Contrastive Learning for Time-Series Anomaly Detection in IoT

QiPingZhi Xiao
m202472199@hust.edu.cn
School of Cyber Science and Engineering, Huazhong University of Science and Technology
Wuhan, Hubei, China

Abstract

The Internet of Things (IoT) generates vast time-series data from interconnected devices, where anomalies may indicate critical failures, cyber threats, or operational inefficiencies. Despite advances in anomaly detection, challenges persist due to complex temporal patterns, scarcity of labeled anomalies, and intricate dependencies in multivariate data. Traditional unsupervised methods often fail to capture temporal dynamics or suffer from high computational costs, while deep learning approaches struggle with representation consistency across domains. In this work proposes a Time-Frequency Transformer Model for multivariate time-series anomaly detection, leveraging dual-path reconstruction in time and frequency domains to exploit the inherent instability of anomalous patterns. Key innovations include: (1) a cross-domain reconstruction error analysis to enhance anomaly discrimination, (2) a multi-perspective contrastive learning mechanism for robust feature representation, and (3) a hierarchical loss aggregation strategy that computes stage-wise reconstruction errors for improved sensitivity.Extensive experiments on univariate and multivariate datasets demonstrate that our model surpasses state-of-the-art baselines, achieving superior detection performance. The framework's ability to integrate temporal and spectral insights offers broad applicability in IoT domains, from infrastructure monitoring to predictive maintenance.

Keywords

Contrastive learning, time Series, anomaly Detection, internet of Things

ACM Reference Format:
QiPingZhi Xiao. 2025. Contrastive Learning for Time-Series Anomaly Detection in IoT. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX)*. ACM, New York, NY, USA, 5 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

The Internet of Things (IoT) has become a cornerstone of modern industry and everyday life, enabling seamless connectivity among computing devices, mechanical systems, and digital machines. These interconnected devices, each assigned unique identifiers, autonomously collect and transmit data across networks, generating time-series signals that reflect system dynamics. Despite their widespread adoption, IoT systems remain susceptible to various security risks and operational vulnerabilities.

Anomalies in IoT data can arise from unexpected technical malfunctions, human errors, or malicious intrusions, potentially disrupting system stability and leading to service failures. For instance, in a distributed server environment, real-time monitoring of performance metrics—such as user traffic, CPU utilization, and memory consumption—is essential. The presence of outliers in these metrics may signal cyber threats or system inefficiencies, underscoring the importance of anomaly detection in maintaining operational integrity and cybersecurity.

Similarly, in industrial IoT applications, sensor anomalies often indicate critical failures requiring immediate intervention. Consider a water distribution (WADI) system equipped with sensors to monitor water quality. Anomalous readings during disinfection could suggest hazardous chlorine levels, necessitating rapid alerts to prevent health risks. Thus, time-series anomaly detection has emerged as a vital tool across IoT domains, including infrastructure management, health monitoring, and predictive maintenance.

Although anomaly detection techniques have broad applicability, achieving precise anomaly identification in complex time-series data still faces several critical challenges.First, time-series data often exhibit multiple intricate patterns, including but not limited to seasonality, trends, and periodicity. Effectively distinguishing these patterns while accurately detecting anomalies within them remains a significant difficulty. Second, anomalous events are inherently rare in real-world scenarios, making it challenging to obtain sufficient high-quality labeled training data. This scarcity hinders the development of robust supervised learning models. Third, the temporal and feature-wise dependencies embedded in time-series data must be carefully considered. The ability of an anomaly detection model to properly capture and process these dependencies is crucial for reliable performance.

Anomalous data exhibits two inherent characteristics that make detection challenging: its scarcity compared to normal data and its concealment within large volumes of regular observations. To address the scarcity of both labeled anomalies and anomaly examples, researchers have developed numerous unsupervised learning approaches.These conventional unsupervised methods employ diverse strategies for distinguishing normal patterns from anomalies and have demonstrated reasonable effectiveness. However, they suffer from three critical limitations: (1) failure to account for temporal dependencies in time-series data, (2) high computational complexity when processing large-scale datasets, and (3) heightened sensitivity to parameter configurations. These constraints ultimately restrict their detection performance and practical applicability.Unsupervised approaches extend beyond conventional machine learning methods, with numerous deep learning models now

Conference acronym 'XX, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/2025/05
https://doi.org/XXXXXXX.XXXXXXX

employing unsupervised techniques for time-series anomaly detection. These methods share a common underlying principle: they exploit dual perspectives to create significant divergence between normal and anomalous data in either feature space representation or reconstruction outcomes, thereby enabling effective anomaly discrimination.

Inspired by these approaches, we observe that normal samples maintain representation consistency during multi-perspective feature learning and reconstruction, while anomalous samples exhibit unstable cross-dimensional representations due to their inherent pattern instability, making it difficult to achieve consistent or approximate reconstruction results. Furthermore, according to the uncertainty principle of time series representation, anomaly data that demonstrates significant representational advantages in either the time or frequency domain typically fails to maintain comparable performance in the corresponding counterpart domain.Building upon these insights, this paper proposes a Time-Frequency Transformer Based Model for Multivariate Time Series Anomaly Detection. The model simultaneously performs feature representation and reconstruction in both time and frequency domains, effectively capturing anomalies by comparing the discrepancies between reconstruction results across these dual domains.Notably, our approach introduces a significant improvement over conventional methods that only compute reconstruction loss at the final stage. Instead, we implement a stage-wise loss aggregation mechanism that calculates and averages the reconstruction loss at each processing stage. This enhancement has demonstrably improved the model's overall performance.

In summary, the contributions of our work are as follows.

- We propose a novel anomaly detection framework that effectively integrates time-domain and frequency-domain information. The model performs dual-path reconstruction from both temporal and spectral perspectives, enabling accurate discrimination between normal and anomalous patterns through cross-domain reconstruction error analysis.
- We develop a multi-perspective contrastive learning mechanism that systematically compares temporal and spectral representations. This approach facilitates comprehensive exploration of feature extraction across different data modalities.
- We introduce a hierarchical reconstruction loss aggregation strategy that computes and averages mean squared errors at each processing stage. This novel loss computation method significantly enhances the model's detection capability by capturing multi-scale reconstruction discrepancies.
- Extensive experimental results demonstrate that our model outperforms existing baseline methods across multiple univariate and multivariate datasets, establishing new state-of-the-art performance benchmarks.

2 Related Work

2.1 Prediction-Based Anomaly Detection Models

The fundamental principle of prediction-based anomaly detection models involves training models on historical data to forecast future values, with anomalies identified through discrepancies between predicted and observed time series. Data points exhibiting deviations beyond a predefined threshold are classified as anomalous.Several notable approaches have advanced this paradigm: THOC employs multi-scale dilated convolutional recurrent neural networks with skip connections to capture temporal dynamics, coupled with a hierarchical clustering process that generates multiple hyperspheres to define its novel Multiscale Vector Data Description objective [9]. Hundman et al. developed an LSTM-based forecasting model integrated with an unsupervised, parameter-free thresholding technique for monitoring anomalies in spacecraft telemetry data [2]. Ren et al. designed a hybrid algorithm combining Spectral Residual (SR) analysis with Convolutional Neural Networks (CNNs) for anomaly detection in Microsoft service operations [8]. Ahmad et al. proposed a Hierarchical Temporal Memory (HTM) model, an unsupervised online sequence memory algorithm for real-time anomaly detection in data streams [1]. While prediction-based methods demonstrate strong performance in modeling temporal progression, they face two critical limitations: (1) susceptibility to noise and artifacts in historical training data, and (2) potential failure to detect non-conventional anomalies due to their rigid definition of deviation patterns.

2.2 Reconstruction-Based Anomaly Detection Models

Reconstruction-based anomaly detection models typically employ an encoder-decoder architecture, where the encoder maps raw time series into a latent space representation and the decoder attempts to reconstruct the original sequence from this compressed form. Data points exhibiting reconstruction errors exceeding a predetermined threshold are identified as anomalies. The Variational Autoencoder (VAE) represents a fundamental reconstruction-based model, originally proposed as a directed probabilistic graphical model for efficient approximate inference and learning [4]. VAEs have found widespread application in various domains including denoising, data compression, and anomaly detection. Another notable approach, DAGMM (Deep Autoencoding Gaussian Mixture Model), performs unsupervised anomaly detection by generating low-dimensional representations and reconstruction errors through deep autoencoders [17]. Despite the prevalence of VAEs in reconstruction-based methods, significant variations exist in encoder design: Wang et al. employed simple Multilayer Perceptrons (MLPs) and Recurrent Neural Networks (RNNs) as encoders for air quality anomaly detection [13]. Zhang et al. developed a more sophisticated approach incorporating time-frequency analysis, using Temporal Convolutional Networks (TCNs) as primary encoder components to separately reconstruct temporal and spectral features, along with trend

and residual components [16]. While these methods have demonstrated promising results, most existing approaches focus exclusively on time-domain modeling, neglecting the potentially valuable information contained in frequency-domain representations. This limitation may restrict their ability to detect certain types of anomalies that manifest more clearly in the spectral domain.

2.3 Transformer-Based Anomaly Detection Models

Since its inception, the Transformer architecture has achieved remarkable success in natural language processing and has subsequently been widely adopted in computer vision applications. Recently, an increasing number of Transformer-based models are being applied to time series tasks. Several notable Transformer-based approaches have advanced time series anomaly detection: The Anomaly Transformer introduces a novel Anomaly-Attention mechanism that simultaneously models prior associations and sequential relationships to capture association discrepancies, effectively distinguishing between normal and anomalous patterns [15]. Nam et al. proposed a nested window approach combining external and internal windows to align anomaly scores from time-domain and frequency-domain reconstructions, enabling more precise identification of abnormal pattern boundaries [7]. TranAD developed a two-stage encoder-decoder architecture stabilized through adversarial training, significantly improving reconstruction performance [10]. AnomalyBert addressed the scarcity of real-world anomalies by proposing four distinct degradation methods to synthesize anomalous patterns, effectively augmenting training data for rare anomaly cases [3].

2.4 Time Series Anomaly Detection Models Based on Time Domain Analysis

Time series data typically exhibit multiple complex temporal patterns, where decomposition techniques play a crucial role in extracting distinct components to facilitate deeper understanding and analysis of temporal characteristics. Recent advances have demonstrated the effectiveness of decomposition-based approaches in anomaly detection: Lei et al. developed a novel deep learning framework that integrates time series decomposition with spectral analysis for enhanced anomaly detection [5]. Autoformer introduced an innovative inner decomposition block that endows deep forecasting models with inherent progressive decomposition capabilities [14]. MICN validated the necessity and effectiveness of separately modeling complex temporal patterns through multi-scale kernel decomposition of input data [12]. TFDNet proposed a specialized sequence decomposition method for long-horizon time series, significantly improving both prediction efficiency and robustness [6]. D3R presented a dynamic decomposition approach for long-period multivariate time series, effectively utilizing external information to overcome limitations of local sliding windows [11].

3 COMMENTS

3.1 Excessively long declarative sentences

The first comment addresses the issue of overly long declarative sentences (Figure 1). I think The sentence is too lengthy and somewhat confusing in its description. It is suggested that it be split into two clearer statements, for example: By implementing PSI protocols based on different algorithmic schemes, one can better understand them. Further, by comparing and analyzing these protocols in different application environments, one can maximize their value.

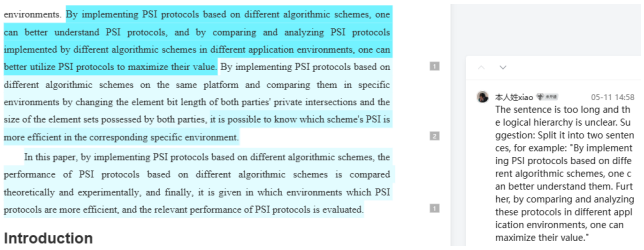

Figure 1: Excessively long declarative sentences

Similarly, the sentence is too long and repeats "cloud environment." (Figure 2) It is suggests that: Split it into two sentences, for example: PSI protocols have broad applications, including COVID-19 contact tracing, address book lookup, and blockchain. Additionally, cloud environments, as a key scenario for secure multiparty computation, heavily rely on PSI.

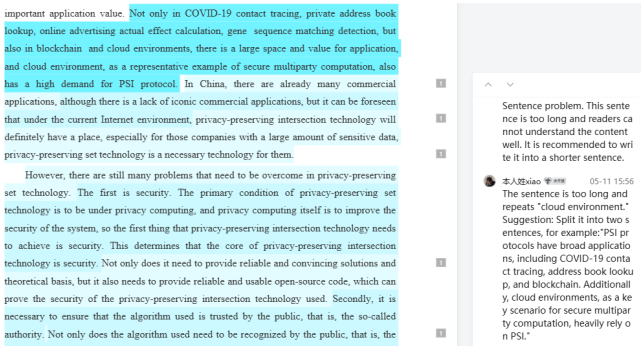

Figure 2: Excessively long declarative sentences and repeated words

3.2 Passive sentences

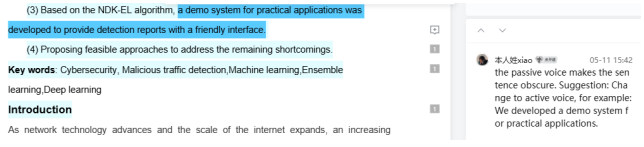

Figure 3: Passive sentences

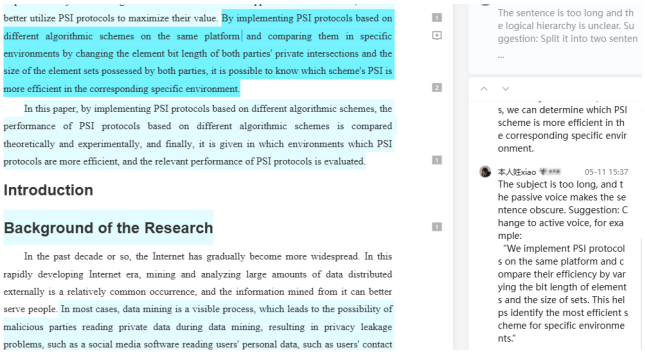

Figure 4: Passive sentences and subject is too long

An active sentence is better than a passive sentence, so this sentence (Figure 3) might be better stated this way: We developed a demo system for practical applications.

Similarly, the recommended way of passive and the subject is too long (Figure 4) is: We implement PSI protocols on the same platform and compare their efficiency by varying the bit length of elements and the size of sets. This helps identify the most efficient scheme for specific environments.

3.3 Use of punctuation

"Different countries and organizations have introduced laws and regulations to protect privacy data, and data privacy protection has long been a hot issue." I think it should replace the comma with a semicolon, i.e., "...privacy data; data privacy protection...", as the two parts are independent yet related clauses.

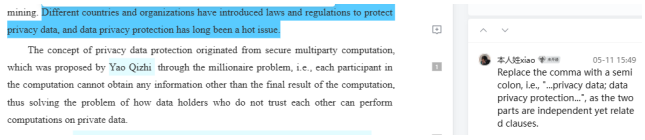

Figure 5: Use of punctuation

A term "machine learningbased" is missing a hyphen (Figure 6), resulting in incorrect word formation. The correct form should be "machine learning-based," so a hyphen needs to be added.

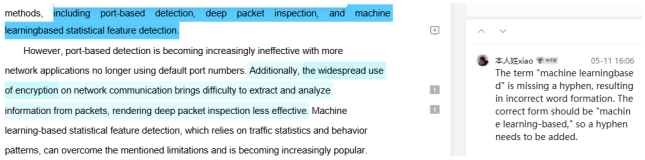

Figure 6: Use of punctuation

3.4 Confusing statements

The logical connection is unclear and confusing (Figure 7), as "through a technology" does not flow coherently with the main clause. I recommend rewriting this part of the sentence, for example: "Although China lacks iconic commercial applications of PSI, enterprises holding sensitive data urgently need this technology—it enables deep data mining while protecting privacy."

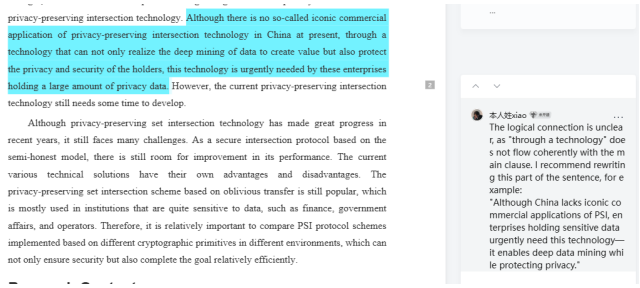

Figure 7: Confusing statements

3.5 Grammar errors

There is a grammatical error (Figure 8), 'the' should be added before the sentence.

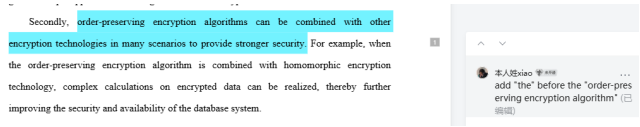

Figure 8: Grammar errors

Similarly, there is a grammatical error (Figure 9), 'the' should be added before the 'database security'.

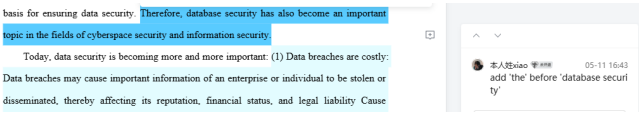

Figure 9: Grammar errors

3.6 Use of conjuctions

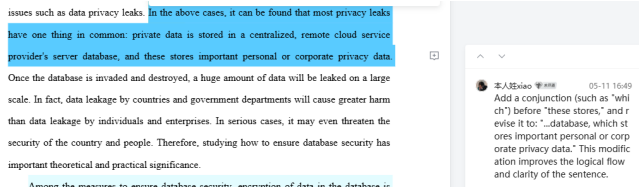

Figure 10: Use of conjuctions

Logical connection missing (Figure 10): The original sentence reads: "In the above cases, it can be found that most privacy leaks have one thing in common: private data is stored in a centralized, remote cloud service provider's server database, and these stores

important personal or corporate privacy data." Suggestion: Add a conjunction (such as "which") before "these stores," and revise it to: "...database, which stores important personal or corporate privacy data." This modification improves the logical flow and clarity of the sentence.

References

[1] Subutai Ahmad, Alexander Lavin, Scott Purdy, and Zuha Agha. 2017. Unsupervised real-time anomaly detection for streaming data. *Neurocomputing* 262 (2017), 134–147.

[2] Kyle Hundman, Valentino Constantinou, Christopher Laporte, Ian Colwell, and Tom Soderstrom. 2018. Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding. In *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*. 387–395.

[3] Yungi Jeong, Eunseok Yang, Jung Hyun Ryu, Imseong Park, and Myungjoo Kang. 2023. Anomalybert: Self-supervised transformer for time series anomaly detection using data degradation scheme. *arXiv preprint arXiv:2305.04468* (2023).

[4] Diederik P Kingma, Max Welling, et al. 2013. Auto-encoding variational bayes.

[5] Tianyang Lei, Chang Gong, Gang Chen, Mengxin Ou, Kewei Yang, and Jichao Li. 2023. A novel unsupervised framework for time series data anomaly detection via spectrum decomposition. *Knowledge-Based Systems* 280 (2023), 111002.

[6] Yuxiao Luo, Songming Zhang, Ziyu Lyu, and Yuhan Hu. 2025. Tfdnet: Time-frequency enhanced decomposed network for long-term time series forecasting. *Pattern Recognition* (2025), 111412.

[7] Youngeun Nam, Susik Yoon, Yooju Shin, Minyoung Bae, Hwanjun Song, Jae-Gil Lee, and Byung Suk Lee. 2024. Breaking the time-frequency granularity discrepancy in time-series anomaly detection. In *Proceedings of the ACM Web Conference 2024*. 4204–4215.

[8] Hansheng Ren, Bixiong Xu, Yujing Wang, Chao Yi, Congrui Huang, Xiaoyu Kou, Tony Xing, Mao Yang, Jie Tong, and Qi Zhang. 2019. Time-series anomaly detection service at microsoft. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining*. 3009–3017.

[9] Lifeng Shen, Zhuocong Li, and James Kwok. 2020. Timeseries anomaly detection using temporal hierarchical one-class network. *Advances in neural information processing systems* 33 (2020), 13016–13026.

[10] Shreshth Tuli, Giuliano Casale, and Nicholas R Jennings. 2022. Tranad: Deep transformer networks for anomaly detection in multivariate time series data. *arXiv preprint arXiv:2201.07284* (2022).

[11] Chengsen Wang, Zirui Zhuang, Qi Qi, Jingyu Wang, Xingyu Wang, Haifeng Sun, and Jianxin Liao. 2023. Drift doesn't matter: dynamic decomposition with diffusion reconstruction for unstable multivariate time series anomaly detection. *Advances in Neural Information Processing Systems* 36 (2023), 10758–10774.

[12] Huiqiang Wang, Jian Peng, Feihu Huang, Jince Wang, Junhui Chen, and Yifei Xiao. 2023. Micn: Multi-scale local and global context modeling for long-term series forecasting. In *The eleventh international conference on learning representations*.

[13] Ziyu Wang, Jingjing Feng, Qingyan Fu, Song Gao, Xiaojia Chen, and Jinping Cheng. 2019. Quality control of online monitoring data of air pollutants using artificial neural networks. *Air Quality, Atmosphere & Health* 12 (2019), 1189–1196.

[14] Haixu Wu, Jiehui Xu, Jianmin Wang, and Mingsheng Long. 2021. Autoformer: Decomposition transformers with auto-correlation for long-term series forecasting. *Advances in neural information processing systems* 34 (2021), 22419–22430.

[15] Jiehui Xu, Haixu Wu, Jianmin Wang, and Mingsheng Long. 2021. Anomaly transformer: Time series anomaly detection with association discrepancy. *arXiv preprint arXiv:2110.02642* (2021).

[16] Chaoli Zhang, Tian Zhou, Qingsong Wen, and Liang Sun. 2022. Tfad: A decomposition time series anomaly detection architecture with time-frequency analysis. In *Proceedings of the 31st ACM international conference on information & knowledge management*. 2497–2507.

[17] Bo Zong, Qi Song, Martin Renqiang Min, Wei Cheng, Cristian Lumezanu, Daeki Cho, and Haifeng Chen. 2018. Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In *International conference on learning representations*.

Received 20 February 2025; revised 12 March 2025; accepted 5 June 2025