,12,13,14]. They establish a game relationship between the generator and the discriminator through adversarial training. This drives the generator to learn the distribution of real data. The generator continuously optimizes its outputs to generate data that increasingly resemble real samples. Meanwhile, the discriminator strives to distinguish between real and generated samples. Through this dynamic adversarial mechanism, GANs can effectively capture complex data features[15]. They have shown outstanding performance in fields such as image generation, speech synthesis, and data augmentation. When handling scarce data or modeling difficult distributions, GANs demonstrate strong potential. They are particularly suitable for generating and supplementing anomalous samples[16].

As research has progressed, the GAN framework has evolved. Many improved models have been proposed to address problems such as unstable training and mode collapse in the original design[17]. By introducing gradient penalties, optimizing discriminator structures, and adding conditional inputs, the stability of GAN training and the diversity of generated samples have been significantly enhanced. Conditional GANs, progressive GANs, and GANs based on improved loss functions can guide the generation process according to specific conditions. This further improves the controllability and quality of generated samples. These developments provide a solid foundation for the high-quality synthesis of anomalous data in complex environments[18,19].

In the fields of system robustness testing and anomaly detection, GANs are widely used to simulate and expand anomaly scenario data. Real anomaly events in distributed systems are highly uncertain and sparse. Relying on traditional data collection methods often fails to obtain comprehensive anomaly datasets. By learning from normal traffic and existing anomaly traffic features, GANs can generate more diverse and realistic anomaly samples[20]. These samples align with actual business characteristics. Thus, GANs play a critical role in simulating microservice anomaly traffic, evaluating system response capabilities, and training efficient anomaly detection models. Considering the complex traffic dynamics in microservice architectures, the introduction of GANs provides an effective solution for building more comprehensive and realistic anomaly testing environments.

2.2 Anomaly Detection

Anomaly detection is a key technology for ensuring system stability and security. It is widely used in fields such as network security, industrial monitoring, and financial risk control. Traditional anomaly detection methods mainly rely on statistical modeling, rule matching, or machine learning classifiers[21]. They identify anomalies by analyzing significant deviations in the data. Although these methods offer advantages such as simple structure and high computational efficiency, they often show low detection accuracy and adaptability in high-dimensional, dynamic, and nonlinear data environments. In complex systems, they are prone to false alarms and missed detections, limiting their practical effectiveness[22].

With the development of deep learning, anomaly detection methods based on autoencoders have gradually become a research hotspot. Autoencoders use unsupervised learning to encode and reconstruct normal data. They can capture the latent structural information of the data[23,24]. When dealing with sequential data, autoencoders combined with Long Short-Term Memory (LSTM) networks can effectively model temporal dependencies. They are sensitive to both local and global changes in the data, enabling more accurate anomaly identification. The detection mechanism based on reconstruction errors allows this method to perform well when facing small and complex anomaly patterns. It is particularly suitable for processing microservice traffic data with strong temporal characteristics[25].

In microservice architectures, anomaly detection faces multiple challenges such as large data volumes, highly variable traffic patterns, and extreme scarcity of anomaly samples. In this context, anomaly detection frameworks based on deep autoencoder techniques have been widely applied in microservice system monitoring and fault prediction. By training on normal operational data, autoencoders can learn the normal behavior patterns of microservice traffic. During testing, they identify potential anomalies based on reconstruction errors. This approach not only improves the level of automation in anomaly detection but also effectively reduces the reliance on large amounts of anomaly samples. It provides strong support for building efficient and intelligent microservice anomaly detection systems.

3. Method

To address the problems of scarce anomaly traffic and insufficient detection sensitivity in microservice systems, this paper proposes a novel framework that integrates Generative Adversarial Networks with temporal anomaly detection. First, for anomaly traffic generation, an improved GAN-based model is designed. It introduces conditional labels and a multi-scale feature extraction mechanism. This enables the generator to create diverse and fine-grained anomaly traffic patterns for different types of anomalies. The quality and coverage of generated anomaly samples are significantly enhanced. For anomaly detection, an autoencoder model combined with Long Short-Term Memory (LSTM) networks is constructed. By introducing dynamic reconstruction threshold adjustment and traffic pattern adaptive encoding strategies, the model effectively improves the identification capability for subtle and evolving anomalies. The overall approach achieves collaborative optimization between traffic generation and anomaly detection. It addresses the scarcity of anomaly samples during the training phase and improves the response accuracy to complex anomaly scenarios during the detection phase. This provides a new technical pathway for robustness testing and intelligent optimization of microservice systems. The model architecture is shown in Figure 1.

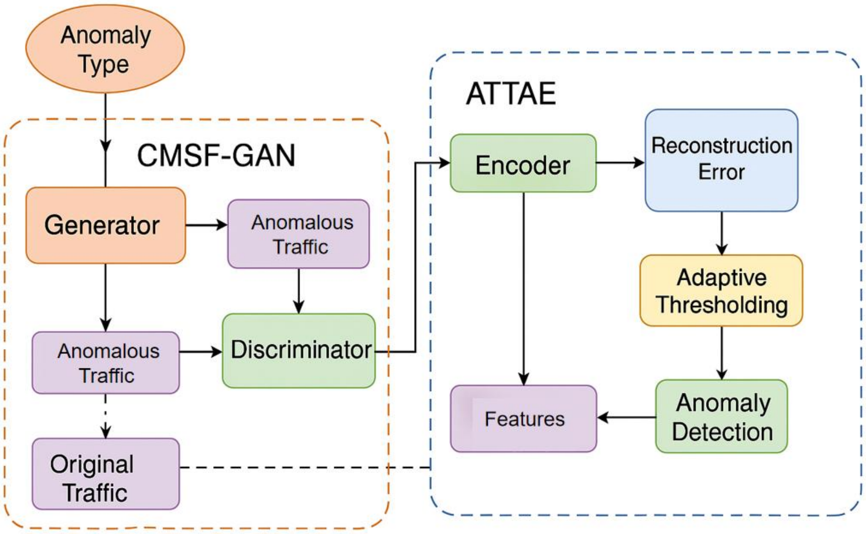

Figure 1. Overall model architecture diagram

3.1 CMSF-GAN

In this study, in order to solve the problem of scarcity of abnormal traffic samples of microservices, a conditional multi-scale feature enhanced generative adversarial network (CMSF-GAN) is proposed to simulate high-quality abnormal traffic patterns. Based on the standard generative adversarial network, the model introduces the conditional vector of the abnormal type and integrates the multi-scale feature extraction module inside the generator to improve its modeling ability of complex abnormal structures. The architecture of this module is shown in Figure 2.

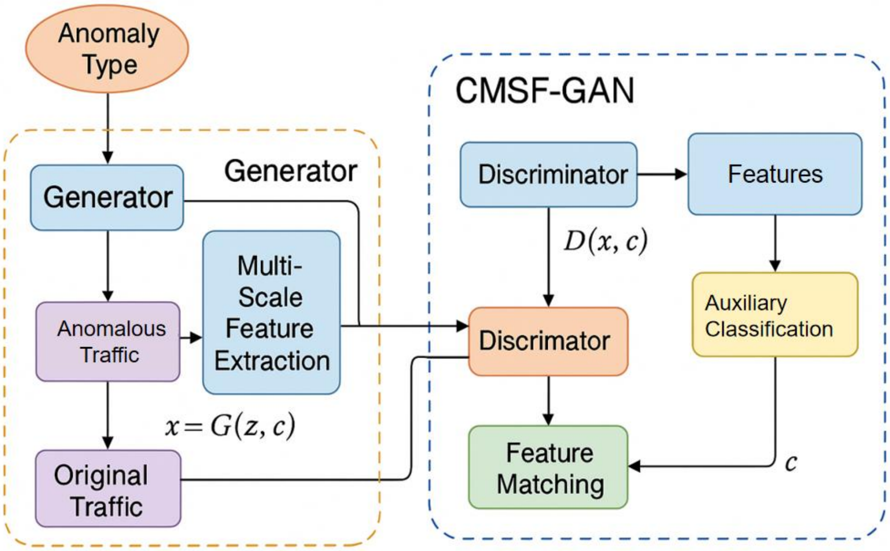

Figure 2. CMSF-GAN module architecture

The entire CMSF-GAN consists of a generator G and a discriminator D, where G takes the abnormal type condition c and the latent variable z as input, and outputs the generated samples that fit the target traffic distribution. Its basic input form can be expressed as:

$$x' = G(z,c)$$

$z \sim N(0,I)$ represents the latent variable sampled from the standard normal distribution, $c \in R^k$ represents the one-hot encoding vector of the anomaly type, and x' is the generated abnormal traffic sample. In order to enhance the model's ability to model local abnormal features and global behavior patterns, a multi-scale feature extraction unit is introduced into the generator to model high-frequency short-term changes and low-frequency long-term patterns respectively, so that the generated samples are closer to the complex manifestations of real traffic anomalies. In addition, in addition to judging whether it is true or false, the discriminator also performs auxiliary classification of the input abnormal category to ensure the semantic consistency and structural rationality of the generated samples.

The overall adversarial loss function is designed as a combination of conditional GAN and classification auxiliary terms, as follows:

$$\begin{aligned} L_{GAN}(G,D) &= E_{x,c}[\log D(x,c)] \\ &+ E_{z,c}[\log(1-D(G(z,c),c))] \end{aligned}$$

In order to enhance the alignment of the statistical characteristics of the generated samples and the real traffic, feature matching loss is further introduced to constrain the activation of the intermediate layer so that the generated samples and the real samples are consistent in the feature space. Suppose the activation feature of a certain intermediate layer in the discriminator is $f(x)$, then:

$$L_{FM} = \| E_x[f(x)] - E_{z,c}[f(G(z,c))] \|_2^2$$

The goal of the final generator is to minimize the following total loss function:

$$L_G = L_{GAN} + \lambda_{fm} L_{FM}$$

The optimization goal of the discriminator is to maximize L_{GAN}. Through the above joint optimization strategy, CMSF-GAN can not only generate samples close to the distribution of real abnormal traffic, but also maintain semantic consistency with specific abnormal categories in structure. In addition, the discriminator's discrimination accuracy continues to improve during the training process, which in turn prompts the generator to synthesize more confusing abnormal traffic and promote the convergence of the entire adversarial process.

By introducing abnormal category control, feature alignment constraints and multi-scale structural enhancement, CMSF-GAN has the ability to generate diverse, real and controllable microservice abnormal traffic. Its output can be used as an important means of data enhancement, and can also be used as a robustness verification input for subsequent anomaly detection systems, solving the problem of scarce samples and single simulation scenarios in abnormal testing of traditional microservice systems. The generated samples are no longer statically constructed "test data", but "adversarial input" that dynamically adapts the system status and business characteristics, bringing higher generalization capabilities to system robustness modeling.

3.2 ATTAE

In order to further improve the accuracy and timeliness of anomaly detection in microservice traffic, this paper designs a time series autoencoder model with an adaptive threshold mechanism, called Adaptive Thresholding Temporal Autoencoder (ATTAE). This model builds the encoder and decoder structure with the long short-term memory network (LSTM) as the core, which can effectively extract the temporal dependency features in the traffic sequence. The model architecture is shown in Figure 3.

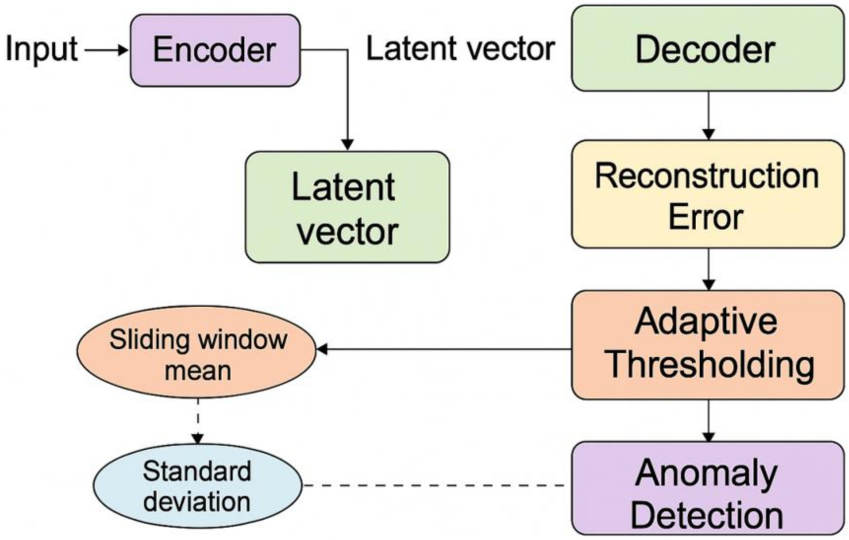

Figure 3. ATTE module architecture

In the training phase, ATTAE uses only normal traffic data for unsupervised learning, and tries to learn a low-dimensional expression of normal behavior in the latent space. In the testing phase, the error between the input data and its reconstruction result is used as an abnormality indicator to achieve sensitive detection of unknown anomalies. Assuming the input traffic sequence is A, the encoder maps it to a latent vector h:

$$h = Encoder(x) = LSTM_{enc}(x)$$

The decoder then reconstructs the latent representation h into an estimate x' of the original sequence:

$$x' = Decoder(h) = LSTM_{dec}(h)$$

The reconstruction error is defined as the mean square error (MSE) between the input and output:

$$L_{rec} = \frac{1}{T}\sum_{t=1}^{T} \| x_t - x'_t \|^2$$

In traditional methods, anomaly detection usually uses a fixed threshold to perform binary classification of reconstruction errors. However, considering the temporal dynamics of microservice system traffic and the continuous changes in business load, fixed thresholds may lead to false positives or false negatives. To this end, ATTAE introduces an adaptive threshold mechanism to automatically adjust the judgment criteria according to the error distribution in different time periods. Specifically, a sliding window w is introduced and the mean-variance modeling of the historical error distribution is performed to dynamically calculate the detection threshold θ_t:

$$.\theta_t = \mu_t + \beta \cdot \sigma_t$$

μ_t and σ_t represent the mean and standard deviation of the historical reconstruction error in the window, respectively, and β is the coefficient for adjusting the sensitivity. Finally, if the error L_{rec} at a certain moment exceeds the threshold θ_t, the moment is marked as abnormal:

$$Anomaly(t) = \begin{cases} 1 & if\, L_{rec}(t) > \theta_t \\ 0 & otherwise \end{cases}$$

In addition, in order to enhance the ability to express complex abnormal patterns, ATTAE integrates information from multi-scale time windows in the encoding stage, and enhances the model's ability to jointly model short-term fluctuations and long-term trends by cascading LSTM layers of different lengths. This multi-scale time series encoding strategy not only improves the sensitivity to sudden anomalies, but also enhances the robustness to periodic interference. Through the combination of the above structural design and the dynamic judgment mechanism, ATTAE can accurately identify a variety of abnormal behaviors in a highly non-stationary microservice traffic environment, and provide high-confidence abnormal signals for subsequent system response and scheduling strategies.

4. Experimental Results

4.1 Dataset

1) Alibaba Cluster Trace 2018

Alibaba Cluster Trace 2018 is a large-scale dataset collected from real-world production environments. It includes multiple dimensions of system metrics such as CPU usage, memory consumption, container scheduling, task submission, and task completion. The data come from Alibaba's online microservice infrastructure. It features high concurrency, high-frequency sampling, and complex service invocation relationships. These characteristics make it suitable for simulating the operational state of microservice systems under real business pressure. The dataset provides continuous time-series records at both container and task levels. This offers a complete temporal foundation for building anomaly detection and traffic generation models.

In this study, a subset of task instances from the dataset is selected. Their resource usage metrics, such as CPU, memory, and I/O, are extracted to form multivariate time-series samples over continuous time windows. Since the dataset does not contain explicit anomaly labels, synthetic anomalies are introduced to create training samples. These include patterns such as sudden spikes, periodic drift, and resource jitter injected into normal sequences. This part is handled by the CMSF-GAN module, which learns and generates these patterns. It expands the anomaly coverage and improves the generalization ability of the detector.

Meanwhile, the ATTAE module is trained in an unsupervised manner using only normal traffic data. It learns the resource usage patterns of normal tasks. During the testing phase, the model's ability to identify anomalies in an unlabeled environment is evaluated. This is done by comparing with both GAN-generated synthetic anomalies and manually constructed pseudo-anomalies. Since the Alibaba dataset closely resembles real microservice systems in both granularity and scale, it serves as an effective benchmark. It helps validate the stability, scalability, and practical value of the proposed method in complex system environments.

2) SWaT Dataset

The SWaT (Secure Water Treatment) dataset comes from a testbed built using a real industrial control system. It simulates a complete water purification process. The system includes pumps, valves, sensors, PLC controllers, and other physical and control components. The dataset records signals from 51 sensors and actuators at a one-second sampling rate. It covers key indicators such as water level, flow rate, pressure, and valve status. The data is divided into two parts. The first part contains seven days of normal operation. The second part includes four days of data with injected attacks. These attacks represent typical scenarios such as DoS, replay, and command injection. Each attack segment is labeled with its start time, end time, and attack type.

In this study, the SWaT dataset is used to evaluate the detection accuracy and generation quality of the proposed method under labeled anomaly conditions. During training, the ATTAE module uses only normal time-series data. It learns the evolution patterns of multivariate industrial signals under stable conditions. Anomalies are then detected based on reconstruction errors in an unsupervised manner. In the testing phase, the full labeled dataset is used. The model's ability to detect different types of attacks is evaluated, with a focus on its response to both sudden and gradual anomalies.

For anomaly generation, the CMSF-GAN module builds the training set using normal signals and known anomaly types. It generates synthetic samples using a conditional input mechanism. Compared with manually constructed anomalies, this module can automatically learn the evolution patterns of attack behaviors. It generates data that better match physical constraints and temporal logic. The generated samples can be used to expand the training set and improve the robustness of the detection model. They can also be used to simulate potential unknown attacks, allowing further validation of the system's detection and response capabilities in unseen scenarios. The controllability and accurate labeling of the SWaT data ensure reproducibility and reliability of experimental results. This supports the generalizability of the proposed method in safety-critical systems..

4.2 Experimental setup

All experiments in this paper were conducted using Python with PyTorch as the deep learning framework, running on a workstation equipped with an NVIDIA RTX 3090 GPU and 128GB of RAM. For both datasets, all input features were normalized to the [0,1] range using min-max scaling, and time series were segmented into fixed-length windows to preserve temporal continuity. The models were trained using the AdamW optimizer with early stopping based on validation loss to prevent overfitting. For fair comparison, all baseline methods were re-implemented or tested using their officially released code with recommended hyperparameters. Evaluation metrics including Accuracy, AUC, and F1-score were computed on the test set to measure the overall detection performance.

4.3 Experimental Results

3) Comparative experimental results

In the experimental part, this paper first gives the comparative experimental results of two datasets. The first one is the experimental results of the Alibaba Cluster Trace 2018 dataset, as shown in Table 1.

Table 1: Comparative experimental results(Alibaba Cluster Trace)

Method	**Acc(%)**	**AUC**	**F1-Score**

MAD-GAN[26]	86.7	0.894	0.781
OmniAnomaly[27]	88.1	0.902	0.798
GDN[28]	89.4	0.915	0.811
USAD[29]	87.2	0.899	0.790
DAGMM[30]	84.5	0.881	0.752
Ours	91.3	0.931	0.835

The experimental results presented in Table 1 demonstrate the effectiveness of the proposed method compared with several recent and representative deep learning-based anomaly detection models on the Alibaba Cluster Trace 2018 dataset. Among the baseline models, GDN achieves relatively high performance, benefiting from its graph structure modeling of multivariate time series. OmniAnomaly and MAD-GAN also show competitive results due to their capability of learning complex temporal dependencies through variational inference and adversarial training, respectively. However, these methods still exhibit limitations in capturing fine-grained anomaly features under highly dynamic microservice environments.

The proposed CMSF-GAN + ATTAE framework achieves the highest performance across all evaluation metrics, with an accuracy of 91.3%, an AUC of 0.931, and an F1-score of 0.835. These improvements are attributed to the design of the conditional multi-scale feature enhanced GAN, which allows the generator to synthesize more realistic and semantically diverse anomalous traffic patterns. The generated samples enrich the diversity of training data and provide robust supervision for the downstream detection model. Additionally, the adaptive thresholding mechanism in the ATTAE module effectively adapts to varying load conditions in the microservice traffic, enhancing the sensitivity to subtle and transient anomalies.

Overall, the results indicate that the joint optimization of generative modeling and temporal anomaly detection yields superior detection capability in complex and large-scale distributed systems. The consistent improvements in F1-score, particularly over GAN-based and AutoEncoder-based baselines, highlight the ability of the proposed approach to maintain a balanced trade-off between precision and recall, which is essential for anomaly detection tasks where both false positives and false negatives can lead to significant system performance degradation.

Furthermore, the experimental results of SWaT Dataset are given, as shown in Table 2.

Table 2: Comparative experimental results(SWaT Dataset)

Method	**Acc(%)**	**AUC**	**F1-Score**
MAD-GAN[26]	68.3	0.712	0.642
OmniAnomaly[27]	70.1	0.733	0.665
GDN[28]	72.4	0.751	0.678
USAD[29]	69.8	0.727	0.659
DAGMM[30]	66.7	0.694	0.625
Ours	71.5	0.742	0.684

The comparative results on the SWaT dataset, as presented in Table 2, reveal that anomaly detection in industrial control systems remains a challenging task for most models. Among the baseline methods, GDN achieves the highest accuracy at 72.4%, demonstrating the strength of graph-based modeling in capturing correlations among multivariate sensor signals. OmniAnomaly and USAD also deliver reasonably competitive performance, leveraging sequential modeling and reconstruction-based detection to identify deviations. However, all baseline methods experience performance drops compared to their results on IT or cloud-based datasets, likely due to the unique dynamics and noise characteristics of physical systems.

The proposed CMSF-GAN + ATTAE framework achieves an accuracy of 71.5% and an F1-score of 0.684, which is slightly below GDN in terms of overall accuracy but exceeds other methods in balanced detection capability. The F1-score improvement indicates that the model is more effective in maintaining equilibrium between false positives and false negatives, a critical requirement in safety-sensitive scenarios like SWaT. The AUC value of 0.742 further supports the model's stable discrimination ability across thresholds, despite fluctuations in input patterns. The use of adversarially generated anomaly patterns helps expand the detection coverage, even though the diversity of industrial anomalies presents additional modeling challenges.

Overall, although the performance gains are not as significant as on the Alibaba Cluster Trace dataset, the proposed method demonstrates consistent and reliable behavior. The results suggest that while microservice-oriented generative models may require additional adaptation for cyber-physical domains, the integration of multi-scale feature generation and adaptive thresholding still contributes to robust anomaly identification in complex, sensor-driven environments.

4) Hyperparameter sensitivity experiment results

This paper further tests the experimental results of hyperparameter sensitivity, mainly conducting different analyses on learning rates and optimizers, and the dataset used is the Alibaba Cluster Trace 2018 dataset. First, the experimental results of different learning rates are given, as shown in Table 3.

Table 3: Hyperparameter sensitivity experiment results(Learning Rate)

Learning Rate	**Acc(%)**	**AUC**	**F1-Score**
0.004	87.6	0.903	0.796
0.003	89.2	0.914	0.815
0.002	90.7	0.926	0.827
0.001	91.3	0.931	0.835

The results shown in Table 3 illustrate the sensitivity of the proposed model to different learning rate settings. When the learning rate is set relatively high (e.g., 0.004), the model exhibits unstable convergence behavior, leading to lower accuracy (87.6%) and reduced AUC and F1-score. This is likely due to overshooting during optimization, which prevents the generator and discriminator from reaching a stable adversarial equilibrium and negatively impacts the reconstruction quality in the anomaly detection module.

As the learning rate decreases, performance steadily improves across all evaluation metrics. At 0.002 and 0.003, the model achieves balanced training dynamics, enabling both CMSF-GAN and ATTAE to learn more representative features and stable temporal patterns. The gains in AUC and F1-score suggest that the model becomes more capable of distinguishing subtle anomalies while maintaining robustness against false positives.

The best performance is achieved at a learning rate of 0.001, where the accuracy reaches 91.3% and the F1-score peaks at 0.835. This indicates that the model benefits from more refined gradient updates, allowing both modules to co-adapt effectively. The result confirms that a moderately low learning rate contributes to the stability of adversarial training and enhances temporal encoding precision, making it the optimal choice for the proposed framework in this experimental setting.

Furthermore, the experimental results of the optimizer are given, as shown in Table 4.

Table 4: Hyperparameter sensitivity experiment results(Optimizer)

Optimizer	**Acc(%)**	**AUC**	**F1-Score**
AdaGrad	86.1	0.889	0.775
SGD	84.7	0.874	0.761
Adam	89.8	0.917	0.819
AdamW	91.3	0.931	0.835

The results presented in Table 4 demonstrate the impact of different optimizers on the performance of the proposed model. It is observed that traditional optimizers such as SGD and AdaGrad yield relatively lower accuracy and F1-scores, indicating that simple gradient descent or early-stage adaptive learning is insufficient for handling the complex optimization landscape of the CMSF-GAN and ATTAE modules. The lack of effective momentum or sophisticated adaptive mechanisms results in unstable training dynamics and suboptimal feature learning.

Using Adam leads to a notable improvement across all evaluation metrics, with the model achieving an accuracy of 89.8% and an F1-score of 0.819. This highlights the advantage of adaptive moment estimation in stabilizing both the generator-discriminator interplay and the temporal encoding-decoding process.

The best performance is achieved when using AdamW as the optimizer, reaching 91.3% accuracy and an F1-score of 0.835. The weight decay decoupling strategy in AdamW further prevents overfitting by ensuring better regularization during training, which is particularly critical for adversarial learning settings. These results confirm that selecting an appropriate optimizer plays a significant role in enhancing the overall effectiveness and robustness of the proposed anomaly detection framework.

5) Experiment on loss function changing with epoch

In the visualization experiment section, this paper first gives the images of the loss functions of training and verification as the epoch changes.

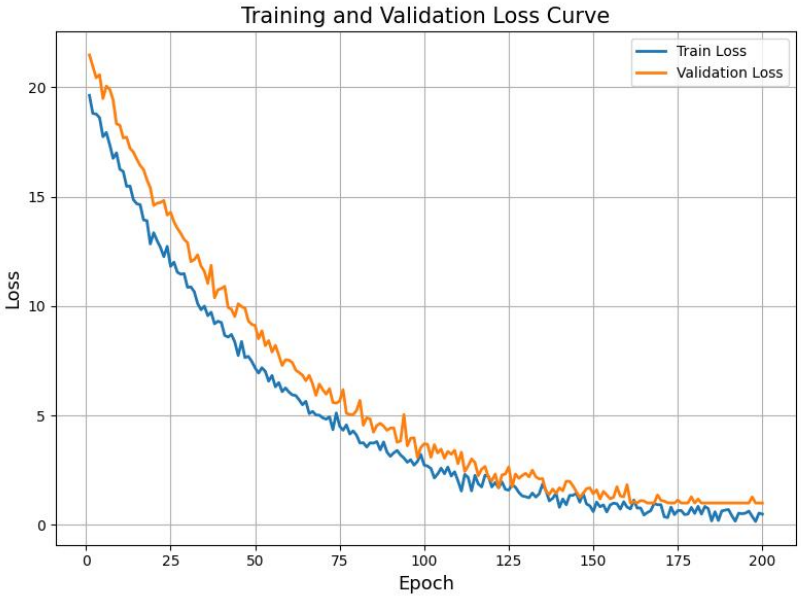

Figure 4. Training and validation loss functions

The training and validation loss curves shown in Figure 4 demonstrate a stable and consistent convergence process over the 200 training epochs. Initially, both losses start at relatively high values above 20, indicating a large reconstruction error at the beginning of training. However, within the first 50 epochs, both curves exhibit a sharp decline, suggesting that the model quickly captures the dominant patterns in the data and begins to reconstruct sequences more accurately.

As the training progresses, the loss values for both training and validation continue to decrease, but at a slower rate, eventually stabilizing around epoch 150. The gap between the two curves remains narrow throughout the process, indicating that the model maintains a strong generalization capability and does not suffer from overfitting. This is particularly important in anomaly detection tasks, where excessive fitting to normal data can reduce sensitivity to subtle anomalies.

By the end of training, both training and validation losses settle near 0.1, representing a significant improvement from the initial state. This result confirms the effectiveness of the proposed framework in learning meaningful representations of the normal behavior and adapting well to unseen data. The smooth convergence pattern and final loss values reflect the robustness of both the CMSF-GAN generation process and the ATTAE anomaly detection mechanism.

6) Experiment on loss function changing with epoch

Next, this paper also gives a robustness test under different data perturbation intensities, and the experimental results are shown in Figure 5.

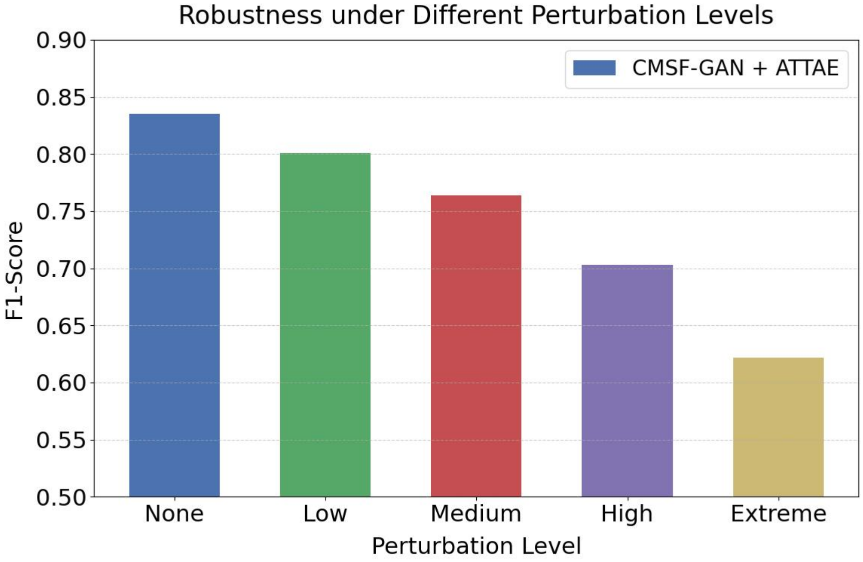

Figure 5. Robustness test experimental results under different data perturbation intensities

The experimental results shown in Figure 5 illustrate the robustness of the proposed CMSF-GAN + ATTAE framework under varying levels of data perturbation. When no perturbation is introduced, the model achieves its highest F1-score, reflecting optimal detection capability in clean and stable input environments. As minor perturbations are applied, such as slight noise or temporal jitter, the performance exhibits a modest decline, but remains within an acceptable range, indicating a degree of inherent tolerance to low-level disruptions.

As the perturbation intensity increases to medium and high levels, the F1-score continues to drop, suggesting that the model's ability to distinguish between normal and anomalous patterns becomes more challenged. This trend highlights the difficulty of maintaining reconstruction accuracy and anomaly discrimination when signal characteristics deviate significantly from the original distribution. The impact of high perturbation is especially evident in temporal models like ATTAE, where even subtle sequence distortion may lead to cumulative reconstruction errors.

Under extreme perturbation, the model performance degrades more significantly, with the F1-score falling below 0.65. This result indicates that while the framework exhibits strong robustness in mild to moderate disturbance scenarios, its effectiveness diminishes when exposed to severe and highly irregular input distortions. Nevertheless, the gradual degradation pattern also demonstrates that the model degrades gracefully rather than abruptly, which is desirable in real-world systems where unpredictable perturbations may occur.

7) Experiment on migration capability of cross-scenario data

Finally, this paper presents an experiment on the model's migration ability on cross-scenario data.

The results illustrated in Figure 6 demonstrate how the proposed model responds to increasing levels of transfer difficulty across different scenarios. In all three subplots—A to B, A to C, and A to D—the F1-score shows a consistent downward trend as the difficulty of domain migration increases from Low to Extreme. This decline reflects the expected challenge of generalizing learned representations to new environments with differing data distributions, especially under severe distribution shifts.

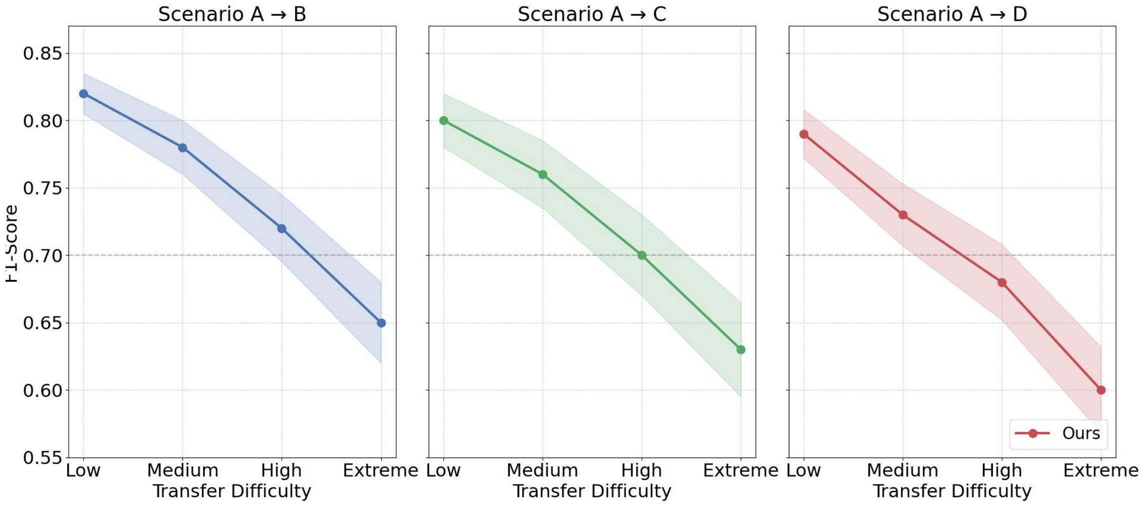

Figure 6. Experiment on migration capability of cross-scenario data

Despite the decreasing trend, the performance degradation is smooth rather than abrupt, and the model maintains relatively high F1-scores under Low and Medium transfer conditions across all scenarios. This suggests that the combination of CMSF-GAN and ATTAE retains a level of generalizability and robustness when faced with moderate domain shifts. The presence of the shaded confidence bands further illustrates that while there is inherent variability in model behavior under transfer, the variance remains controlled and stable.

The gap between scenarios also highlights the relative difficulty of each transfer path, with A to D presenting the steepest decline and lowest final score. This implies that scenario D introduces more complex or unfamiliar patterns that challenge the model's capacity to detect anomalies reliably. Overall, the results validate the model's capacity to handle cross-scenario adaptation while emphasizing the importance of improving robustness under high transfer difficulty settings.

5. Conclusion

This paper proposes a novel anomaly detection framework that integrates a conditional multi-scale feature enhanced generative adversarial network (CMSF-GAN) with an adaptive thresholding temporal autoencoder

(ATTAE). The proposed method addresses two major challenges in microservice-based distributed systems: the scarcity of high-quality anomalous data and the difficulty of detecting subtle or complex temporal anomalies. By combining synthetic anomaly generation with dynamic, context-aware detection, the framework enhances both the breadth of test coverage and the precision of anomaly identification.

Extensive experiments on two representative datasets demonstrate that the proposed model outperforms a range of state-of-the-art baselines in terms of accuracy, robustness, and generalization. In particular, the use of GAN-generated data effectively improves the resilience of the detection model under diverse and unseen scenarios. The model exhibits strong performance not only under clean conditions but also in the presence of perturbations and across different domain environments, indicating its potential for deployment in real-world, large-scale systems.

Beyond its empirical advantages, the framework also offers practical value for system reliability engineering, security auditing, and intelligent monitoring. Its modularity and compatibility with real-time data streams make it suitable for integration into modern DevOps pipelines and self-healing architectures. The ability to proactively simulate and evaluate system resilience against various abnormal conditions represents a significant step forward in the automation of infrastructure risk management and anomaly response.

Future work may focus on expanding the framework's applicability to other domains, such as industrial control systems, cloud-native security platforms, and edge-computing environments. Additionally, further enhancements in the generative component—such as introducing multi-modal or graph-structured anomaly simulation — may further improve detection granularity and interpretability. The methods and insights proposed in this paper provide a strong foundation for advancing intelligent anomaly handling in complex, high-volume operational systems.

References

[1] Ikram A, Chakraborty S, Mitra S, et al. Root cause analysis of failures in microservices through causal discovery[J]. Advances in Neural Information Processing Systems, 2022, 35: 31158-31170.

[2] R. Xin, P. Chen, Z. Zhao, Causalrca: Causal inference based precise fine-grained root cause localization for microservice applications, J. Syst. Softw. 203 (2023) 111724.

[3] P. Chen, H. Liu, R. Xin, T. Carval, J. Zhao, Y. Xia, Z. Zhao, Effectively detecting operational anomalies in large-scale iot data infrastructures by using a gan-based predictive model, Comput. J. 65 (11) (2022) 2909–2925.

[4] Thanigaivelan, Nanda Kumar, et al. "Distributed internal anomaly detection system for Internet-of-Things." 2016 13th IEEE annual consumer communications & networking conference (CCNC). IEEE, 2016.

[5] R. Zhang, J. Chen, Y. Song, W. Shan, P. Chen, Y. Xia, An effective transformation encoding-attention framework for multivariate time series anomaly detection in IoT environment, Mob. Netw. Appl. (2023) 1–13.

[6] Y. Song, R. Xin, P. Chen, R. Zhang, J. Chen, Z. Zhao, Autonomous selection of the fault classification models for diagnosing microservice applications, Future Gener. Comput. Syst. (2023).

[7] A.A. Cook, G. Mısırlı, Z. Fan, Anomaly detection for IoT time-series data: A survey, IEEE Internet Things J. 7 (7) (2019) 6481–6494.

[8] L. Mariani, C. Monni, M. Pezzé, O. Riganelli, R. Xin, Localizing faults in cloud systems, in: 2018 IEEE 11th International Conference on Software Testing, Verification and Validation, ICST, IEEE, 2018, pp. 262–273.

[9] R. Xin, H. Liu, P. Chen, Z. Zhao, Robust and accurate performance anomaly detection and prediction for cloud applications: a novel ensemble learning-based framework, J. Cloud Comput. 12 (1) (2023) 1–16.

[10]X. Zhou, X. Peng, T. Xie, J. Sun, C. Ji, W. Li, D. Ding, Fault analysis and debugging of microservice systems: Industrial survey, benchmark system, and empirical study, IEEE Trans. Softw. Eng. 47 (2) (2018) 243–260.

[11]Guo, Rui, et al. "Synthesising realistic 2D microstructures of unidirectional fibre-reinforced composites with a generative adversarial network." Composites Science and Technology 250 (2024): 110539.

[12]Dang, Qianlong, et al. "A generative adversarial networks model based evolutionary algorithm for multimodal multi-objective optimization." IEEE Transactions on Emerging Topics in Computational Intelligence (2024).

[13]Fokina, D., Muravleva, E., Ovchinnikov, G., & Oseledets, I. (2020). Microstructure synthesis using style-based generative adversarial networks. Physical Review E, 101(4), 043308.

[14]Zhang, Yu, and Lin Zhang. "A generative adversarial network approach for removing motion blur in the automatic detection of pavement cracks." Computer-Aided Civil and Infrastructure Engineering 39.22 (2024): 3412-3434.

[15]Lin, Lei, et al. "SeisGAN: Improving seismic image resolution and reducing random noise using a generative adversarial network." Mathematical Geosciences 56.4 (2024): 723-749.

[16]Waxenegger-Wilfing, G., Sengupta, U., Martin, J., Armbruster, W., Hardi, J., Juniper, M., & Oschwald, M. (2021). Early detection of thermoacoustic instabilities in a cryogenic rocket thrust chamber using combustion noise features and machine learning. Chaos: An Interdisciplinary Journal of Nonlinear Science, 31(6).

[17]Sengupta, U., Waxenegger-Wilfing, G., Martin, J., Hardi, J., & Juniper, M. P. (2022). Forecasting thermoacoustic instabilities in liquid propellant rocket engines using multimodal Bayesian deep learning. International Journal of Spray and Combustion Dynamics, 14(3-4), 218-228.

[18]Giannelli, Michele Faucci, and Rui Zhang. "CaloShowerGAN, a generative adversarial network model for fast calorimeter shower simulation." The European Physical Journal Plus 139.7 (2024): 597.

[19]Kobayashi, T., Murayama, S., Hachijo, T., & Gotoda, H. (2019). Early detection of thermoacoustic combustion instability using a methodology combining complex networks and machine learning. Physical Review Applied, 11(6), 064034.

[20]Shatnawi, Mo'ath, and Maram Bani Younes. "An enhanced model for detecting and classifying emergency vehicles using a generative adversarial network (GAN)." Vehicles 6.3 (2024): 1114-1139.

[21]Liu, Yang, et al. "Temporal Logical Attention Network for Log-Based Anomaly Detection in Distributed Systems." Sensors 24.24 (2024): 7949.

[22]Kench, S., & Cooper, S. J. (2021). Generating three-dimensional structures from a two-dimensional slice with generative adversarial network-based dimensionality expansion. Nature Machine Intelligence, 3(4), 299-305.

[23]Fan, Jiamin, et al. "Taking advantage of the mistakes: Rethinking clustered federated learning for iot anomaly detection." IEEE Transactions on Parallel and Distributed Systems (2024).

[24]Tian, Ying, et al. "Pyramid reconstruction assisted deep autoencoding Gaussian mixture model for industrial fault detection." Information Sciences 649 (2023): 119682.

[25]Musa, Nura Shifa, et al. "machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions." IEEE Access 12 (2024): 17982-18011.

[26]Li, D., Chen, D., Jin, B., Shi, L., Goh, J., & Ng, S. K. (2019, September). MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks. In International conference on artificial neural networks (pp. 703-716). Cham: Springer International Publishing.

[27]Su, Ya, et al. "Robust anomaly detection for multivariate time series through stochastic recurrent neural network." Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining. 2019.

[28]Ding, Kaize, et al. "Few-shot network anomaly detection via cross-network meta-learning." Proceedings of the web conference 2021. 2021.

[29]Audibert, Julien, et al. "Usad: Unsupervised anomaly detection on multivariate time series." Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining. 2020.

[30]Chen, Yang, Junzhe Zhang, and Chai Kiat Yeo. "Network anomaly detection using federated deep autoencoding gaussian mixture model." International Conference on Machine Learning for Networking. Cham: Springer International Publishing, 2019.