International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

A Review and Experimental Framework for Precursor-of-Anomaly Detection in Time-Series Systems

Mr. Ashish Kumar, Dr. Satender Kumar
Department of Computer Science and Engineering
Quantum University, Roorkee, India

Abstract- — The study of anomaly detection in time series has become one of the key topics in intelligent monitoring systems such as industrial automation, cybersecurity, healthcare, finance, IoT. The traditional approaches to anomaly detection primarily focused on detecting any signs of anomalous behaviour following their occurrence. However, in many cases, reactive anomaly detection does not allow for timely response to detected anomalies. Recently, some researchers have suggested the novel idea of Precursor-of-Anomaly (PoA) detection to detect and analyse warning signs prior to anomalies' occurrence. The present paper provides a review and experimental framework of PoA detection in time series. The paper outlines approaches to traditional anomaly detection, deep learning based forecasting models, uncertainty-aware models, and early warning approaches. Also, the paper outlines a practical framework of PoA analysis using industrial SWaT dataset and Isolation Forest approach. Experimental results prove that uncertainty-aware PoA detection is capable of delivering early warning signals before critical anomalies occur. The paper considers modern limitations and challenges in designing proactive anomaly prediction systems.

Keywords— Time-Series Analysis, Anomaly Detection, Precursor-of-Anomaly, Early Warning Systems, Artificial Intelligence, Forecasting Models, SWaT Dataset.

I. INTRODUCTION

The fast development of intelligent monitoring systems has been witnessed by the emergence of big amounts of time series data in different industries such as medicine, automation, finance, cybersecurity, transportation, and IoT systems. Effective monitoring of such systems is possible when one can detect unusual behaviour which could be a sign of failure, attack, fault, or instable working condition.

Anomaly detection is defined as the process of detecting unusual patterns of behaviour which deviate significantly from the norm in the system. The usual design of an anomaly detection system assumes that it works reactively, which means that its work involves detecting anomalies after their occurrence. Despite efficiency of such systems in monitoring systems, it is difficult to take measures in advance.

Thus, recently a new concept – precursor-of-anomaly (PoA) detection was suggested to solve this problem. The idea behind PoA detection is that one should find patterns that could become signs of upcoming anomalies before their occurrence. Unlike traditional systems, PoA systems are aimed at predicting future anomalies.

The notion of early warning systems becomes especially valuable when considering critical situations and critical environment. Prediction of equipment breakdown in industrial applications may lower operational time and repair costs. Proactive prediction of attack in cybersecurity can contribute to the security of the system before its compromise. Likewise, early detection of diseases and physiological anomalies in medical monitoring may increase their accuracy.

Recent advances in artificial intelligence and deep learning have significantly influenced PoA detection research. Such methods as neural controlled differential equations, transformer architecture, uncertainty-based forecasting methods, and assembling have been proven to perform well at anomaly prediction tasks.

The principal goals of the paper are as follows:

- Reviewing classical anomaly detection approaches.
- Analysing contemporary PoA detection techniques.
- Proposing experimental PoA detection framework.
- Evaluating precursor detection on SWaT dataset.
- Presenting future research directions on proactive monitoring systems.

Objectives of the Study
The primary objectives of this research paper are as follows:

- To review traditional anomaly detection techniques used in time-series monitoring systems.
- To analyze modern Precursor-of-Anomaly (PoA) detection frameworks such as PAD and FATE.
- To design an uncertainty-aware proactive monitoring framework for early anomaly prediction.
- To evaluate precursor detection capability using the industrial SWaT dataset.
- To study the role of forecasting uncertainty and instability in predicting future anomalies.
- To identify current challenges and future research directions in proactive anomaly detection systems.

II. TRADITIONAL ANOMALY DETECTION METHODS

1. Statistical Approaches
Traditional anomaly detection approaches mainly made use of statistical approaches. Statistical anomaly detection algorithms work under the assumption that normal behaviour of the system is defined by some known probability distribution. Instances that diverge from expected probability distribution are anomalies.

Some of the popular statistical approaches used are:

Gaussian Distribution
Z-Score Method
Moving Average
Bayesian Models

However, while statistical approaches are relatively fast, they are ineffective in dealing with multidimensional and non-linear time series data.

2. Machine Learning-Based Methods
Machine learning technology greatly enhanced the anomaly detection process due to the ability of machines to learn complicated patterns in the data directly.
Some of the most commonly used machine learning techniques are:

- Isolation Forest
- Local Outlier Factor (LOF)
- One-Class Support Vector Machine (OCSVM)
- Clustering-based Detection

The Isolation Forest algorithm learns to isolate outliers using recursive partitioning.

The Local Outlier Factor technique estimates local density differences to detect outliers.

While machine learning techniques helped to improve anomaly detection, many systems were still reactive and did not have any prediction abilities.

3. Deep Learning Approaches
Deep learning algorithms showed impressive results for performing complex time-series anomaly detection.

Autoencoders
Autoencoders create a compressed latent space of the normal pattern and use reconstruction loss to perform anomaly detection.

Recurrent Neural Networks (RNN)
RNNs and LSTM networks can capture dependencies between events within time-series data.

Transformer-Based Models
Transformers enhanced long-term dependencies capturing by introducing self-attention mechanism.

Even though they performed well in detecting anomalies, most deep learning methods are more concerned about current anomalies than predicting anomalies in the future.

III. PRECURSOR-OF-ANOMALY DETECTION

1. Concept of PoA Detection
PoA Detection stands for the detection of signals or patterns indicating future anomalies.

Whereas classical anomaly detection systems work on detecting abnormalities after they occur, PoA detection systems try predicting them prior to any failures actually occurring.

A general PoA system operates in the following manner:

Input Time Series Data
→ Temporal Features Learning
→ Early Warning Signals Extraction
→ Anomalies Prediction in the Future

PoA detection is especially helpful in:

- predictive maintenance;
- industrial monitoring;
- healthcare monitoring;

- financial forecasting;
- cybersecurity systems.

2. PAD Framework

One of the early PoA frameworks was PAD (Precursor-of-Anomaly Detection for Irregular Time Series).

PAD established an integrated framework for performing both:

- Current anomalies detection
- Future anomalies prediction

This integrated framework is built upon the neural controlled differential equation model that captures the irregular time-series nature.

PAD utilized two evolving neural controlled differential equations models that were:

- Anomaly Detection NCDE
- PoA Detection NCDE

Furthermore, the PAD framework made use of:

- Multi-task learning
- Knowledge distillation
- Self-supervised learning

The PAD showed good results on irregular time-series environment with a downside of high computational complexity.

3. FATE Framework

FATE (Forecasting Anomalies with Time-Series Forecast Ensembles) proposed uncertainty aware anomaly precursors.

Contrary to PAD, FATE identifies anomaly precursors using forecasting uncertainty.

Steps involved in the process are as under:

Input Sequence

→ Forecasting Model Ensemble
→ Forecast Variance
→ Uncertainty Calculation
→ Precursors Prediction

The basic premise of FATE is:

Greater forecasting variance shows greater instability of the system

IV. METHODOLOGY

The proposed research methodology is a combination of review-based and experimental study on PoA detection in time-series systems.

In the beginning, an exhaustive literature review was performed to examine traditional anomaly detection techniques, deep learning solutions, as well as current state-of-the-art PoA detection frameworks such as PAD and FATE. Different papers in the IEEE, ACM, Springer, and Elsevier journals were analyzed in order to evaluate existing approaches for proactive anomaly detection.

As a result of literature review, the experimental methodology for precursor detection from industrial time-series dataset was established. The SWaT (Secure Water Treatment) dataset was chosen as it includes real-life sensor readings and attack labeling which can be used for anomaly prediction studies.

The experiment methodology includes several stages:

Data Collection

SWaT dataset including industrial time-series data was used for experiment.

Data Preprocessing

Numerical readings were scaled using Standard Scaler.

Feature Monitoring

Rolling variance uncertainty estimation was implemented in order to analyse the behaviour of sensors for detecting time-series instability.

Anomaly detection

Isolation Forest algorithm was used to perform detection of outliers within the time-series dataset.

Precursor signal generation

Uncertainty estimation and instability forecasting were applied for precursor signal generation.

Analysis of the results

The anomalies and the precursors created by the model have been studied.

Overall Workflow of the Proposed Methodology:

Sensor Data
→ Data Preprocessing
→ Feature Normalization
→ Uncertainty Estimation
→ Anomaly Detection using Isolation Forest
→ Precursor Alert Generation
→ Results Visualization

This methodology has the potential of combining anomaly detection and precursor estimation to provide proactive monitoring of industrial systems.

V. PROPOSED EXPERIMENTAL FRAMEWORK

The proposed framework combines anomaly detection and uncertainty-aware precursor analysis for proactive monitoring of industrial time-series systems. The primary objective of the framework is to identify instability patterns and warning signals before the occurrence of critical anomalies.

The framework integrates statistical uncertainty estimation with machine learning-based anomaly detection to improve early warning capability in intelligent monitoring environments such as industrial automation, IoT systems, healthcare monitoring, and cybersecurity applications.

The major components of the proposed framework are as follows:

- Acquisition of Sensor Data
- Data Preprocessing
- Feature Normalization
- Variance-Based Uncertainty Estimation
- Anomaly Detection using Isolation Forest
- Precursor Alert Generation
- Results Visualization and Analysis

The overall workflow of the proposed framework can be represented as:

Sensor Data
→ Data Preprocessing
→ Feature Normalization
→ Uncertainty Estimation
→ Isolation Forest Detection
→ Precursor Alert Generation
→ Visualization and Analysis

The proposed system continuously monitors the behaviour of sensor signals and analyses temporal instability using rolling variance estimation. Increased uncertainty in sensor behaviour is considered a possible indicator of future abnormal events.
The risk estimation function used in the framework is defined as:

RiskScore=αE_f+βU_p

Where:

- E_f= Forecasting Error
- U_p= Prediction Uncertainty
- $\alpha$and β= Weighting coefficients controlling contribution of forecasting error and uncertainty respectively.

The uncertainty estimation is calculated using rolling variance analysis:

$$U_p(t) = \frac{1}{w}\sum_{i=t-w}^{t}(x_i - \mu)^2$$

Where:

- $U_p(t)$= Prediction uncertainty at time (t)
- w= Rolling window size
- x_i= Sensor observation
- μ= Rolling mean of observations

A higher uncertainty value indicates greater instability within the monitored system. Such instability may act as a precursor signal before the occurrence of an anomaly.

For anomaly detection, the Isolation Forest algorithm is employed because of its efficiency in identifying outliers within high-dimensional time-series datasets. The algorithm isolates abnormal observations using recursive random partitioning of feature space.

The proposed framework combines:

- anomaly detection,
- forecasting instability,
- and uncertainty estimation

to generate proactive alerts before critical failures occur.Compared with traditional reactive anomaly detection systems, the proposed framework attempts to improve system reliability by enabling early warning generation and predictive monitoring capabilities.

Experimental Results
The proposed precursor-of-anomaly detection framework was experimentally evaluated using the SWaT industrial control system dataset. The objective of the experiment was to analyze whether uncertainty-aware monitoring could identify instability patterns before the occurrence of anomalous events. The dataset contained 54,621 industrial time-series instances and 53 sensor features representing different operational parameters of the water treatment system. During experimentation, the FIT101 sensor attribute was selected for

precursor analysis because of its continuous temporal behaviour and sensitivity to operational fluctuations.

The Isolation Forest algorithm was used to detect anomalous observations within the sensor stream, while rolling variance estimation was applied to monitor uncertainty and instability in the time-series data.

The following experimental observations were obtained:

Experimental Metric	Result
Total Dataset Instances	54,621
Total Features	53
Detection Algorithm	Isolation Forest
Uncertainty Technique	Rolling Variance
Total Detected Anomalies	1073
Total Detected Precursors	369

The results indicate that the proposed framework successfully identified abnormal behaviour al patterns within the industrial sensor data. A total of 1073 anomalies were detected by the Isolation Forest model, while 369 precursor alerts were generated using uncertainty-based rolling variance estimation. The experimental findings suggest that instability and fluctuation within sensor signals may act as precursor indicators before the occurrence of critical anomalies.

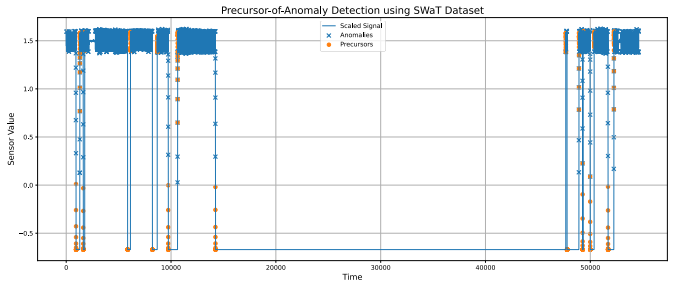

Figure 1 illustrates the visualization of the scaled sensor signal along with detected anomalies and precursor alerts generated by the proposed framework.

Figure 1. Precursor-of-Anomaly Detection using Isolation Forest and Rolling Variance on SWaT Dataset

The blue signal represents the normalized industrial sensor readings obtained from the SWaT dataset. Cross markers indicate anomalies detected by the Isolation Forest algorithm, whereas circular markers represent precursor alerts generated through rolling variance-based uncertainty estimation.

The visualization demonstrates that precursor alerts appear near several anomalous regions before complete anomaly manifestation. This behaviour indicates that uncertainty estimation can provide early warning capability in industrial monitoring systems.

The clustering of precursor points around anomalous regions suggests that instability in sensor behaviour may serve as an indicator of future abnormal events.

The proposed framework combines:

- anomaly detection,
- uncertainty estimation,
- and temporal instability analysis

to transform traditional reactive monitoring systems into proactive early warning systems.

Overall, the experimental evaluation confirms the feasibility of using uncertainty-aware precursor detection for intelligent industrial monitoring applications such as predictive maintenance, cyber-physical system security, and fault prediction.

Comparative Analysis

Method	Core Idea	Strength	Limitation
Isolation Forest	Outlier Isolation	Fast and Simple	Reactive
Autoencoder	Reconstruction Error	Learns Complex Features	Limited Prediction
LSTM	Sequential Learning	Temporal Modeling	Reactive Detection
PAD	NCDE-Based PoA	Irregular Time-Series Support	High Complexity
FATE	Forecast Uncertainty	Interpretable and Practical	Forecast Dependency
Proposed Framework	Uncertainty + Isolation Forest	Early Warning Capability	Threshold Sensitive

Issues and Future Directions for Research

While much progress has been made, there are still many issues that have yet to be solved.

Lack of Data
Anomalies are often infrequent events, making it hard to perform supervised learning.

False Positives
Alerting mechanisms can produce a large number of false alarms.

Computationally Intensive
Some methods like NCDEs can be computationally intensive.

Uninterpretable
The use of deep learning can often make models uninterpretable.

Future Research Directions
Future research can include the study of:

- Interpretable AI in predicting anomalies
- Federated anomaly detection
- Learning systems
- Forecasting precursors using transformers
- Multimodal industry monitoring
- Rewards-based alerting systems

VI. CONCLUSION

This paper outlined a literature review and experimental setup for Precursor of Anomaly detection within time-series systems. Conventional anomaly detection systems have mainly adopted a reactive approach, detecting anomalies only after the occurrence of abnormal events. Emerging systems, such as PAD and FATE, offered proactive ability to predict anomalies based on temporal analysis.

A proactive framework utilizing the industrial SWaT dataset along with the Isolation Forest technique was created for anomaly detection studies. Through experimental analysis, it was found that uncertainty-based precursor detection enables preemptive warnings about anomalies in industrial systems.
This research paper suggests that proactive anomaly prediction constitutes an important step towards intelligent monitoring systems. Future works will be directed toward developing adaptive, interpretable, and computation-efficient precursor detection systems.

REFERENCES

1. Chandola, V., Banerjee, A., & Kumar, V. Anomaly Detection: A Survey. ACM Computing Surveys, 2009.
2. Liu, F. T., Ting, K. M., & Zhou, Z. H. Isolation Forest. IEEE ICDM, 2008.
3. Breunig, M. et al. LOF: Identifying Density-Based Local Outliers. SIGMOD, 2000.
4. Hochreiter, S., & Schmidhuber, J. Long Short-Term Memory. Neural Computation, 1997.
5. Vaswani, A. et al. Attention is All You Need. NeurIPS, 2017.
6. Ruff, L. et al. Deep One-Class Classification. ICML, 2018.
7. Pang, G. et al. Deep Learning for Anomaly Detection: A Review. ACM Computing Surveys, 2021.
8. Jhin, S. Y., Lee, J., & Park, N. Precursor-of-Anomaly Detection for Irregular Time Series. KDD, 2023.
9. Goodfellow, I. et al. Deep Learning. MIT Press, 2016.
10. Aggarwal, C. Outlier Analysis. Springer, 2017.
11. Chalapathy, R., & Chawla, S. Deep Learning for Anomaly Detection: A Survey. arXiv, 2019.
12. Russell, S., & Norvig, P. Artificial Intelligence: A Modern Approach. Pearson, 2020.
13. Dosovitskiy, A. et al. An Image is Worth 16x16 Words. ICLR, 2021.
14. LeCun, Y., Bengio, Y., & Hinton, G. Deep Learning. Nature, 2015.
15. Mathur, A., et al. SWaT: A Water Treatment Testbed for Research and Training on ICS Security. 2016.