A Hybrid Approach of ConvLSTM-DT and GPT-4 for Real-time Anomaly Detection Decision Support in Edge-Cloud Environments

Radityo Fajar Pamungkas, Ida Bagus Krishna Yoga Utama, Khairi Hindriyandhito, Yeong Min Jang*

Department of Electronics Engineering, Kookmin University, Seoul, South Korea

Abstract

Anomaly detection is a critical requirement across diverse domains to promptly identify abnormal behavior. Conventional approaches often face limitations with uninterpretable anomaly detection results, impeding efficient decision-making processes. This paper introduces an innovative hybrid approach, the Convolutional Long Short-term Bayesian Neural Network with nonparametric dynamic thresholding (ConvLSTMBNN-DT), for prediction-based anomaly detection. Additionally, the model incorporates fine-tuned GPT-4 to provide human-interpretable explanations in edge-cloud environments.The method achieves outstanding performance with an F1-score and AUC of 0.91 and 0.84, respectively, on collected data, and successfully generates understandable decision support explanations.

Keywords: Anomaly detection, Large Language Models, ConvLSTM-DT, Human-understandable explanations, Dynamic thresholding

1. Introduction

The Internet of Things (IoT) has witnessed exponential growth, reflecting its pervasive impact on various industries. According to recent market reports **[ref: iot analytics]**, the global IoT market is grew by 18% in 2022 to 14.3 billion active endpoints. This surge is attributed to the widespread adoption of IoT in diverse sectors, notably smart factories and indoor air quality monitoring. Amidst this growth, the urgency for anomaly detection within IoT systems has become paramount. Anomaly detection plays a pivotal role in mitigating threats by identifying irregularities in data patterns, indicative of potential security breaches.

Recent studies indicate that the global market size for anomaly detection is predicted to grow with a compound annual growth rate exceeding 16% **[ref: marketsearchfuture]**. The benefits of implementing anomaly detection in IoT systems are profound, ranging from preemptive threat mitigation to enhanced system reliability. By identifying and addressing anomalies promptly, businesses can safeguard sensitive data and ensure the uninterrupted functionality of their IoT infrastructure, thereby fostering a secure and resilient technological landscape.

1.1. Related work

Several researchers have proposed different algorithms and methods to detect anomalies lies in time series in streaming scenarios. In recent studies, many researchers tend to use deep learning architecture for anomaly detection in time series due to its powerful data dependency modeling. There are two commonly used deep learning techniques which are prediction-based approaches, and reconstruction-based approaches. **[Ref: Hundman et al.]** demonstrated the combination of long short-term memory (LSTM) with nonparametric dynamic thresholding for detecting anomalies within telemetry data in rapid changing environment. **[Ref: Goh et al.]** proposed LSTM as predictor for learning the normal temporal behavior of the data, and subsequently using the Cumulative Sum method to identify anomaly behavior.

Reconstruction-based approaches, on the other hand, have also been acknowledged. Unlike prediction-based

*Corresponding author

Email addresses: radityofajar@gmail.com (Radityo Fajar Pamungkas), ibkyutama@ieee.org (Ida Bagus Krishna Yoga Utama), khairihindri@gmail.com (Khairi Hindriyandhito), yjang@kookmin.ac.kr (Yeong Min Jang)

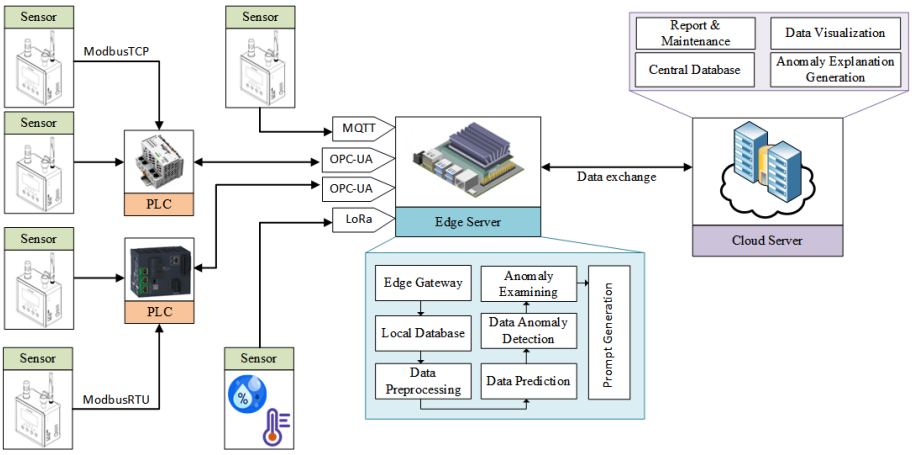

Figure 1. Overall Architecture of Real-time Anomaly Detection Decision Suppoer for Indoor Air Quality Data Monitoring

anomaly detection, these approaches involve recreating the original input through a latent low-dimension representation, ideal for capturing collective anomalies. In **Ref: Park, Yin, Nguyen, and Wei]**, the authors investigated a hybrid deep learning model that combines LSTM layer in the shape of autoencoder (AE) architecture to build reconstruction-based unsupervised anomaly detection.

While there has been extensive research on time series anomaly detection, the study that incorporates anomaly detection with an explanation for decision support has not been explored to a great extent. In **[Ref: Gilpin et al.]**, the author's work represents a pioneering effort that has introduced the emerging field of explanatory anomaly detection, particularly in the realm of system-level explanations through simulated semi-autonomous vehicles. Although previous research is comparable to this paper, the goal of this paper is to design real-time anomaly detection decision support in edge-cloud environments to increase the interpretability and efficiency of tackling anomaly situations. In contrast to previous studies, the anomaly detection algorithm in this article implements a Convolutional LSTM Bayesian neural network with nonparametric dynamic thresholding (ConvLSTMBNN-DT) that accurately forecasts future values and is robust against dynamic environments. Additionally, it employs a fine-tuned generative pre-training version-4 (GPT-4) that can generate human-understandable explanations and enhance interpretability to facilitate quick decision-making.

Therefore, the contributions of our proposed method are summarized as follows:

- We proposed a novel hybrid approach integrating ConvLSTMBNN-DT and Fine-tuned GPT-4 accurately detects point and contextual anomalies and effectively generates anomaly reasoning and possible solutions for decision support.
- The conventional schemes are commonly deployed in high power computing capability without considering resource-constraint devices and latency. In contrast, our proposed method deploys the model in edge-cloud environments, considering seamless and real-world edge-computing integrations. Therefore, low-latency anomaly detection on streaming data can be executed.
- Extensive experiments on generated IAQ datasets demonstrate the effectiveness of the proposed model. Our proposed model outperforms the others anomaly detection models in both F1-score and AUC metrics. Moreover, the proposed method can generate reliable decision support to enhance operation and maintenance system overall performance.

The rest of this paper is structured as follows: Section 2 describes the data preprocessing and methodology of the proposed approach. Section 3 presents the experiments settings to demonstrate the efficacy of our proposed method. Section 4 discusses the experiments results. Section 5 brings the conclusion and future work of this manuscript.

2. Methodology

This study proposes anomaly detection on indoor air quality monitoring and providing decision support. In

particular, we collect practical air quality data in an indoor setting using our developed IoT platform. The proposed architecture is shown in **Fig.1**. The edge server collects air quality data such as temperature, humidity, and particulate matter (PM) from several heterogeneous sensors in different rooms. In this study, we mainly focus to perform anomaly detection on three main features in IAQ data which are temperature, humidity, and PM $2.5\mu m$.

2.1. Data preprocessing

It is essential to implement several data processing techniques before training process to improve data quality. Utilizing Pearson's correlation coefficient, we perform feature selection based on a high correlation score.After this feature selection step, we apply the Z-score normalization technique to normalizing the data. This process helps stabilize the gradient descent during training, enabling the model to converge more rapidly.

2.2. ConvLSTM-PBNN

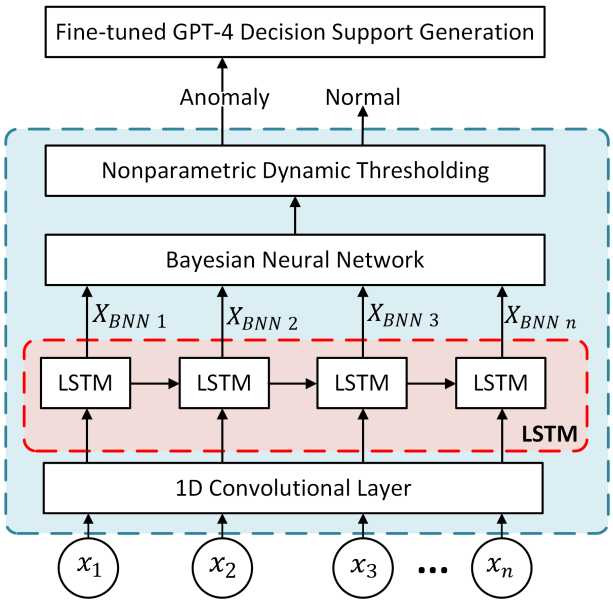

Figure 2. Architecture of ConvLSTMBNN-DT combine with GPT-4 for Anomaly Detection Decision Support

The prediction model plays an important role in this approach, where accurate forecasting indicates the normal behavior of the system itself. In this method, we modified the LSTM-BNN approach proposed by [Ref: Krishna], which demonstrates remarkable prediction performance compared to common existing models. Fig 3 illustrates the proposed ConvLSTMBNN architecture for the prediction model, followed by passing the output data into thresholding for further analysis and GPT-4 for decision support generation. Modifying the LSTM layer into ConvLSTM, with advantages enhancing the effectiveness of processing both temporal and spatial data, achieves spatio-temporal prediction on multivariate time series data by leveraging a 1D convolutional layer before the LSTM layer. This allows for the incorporation of input from various sensors that may bring spatio-temporal information. The key equations of ConvLSTM are as follows:

$$i(t) = \sigma(W_{xi} * X(t) + W_{hi} * H(t-1) + W_{ci} \circ C(t-1) + b_i \quad (1)$$

$$f(t) = \sigma(W_{xf} * X(t) + W_{hf} * H(t-1) + W_{cf} \circ C(t-1) + b_f \quad (2)$$

$$C(t) = f(t) \circ C(t-1) + i(t) \circ tanh(W - xc * X(t) + W_{hc} * H(t-1) + b_c \quad (3)$$

$$o(t) = \sigma(W_{xo} * X(t) + W_{ho} * H(t-1) + W_{co} \circ C(t) + b_o \quad (4)$$

$$H(t) = o(t) \circ tanh(C(t)) \quad (5)$$

2.3. Nonparametric Dynamic Thresholding

After getting the forecast data from the prediction model, thresholding method is needed to determine whether data is classify as normal or abnormal. One main challenge in detecting anomalies in streaming data is the occurrence of data drift, which makes the model and thresholding method irrelevant due to changes in patterns or behavior. To effectively monitor thousands of IoT endpoints influenced by changing environmental conditions, there is a critical need for unsupervised approach to detecting anomalies in dynamic environments. While frequently employed method relies on the assumption of Gaussian distributions for past smoothed errors, enabling swift comparisons with concise representations of previous errors. However, this approach can face challenges when parametric assumptions are violated.

To address this issue, nonparametric dynamic thresholds proposed by **[Ref: Hundmand et al.]** play a crucial role. This method has been proven to be stable and reliable, minimizing false positives and false negatives against noise and dynamic environments by updating the threshold. Therefore, in this study, we modified and implemented this method in our approach by incorporating continuous learning. **Algorithm 1** illustrates the step-by-step procedure for prediction-based anomaly detection employing nonparametric dynamic thresholding.

Algorithm 1 Nonparametric Dynamic Thresholding

Input: y - Streaming data
R - Anomaly rate
h - Sliding window size
z - A factor used to initialize threshold

Output: A- a list of indices where anomaly are detected
N- a list of indices of normal data

while True **do**
  load the streaming data y
  $\hat{y} \leftarrow$ Predict the future value of y
  Calculate deviation $e^{(t)} \leftarrow \hat{y} - y$
  Append $e^{(t)}$ into an array $e = [e^{(t-h)}, ..., e^{(t)}]$
  Calculate $\mu(e)$ and $\sigma(e)$
  if (T is none) **then**
    $T = \mu(e) + z\sigma(e)$
  else
    $T = \frac{(\Delta\mu(e)/\mu(e)+\Delta\sigma(e)/\sigma(e))}{(lengthofA)^2}$
  end if
  if $e^{(t)} > T$ **then**
    Append $e^{(t)}$ into A
  else
    Append $e^{(t)}$ into N
  end if
  Calculate $\Delta\mu(e) = \mu(e) - \mu(N)$
  Calculate $\Delta\sigma(e) = \sigma(e) - \sigma(N)$
  $r \leftarrow$ length of e / length of A
  if $r > R$ **then**
    Re-train the prediction model
  end if
  if Length of $e > h$ **then**
    Remove the oldest data $e^{(t-h)}$ from e
  end if
end while

2.4. Fine-tuned GPT-4 integration

In order to automatically generate understandable decision support based on the provided anomaly detection information, we propose the integration of the (GPT-4 model by OpenAI **[Ref: GPT]**. While GPT-4 is a powerful and large-scale model, its base version is designed to be general-purpose, which may not fully meet the specific requirements of task-specific anomaly detection decision support, especially when applied to domains like time-series anomaly detection in machine and environmental data. The reasoning generated by the base GPT-4 may be overly general for the intricacies of anomaly detection in these domains.

To address this, fine-tuning GPT-4 with a custom dataset provides several key advantages. It allows for tailoring the model's capabilities to the specific task or domain, leading to higher accuracy and more comprehensive reasoning. Additionally, fine-tuned models can be rapidly deployed for practical applications, making them particularly suitable for tasks where real-time or time-sensitive responses, such as anomaly detection decision support, are essential. In this study, we fine-tuned the GPT-4 model using the OpenAI API **[Ref: GPT-4 OpenAI API website]** with 50 prompts of anomaly situations and desired responses and trained it for 10 epochs.

3. Experiments Settings

IAQ data covers five days, from October 20th to 25th, 2023, is collected with a one-second sampling frequency. The dataset consists of 7,661,038 data points obtained from seven sensors placed within a single room and split into three set: training, validation, and test set. To simulate anomalies, a total of 300 anomaly data points are manually injected into testing set. This includes 10 point anomalies and 290 contextual anomalies, facilitating comprehensive evaluation of anomaly detection performance.

3.1. Evaluation metrics

To assess the performance of the anomaly detection model objectively, we utilize two evaluation metrics to measure its efficiency in detecting anomalies within time series data. In this paper, we consider F1-score and AUC as the metrics for evaluating the model's performance. The formula for each evaluation metric is outlined as follows:

$$F1 - score = \frac{TP}{TP + 1/2(FP + FN)} \tag{6}$$

$$TPR = \frac{TP}{TP + FN} \tag{7}$$

$$FPR = \frac{FP}{FP + TN} \tag{8}$$

$$AUC = \int TPR(FPR)dFPR \tag{9}$$

4. Result and Discussion

Various anomaly detection models, including the Isolation Forest (IF) from traditional machine learning and deep learning-based approaches such as AE and LSTM-AE, were implemented to evaluate the efficacy of the novel anomaly detection method within a collected

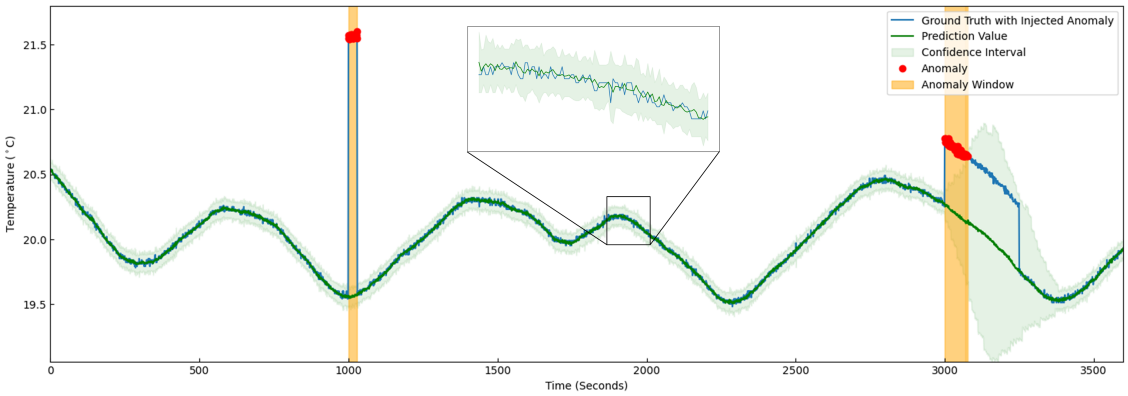

Figure 3. Anomaly Detection Result using ConvLSTMBNN-DT on Temperature Data

dataset with injected point and contextual anomaly data. As depicted in Table 2, presenting the performance analysis outcomes, the proposed model showcases superior performance when compared to other anomaly detection techniques across various features. The evaluation, employing F1-score and AUC metrics, illustrates that the proposed model consistently outperforms its counterparts. This suggests that the proposed model adeptly identifies both generated point anomalies and contextual anomaly data, presenting a noteworthy advancement in comparison to alternative models.

Figure 3 presents the results of the anomaly detection performed by the proposed model. In the plot, the green line represents the ground truth data, the blue line depicts the predicted data, and the green window indicates the confidence interval based on the calculated T value. The zoomed-in plot clearly shows that the proposed model's predictions closely align with the ground truth data, underscoring its robust predictive performance. The model effectively captures the normal pattern or behavior of the data in the 1-hour-ahead prediction window with relatively low error. Notably, the confidence interval dynamically adjusts as the dynamic threshold feature updates. The most significant changes are observed during contextual anomalies, where the confidence interval widens due to an increased number of errors and anomalies in the data. This leads to a lower threshold T value, reflecting the penalization of the total number of anomalies A. Therefore, after reach some points, the new-normal incoming data classified as normal. The results highlight the proposed model's adaptability in dynamic environments, particularly in scenarios where data drift may occur.

The ConvLSTMBNN-DT demonstrates superior anomaly detection performance compared to other models, primarily attributed to the collaborative synergy between ConvLSTM and BNN models, complemented by dynamic thresholding. The ConvLSTMBNN model excels in extracting temporal features from multivariate input data, generating robust predictions by sampling weight values from a learned posterior distribution. This variance in weight values enables the model to dynamically adapt to changing input data. The incorporation of nonparametric dynamic thresholding facilitates automatic adjustments to the threshold, swiftly accommodating data drift and effectively minimizing false positive and false negative detections. The continuous learning aspect further enhances the model's adaptability, ensuring it adeptly captures the temporal patterns within the data. Overall, the ConvLSTMBNN-DT emerges as a powerful anomaly detection solution, proficient in handling dynamic data characteristics and optimizing detection accuracy.

Table 1
Performance analysis of anomaly detection models on generated dataset

Model	Temp		Hum		PM	
	F1	AUC	F1	AUC	F1	AUC
IF	0.86	0.81	0.82	0.77	0.88	0.82
AE	0.88	0.84	0.85	0.80	0.89	0.84
LSTM-AE	0.87	0.82	0.86	0.81	0.90	0.86
Proposed	**0.91**	**0.87**	**0.90**	**0.85**	**0.92**	**0.87**

5. Conclusion

In conclusion, this research introduces a novel hybrid approach that combines prediction-based anomaly detection using ConvLSTMBNN-DT with the fine-tuned GPT-4 model for LLM-based explanation generation, significantly enhancing interpretability and adaptability.

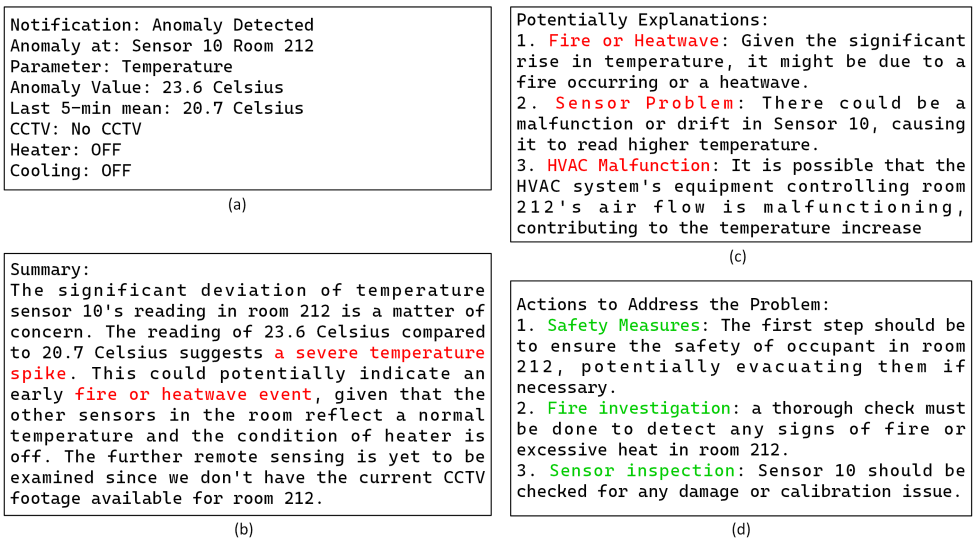

Figure 4. Result of Decision Support Generated by Fine-tuned GPT-4. (a) Input prompt based on anomaly data, (b) Brief summary of the anomaly data, (c) The potential cause of the anomaly, (d) The possible actions to address the issue

By integrating prediction-based algorithms and LLMs, the model not only detects anomalies but also provides human-understandable explanations, making it a powerful tool for quick decision-making in real-world applications. Custom fine-tuning with GPT-4 tailored to the specific anomaly detection task further amplifies interpretability. The presented hybrid approach, along with advanced LLMs, promises to play a pivotal role in improving anomaly detection across various domains.

For future work, enhancing anomaly detection classification could deepen the accuracy of anomaly reasoning. Integrating multimodal sensor fusion, combining time-series data with visual and auditory inputs, may lead to more holistic anomaly detection solutions capable of capturing anomalies across various data modalities. Exploring the integration of reliable control systems for intelligent decision-making in real-time scenarios offers great opportunities.

Acknowledgments

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IIITP-2023-2018-0-01396) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2022-0-00590, Industrial small cell system supporting 5G multi-band).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H. Kwon, K. Kim, C. Lee, The unified UE baseband modem hardware platform architecture for 3GPP specification, J. Commun. Net., 13 (1) (2011) 70-76.
[2] T. Roos, P. Myllymaki, H. Tirri, A statistical modeling approach to location estimation, IEEE Trans. Mobile Comput. 1 (1) (2002) 59-69.
[3] H. Liu, G. Li, OFDM-Based Broadband Wireless Networks: Design and Optimization. Hoboken, NJ: Wiley-Interscience, 2005.
[4] T. L. Marzetta, How much training is required for multiuser MIMO?, in: 2006 Asilomar Conf. Signal. Syst. Comput., Pacific Grove, 2006, pp. 359–363.
[5] J. Arrillaga, B. Giessner, Limitation of short-circuit levels by means of HVDC links, in: 1990 IEEE Summer Power Meeting, Los Angeles, 1990, pp. 1-8.
[6] J. O. Williams, Narrow-band analyzer, Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.
[7] J. H. Davis, J. R. Cogdell, Calibration program for the 16-foot antenna, Elect. Eng. Res. Lab., Univ. Texas, Austin, Tech. Memo. NGL-006-69-3, Nov. 15, 1987.
[8] RealVNC Ltd. Remote control software [Online]. Available: ftp:// www.realvnc.com