Journal of Information Hiding and Multimedia Signal Processing ©2026 ISSN 2073-4212
Ubiquitous International Volume **17**, Number **1**, March **2026**

Real-time Anomaly Detection in Industrial Ovens: An AI and IoT-Based System

Truong Nguyen Xuan[1,2], Thuan Nguyen Dinh[1,2]

[1]University of Information Technology, VNU–HCM, Vietnam
[2]Vietnam National University, Ho Chi Minh City, Vietnam
truongnx.18@grad.uit.edu.vn, thuandd@uit.edu.vn

*Corresponding author: Thuan Nguyen Dinh

Received October 24, 2025, revised January 13, 2026, accepted January 17, 2026.

Abstract. *This research proposes an Artificial Intelligence (AI) and Internet of Things (IoT)–based system for automated anomaly detection in industrial oven machines, with a particular focus on steam valve leakage in the Modular Oven System 700H (MOS 700H) operating in standby mode. The proposed system aims to improve operational efficiency and ensure safety through proactive maintenance while reducing machine downtime. To achieve this objective, multivariate sensor data, including temperature, humidity, and air pressure, are collected from IoT-enabled sensors and used to train a Stacking Ensemble learning model. The proposed model integrates multiple machine learning algorithms to enhance anomaly detection performance, particularly in industrial scenarios where anomalous events are rare and highly imbalanced. Experimental results conducted on datasets spanning from 15 to 180 days demonstrate that the proposed Stacking Ensemble model consistently outperforms other baseline AI models, especially for long-term monitoring tasks. These findings confirm the effectiveness of combining AI and IoT technologies for real-time monitoring of industrial ovens and highlight their potential in improving system reliability and operational stability.*
Keywords: Abnormal Detection; Industrial Oven; Stacking Ensemble; Machine Learning; IoT Data.

1. **Introduction.** According to [1] reports, the anomaly detection market in the world has been increasing rapidly and is expected to achieve 13,4 billion USD in 2030. This trend reflects the importance of ensuring safety and operation efficiency in modern industrial systems [2]. Technical failures, such as steam valve leakage in industrial oven machines used for food processing, can cause significant economic losses because they are effective in the quality and consistency of the product. Although, there is no specific research about damage caused by steam valve leaks in the food industry. However, other reports in the oil and gas industry [3] mentioned that this phenomenon could cause energy loss of up to 20 % in the steam distribution network; this leads to increased maintenance costs and warranty costs. In the context of cost reduction associated with anomalous events, the development of an automated anomaly detection system for the industrial oven investigated in this study is of significant practical importance. Such a system contributes to optimizing production processes, reducing operational risks, and enhancing industrial competitiveness.

The rapid advancement of the Internet of Things (IoT) over the past decade has created new opportunities for monitoring and managing industrial equipment [4]. By integrating IoT-enabled sensors with advanced machine learning techniques, it is possible to continuously collect and analyze large volumes of operational data, enabling early detection of anomalous behaviors such as steam valve leakage [5]. Early anomaly detection allows timely maintenance interventions, thereby reducing downtime, minimizing risks, and improving overall system reliability.

This research identifies steam valve leakage in Modular Oven Systems 700H (MOS 700H), a type of industrial oven widely used in food processing. MOS 700H is a flexible and efficient system that allows

for precise control of critical parameters such as temperature, humidity, and air pressure throughout the cooking, steaming, or baking process. However, even when the oven is in standby mode, steam valve leakage can still occur, affecting the stability of the dew point, which in turn reduces the quality of the final product.

Currently, steam valve leak detection mainly relies on manual inspection by experienced operators. However, this method has several limitations, including: (1) Low accuracy: The ability to detect leaks depends heavily on the inspector's skills and experience, leading to inconsistencies in accuracy between inspections. (2) Time-consuming: Manual inspections often take a considerable amount of time, especially for complex systems with numerous steam valves, resulting in delayed leak detection. (3) Prone to human error: Subjective and objective factors can increase the likelihood of missing or misjudging leaks. Therefore, research and development of a reliable, automated leak detection system for steam valves is crucial. This would overcome the limitations of traditional methods and improve operational efficiency.

This research proposes a machine learning–based model that leverages Artificial Intelligence (AI) and Internet of Things (IoT) technologies to detect anomalous steam valve leakage in industrial ovens. The system is equipped with IoT-enabled sensors to collect operational data, including temperature, humidity, and air pressure, at 5-second intervals. The collected data are preprocessed and subsequently fed into the proposed Stacking Ensemble model to identify anomalous patterns. By combining the continuous data acquisition capability of IoT with robust AI-based analytics, the proposed system provides an accurate and real-time automated solution for monitoring the performance and operational status of industrial ovens.

Research contributions: (1) This study presents a practical AIoT-based anomaly detection framework tailored for industrial oven systems, with a focus on steam valve leakage under standby operating conditions. (2) A stacking ensemble learning strategy is systematically adapted and validated for long-term industrial time-series data with extreme class imbalance, demonstrating stable and robust performance on datasets spanning up to 180 days. (3) Experimental results demonstrate that the proposed Stacking Ensemble model achieves superior performance in detecting steam valve leaks, with a precision of 97% and a recall of 96%.

Summary of Results: This study was evaluated on 15-day, 30-day, 60-day, and 180-day datasets. The results showed that the proposed Stacking Ensemble model consistently outperformed other AI models, including CNN + LSTM, XGBoost, and Transformer, in detecting anomalous events. The Stacking Ensemble model achieved a precision of 97% and a recall of 96%.

The rest of the paper is divided as follows: Section 2 provides an overview of anomaly detection methods in industrial environments. Section 3 details how data was gathered and prepared for the proposed model analysis. Section 4 will show the experimental results of the proposed models and conclusion. Finally, it suggests future research directions to improve the accuracy of Section 5.

2. **Literature review.**

Monitoring and anomaly detection, especially in the food manufacturing sector, play a vital role in ensuring product quality, worker safety, and operational efficiency [6], [7]. Anomaly detection is a critical aspect of industrial manufacturing, as it helps ensure continuous operations and minimize risks. With the proliferation of IoT devices generating large volumes of sensor data, advanced monitoring and predictive maintenance methods are required [4], [8]. Anomalies must be detected early to prevent failures and improve production efficiency, particularly in complex systems such as industrial manufacturing and energy management [8], [9]. In recent years, anomaly detection has been increasingly integrated into Industrial Internet of Things (IIoT) architectures, where large volumes of real-time sensor data are continuously collected from industrial equipment. AI-driven monitoring systems enable early identification of abnormal behaviors that may indicate faults, safety risks, or performance degradation in industrial environments. However, IIoT-based anomaly detection systems also face significant challenges, including data imbalance, computational constraints at the edge, and the need for timely and interpretable decision-making [10].

Traditional methods are typically threshold-based or rule-based, which makes them challenging to adapt to the complexity and variability of real-world operational data [11], [12]. According to the survey in [11], these methods are often ineffective at detecting complex anomalies and are susceptible to noise, as noisy patterns may resemble true anomalies, making them difficult to distinguish. The rise of the Internet of Things (IoT) and Artificial Intelligence (AI) has introduced new opportunities and more effective approaches for anomaly detection [7]. Unsupervised techniques have become increasingly popular for anomaly detection in industrial systems because they can be trained on unlabeled data, for which labeled samples are often difficult and costly to obtain. Autoencoders and Long Short-Term Memory (LSTM) networks have been widely used to reconstruct data and identify anomalies based on reconstruction errors

[13], [14]. In addition, the study in [9] employed an LSTM-based autoencoder (LSTM-AE) to detect anomalies in sequential data, where the LSTM network effectively captures temporal dependencies.

Moreover, supervised learning continues to play an essential role when high classification accuracy and reliable fault prediction are required in industrial applications [4]. In supervised learning, labeled data are used to train a model that can differentiate between normal and anomalous instances [7]. However, a major challenge of this approach is handling data imbalance. In the study reported in [6], the authors employed the Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance issues. Machine learning models such as Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Random Forest have been shown to effectively improve anomaly detection performance in industrial environments [6]. In addition, the study in [15] applied machine learning techniques to detect intrusions in Vehicular Ad Hoc Networks (VANETs) for security enhancement. Using the ToN-IoT dataset together with Chi-square feature selection and SMOTE, the results demonstrate that XGBoost achieves superior performance in intrusion classification tasks [15].

Deep learning is a powerful tool for anomaly detection because it can learn intricate patterns from data. Models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have been shown to be effective in detecting anomalies in time-series data, improving accuracy and reducing false alarm rates [13]. Recently, increasing attention has been paid to exploring the potential of hybrid architectures that combine neural networks with autoencoders for monitoring industrial equipment. This approach enables systems to automatically adapt to rapid operational changes and detect potential problems at an early stage [9]. A representative study in [16] presented an automated system that applied IoT and AI technologies to detect faults in industrial diesel machines. Compared with traditional methods, the proposed system significantly reduces labor costs and enhances maintenance efficiency. In addition, the study in [17] applied Transformer-based technology to develop the TranAD model, a novel approach for anomaly detection in multivariate time-series data. TranAD was designed to achieve fast processing speed and high accuracy despite the challenges posed by complex data and scarce anomaly samples. Its superior performance is achieved by combining attention mechanisms, adversarial training, and meta-learning. Experimental results demonstrate that TranAD outperforms existing methods and confirm its potential for widespread application in the monitoring and management of complex industrial IoT systems.

Research on anomaly detection in the food processing industry remains limited. One of the few notable studies is the master's thesis reported in [18], in which a semi-supervised approach was applied to detect anomalies in smart ovens used in retail stores. The data used in this study were collected from an IoT sensor installed on the oven. The objectives of the study were to improve food quality, ensure food safety compliance, and reduce waste during the baking process [18]. However, the scope of the study was limited to a small-scale oven system. For broader practical applications, particularly in industrial production environments, further in-depth research involving large-scale systems and more diverse operational conditions is required. In the context of anomaly detection in industrial environments, the study in [9] proposed an online anomaly detection approach based on unsupervised deep learning techniques. Specifically, the proposed method combines autoencoder models with multiple machine learning algorithms to identify and prevent faults that may disrupt production processes or cause operational downtime. The approach aims to enable timely maintenance interventions, thereby maintaining stable production operations [9]. Autoencoder-based models are used to identify anomalous patterns in data collected from industrial furnaces, contributing to improved detection accuracy and timeliness of the monitoring system. In addition, the fusion of data from multiple sensors has been shown to significantly enhance monitoring capability and enable rapid responses to critical incidents [9].

Although numerous studies have addressed anomaly detection in industrial systems, the application of the Stacking Ensemble method for monitoring industrial oven machines in food processing remains largely unexplored. This research introduces a methodology that leverages the combined power of AI and IoT data collected from sensors installed on industrial ovens to enhance anomaly detection efficiency and optimize operational procedures in the food industry.

3. Material and Proposed method.

This section describes the methodology used to detect anomalies in industrial ovens. It provides detailed information on the research design, data collection and preprocessing procedures, as well as the model development approach for anomaly detection. Specifically, this section focuses on the following aspects:

- **Data collection (case study):** Describes the IoT sensor system used, including its deployment and the process of collecting operational data from the industrial oven.

- **Data processing:** Presents the data preprocessing steps, including data cleaning, labeling, transformation, and normalization, to ensure the quality of the input data for model training.
- **Model development:** Describes the anomaly detection model in detail, including its architecture, the applied machine learning algorithms, and the model training process.

3.1. **Case study.** This research focuses on fault detection in industrial oven systems used in food production. These systems are complex and consist of five main components, enabling a variety of functions such as steaming, cooking, and baking for different products.

- **Base tower (ascending tower):** This is the first climate zone through which the product passes. It is equipped with a heat exchanger, steam inlet and make-up air valves, and a circulation fan to control temperature, humidity, and air velocity. The conveyor belt in this tower moves upward.
- **Tower connection:** Connects the two towers, protecting the product from the external environment and maintaining a buffer zone between the two climate zones.
- **Secondary tower (descending tower):** This is the second climate zone through which the product passes. It is also equipped with a heat exchanger, steam inlet and make-up air valves, and a circulation fan. The conveyor belt in this tower moves downward.
- **Transport frame:** Facilitates the safe and convenient transportation of the MOS components.
- **Switch box:** Controls the overall system, including the main control cabinet (PLC) and the HMI touchscreen. Each tower has its own control box to interface with local field components.

The data collection process from an industrial oven machine in the food industry is depicted in Figure 1, specifically the MOS 700H, a dual-zone oven that uses hot air to cook, steam, or bake a variety of products.

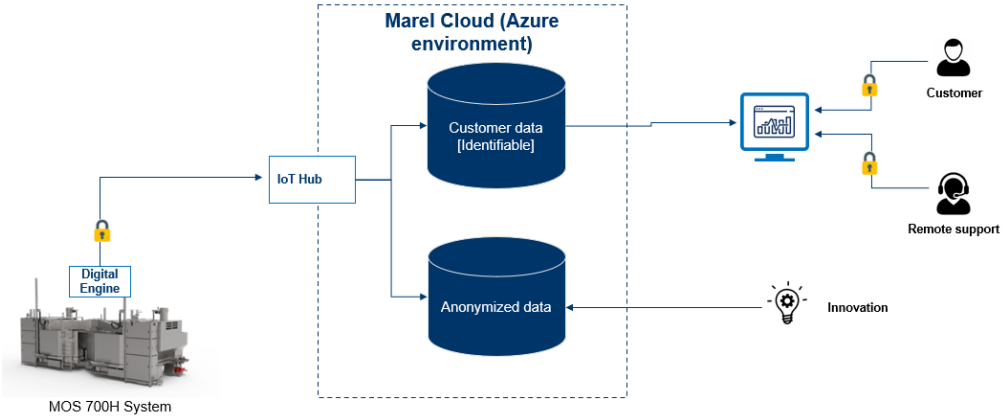

FIGURE 1. Data collection process from the industrial oven.

In this study, we focus on the problem of steam valve leakage in the base and secondary towers during the standby state of the oven. Steam valve leakage can significantly disrupt the dew point stability inside the oven, leading to inconsistent product quality. Therefore, it is very important to promptly handle these leakage incidents. The current manual inspection process, although effective, is labor-intensive and subjective. This study aims to develop a method for detecting anomalies using a machine learning model trained on collected data.

3.2. **Dataset.** The data for this study comes from sensors attached to a real-world industrial oven. It consists of multiple variables collected from March 23 to September 24, 2024, recorded every 5 seconds, resulting in 3,167,408 rows of data for each zone. The data is classified into four main categories, providing a thorough basis for the study.

- **Operating parameters:** These include temperature, humidity, and air pressure, which are recorded by separate sensors during the operation of the industrial oven machine.
- **Machine status:** The oven machine operates in eleven different states; however, this study focuses only on the *standby state*, as this is when steam leakage is effectively monitored.
- **Hood status:** The oven machine hood can be opened or closed. Steam leakage can only be detected when the hood is closed, making this parameter essential for accurate anomaly detection.
- **Air supply:** A sufficient air supply is required to detect steam valve leakage. Therefore, the presence and level of air supply are recorded to ensure suitable conditions for monitoring.

Each zone contains seven attributes, including information about machine operating status, temperature, humidity, air pressure, etc., as illustrated in Table 1.

TABLE 1. Features definitions based on data characteristics.

No.	Message	Name	Data type	Description	Unit
1	**Day**	Day	integer	The day to collect data	Day
2	**Month**	Month	integer	The month to collect data	Month
3	**Year**	Year	integer	The year to collect data	Year
4	**Time Stamp**	TimeStamp	Date Time	Time to collect data with intervals of 5 seconds	Second
5	**Main state**	C_State	dint	The main status of the machine	
6	**Hood**	H508	bool	Actual low-level hood	On Off
7	**Supplies**	S001	bool	Air supply valve zone one	On Off
8		S002	bool	Air supply valve zone two	On Off
Zone 1 (Base Tower)					
9		T101	float	Actual temperature before heater zone one	Celsius
10	**Temperature**	T102	float	Actual temperature after heater zone one	Celsius
11		T103	float	Actual temperature at product level zone one	Celsius
12		H101	float	Actual dewpoint zone one	Celsius
13	**Humidity**	H102	float	Control valve steam zone one	Percentage
14		H103	float	Actual pressure steam supply zone one	Bar
Zone 2 (Secondary Tower)					
15		T201	float	Actual temperature before heater zone two	Celsius
16	**Temperature**	T202	float	Actual temperature after heater zone two	Celsius
17		T203	float	Actual temperature at product level zone two	Celsius
18		H201	float	Actual dewpoint zone two	Celsius
19	**Humidity**	H202	float	Control valve steam zone two	Percentage
20		H203	float	Actual pressure steam supply zone two	Bar

Figure 2 provides a snapshot of the data used to train and evaluate our models. This data represents two zones within the oven.

Anormal 1	Anormal 2	day	month	timeStamp	C_State	H508	S001	H103	H102	H101	T101	T102	T103	S002	H203	H202	H201	T201	T202	T203
0	0	15	7	2024-07-15T00:00:03	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:08	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:13	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:18	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:23	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.2	22	23.4
0	0	15	7	2024-07-15T00:00:28	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:33	8	FALSE	TRUE	0.03	0	55	29.7	18.2	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:38	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:43	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:48	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.03	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:53	8	FALSE	TRUE	0.03	0	55	29.7	18.2	17.9	TRUE	0.04	0	55	32.3	22	23.4
0	0	15	7	2024-07-15T00:00:58	8	FALSE	TRUE	0.03	0	55	29.7	18.3	17.9	TRUE	0.04	0	55	32.3	22	23.4

FIGURE 2. Sample data from an industrial oven used for training and testing machine learning models.

3.3. **Labeling and preprocessing data.** To initiate the training process of the AI model, several data preprocessing steps were performed. The data used for model preparation were obtained from the Azure cloud environment. Before raw data can be fed into a machine learning model, they must be properly

prepared. This process, referred to as data preprocessing, ensures that the data are in a suitable format for effective model learning [17]. The key steps involved in data preprocessing are summarized as follows:

- **Integration of features from multiple sensors into a multivariate time series:** Anomaly prediction is based on various operational conditions, including the *Machine State*, *Oven Hood state*, and *Air Supply state*, as well as sensor measurements of humidity, temperature, and air pressure. These data were stored in four CSV files hosted on the Azure cloud platform and subsequently merged into a single dataset using Excel functions such as *VLOOKUP* and blank-cell handling techniques to ensure data integrity.
- **Data labeling:** In the subsequent step, the dataset was labeled through visual inspection by industry experts with relevant domain knowledge, following the procedure illustrated in **Figure 3**. This figure depicts a critical step in preparing data for supervised model training and accurate labeling. Each decision node in the flowchart represents a specific operational or analytical condition, thereby ensuring transparency and reproducibility of the anomaly detection logic. Although the dataset contains both anonymized and identifiable information, only anonymized data were used to ensure compliance with privacy requirements.
- **Outlier handling:** Outliers are data points with abnormal values that may arise from sensor errors, environmental noise, or data entry inaccuracies [9]. Such extreme values can disrupt data distributions and degrade the performance of machine learning models. To address this issue, several strategies exist, including the removal or replacement of outliers. In this study, outliers were replaced with the **median value**, as it is less sensitive to extreme values and is well suited for skewed data distributions [5]. In addition, the **Interquartile Range (IQR)** method [16] was employed to identify outliers. Specifically, the median, first quartile (Q1), and third quartile (Q3) were computed for each feature, and outlier boundaries were defined as 1.5 times the IQR below Q1 and above Q3. Data points outside these thresholds were replaced with the corresponding median value, thereby improving data reliability and model robustness, particularly for anomaly detection in industrial time-series data [17].
- **Multivariate time-series data normalization:** Prior to feeding the multivariate time-series data into the machine learning models, normalization was performed to enhance training efficiency. The **standard scaling** technique was applied, transforming each feature to have a mean of zero and a standard deviation of one. This prevents features with large numeric ranges from dominating the learning process and ensures that all features contribute equally during model training.

Preprocessing involves filtering out irrelevant information and focusing on key variables such as temperature, humidity, and air pressure. These variables are then visualized using a correlation heatmap, as shown in Figure 4, which illustrates the relationships among features across different zones. This step helps identify the most critical factors for effectively training the anomaly detection model and ensures that the data are organized in a manner that facilitates anomaly identification.

3.4. **Definition of Anomaly.** In this study, an anomaly is defined as an anomaly steam valve leakage event occurring during the standby state of the industrial oven under fixed operational conditions. Specifically, an anomaly is identified when the following conditions are simultaneously satisfied:

- The oven operates in standby mode.
- The oven hood is closed.
- Air supply valves are active.
- Sensor measurements, including dew point, temperature, or steam pressure, exhibit sustained deviations from learned normal standby behavior.

Such deviations are characterized by anomaly increases in dew point, inconsistencies between steam control valve position and measured steam pressure, or prolonged temperature, dew point instability beyond expected operational fluctuations. Short-term transient variations and sensor noise are excluded from anomaly labeling. Anomaly labels were assigned through visual inspection and confirmation by industrial domain experts with extensive operational experience. The labeling process is based on temporal behavior and physical system understanding rather than fixed threshold-based rules, ensuring that detected anomalies correspond to meaningful industrial faults.

3.5. **Sliding windows.** Once the initial data processing was completed, a sliding window technique was employed to prepare the data for time-series analysis, as it is essential for capturing temporal dependencies. The goal of time-series anomaly detection is to identify anomalous time series, where each anomaly corresponds to a continuous sequence of data points that deviates from the expected temporal behavior learned from the training data [17]. In this study, the time window size was set to $n_{\text{steps}} = 10$,

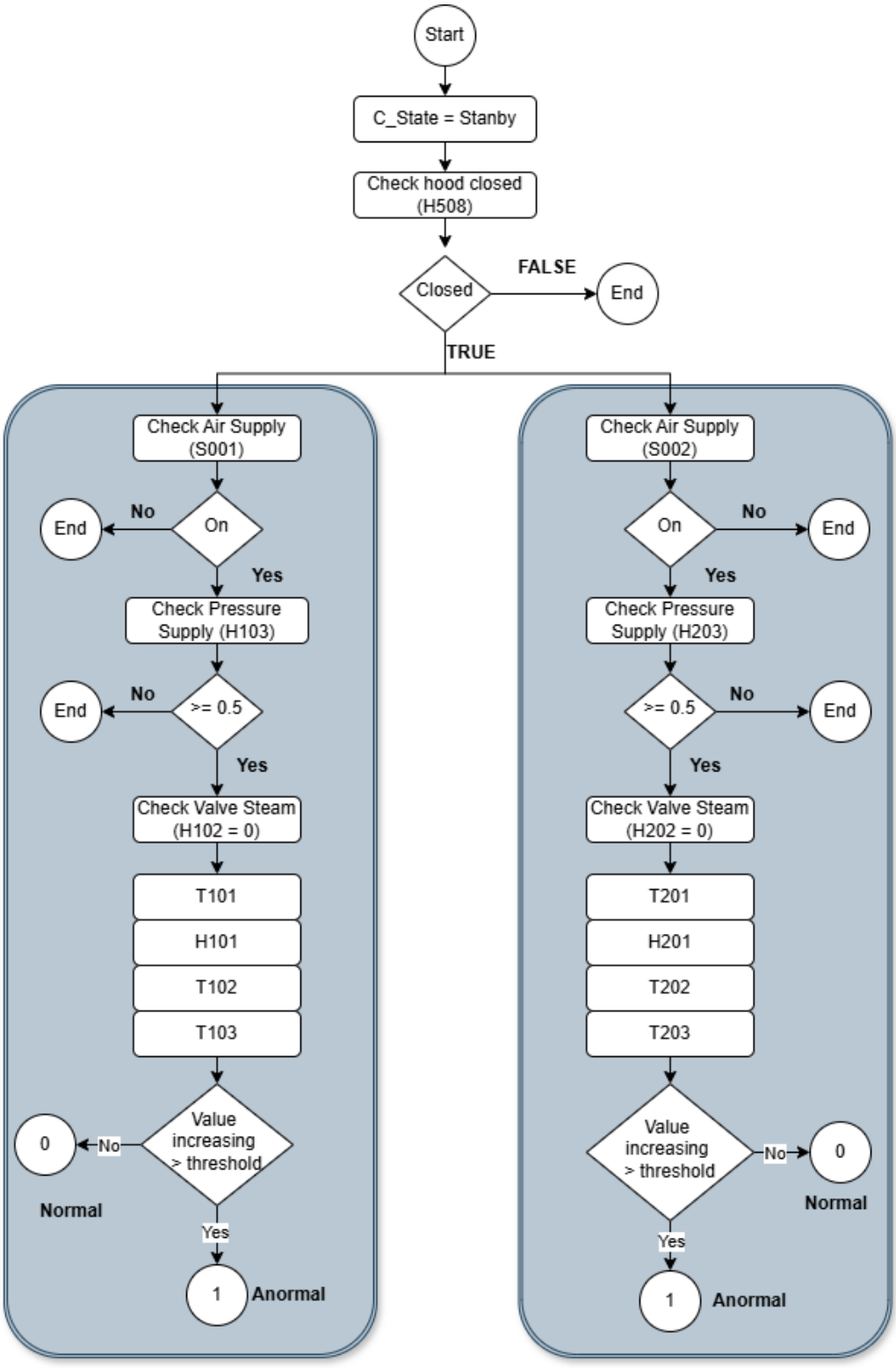

FIGURE 3. Data labeling process conducted by industry experts with domain knowledge.

corresponding to 50 seconds of IoT data, based on two main considerations. First, according to domain experts, early indications of steam valve leakage typically manifest as continuous fluctuations in temperature and dew point over a period of several tens of seconds before the fault becomes clearly observable. Second, preliminary experiments revealed that excessively short time windows were insufficient to capture

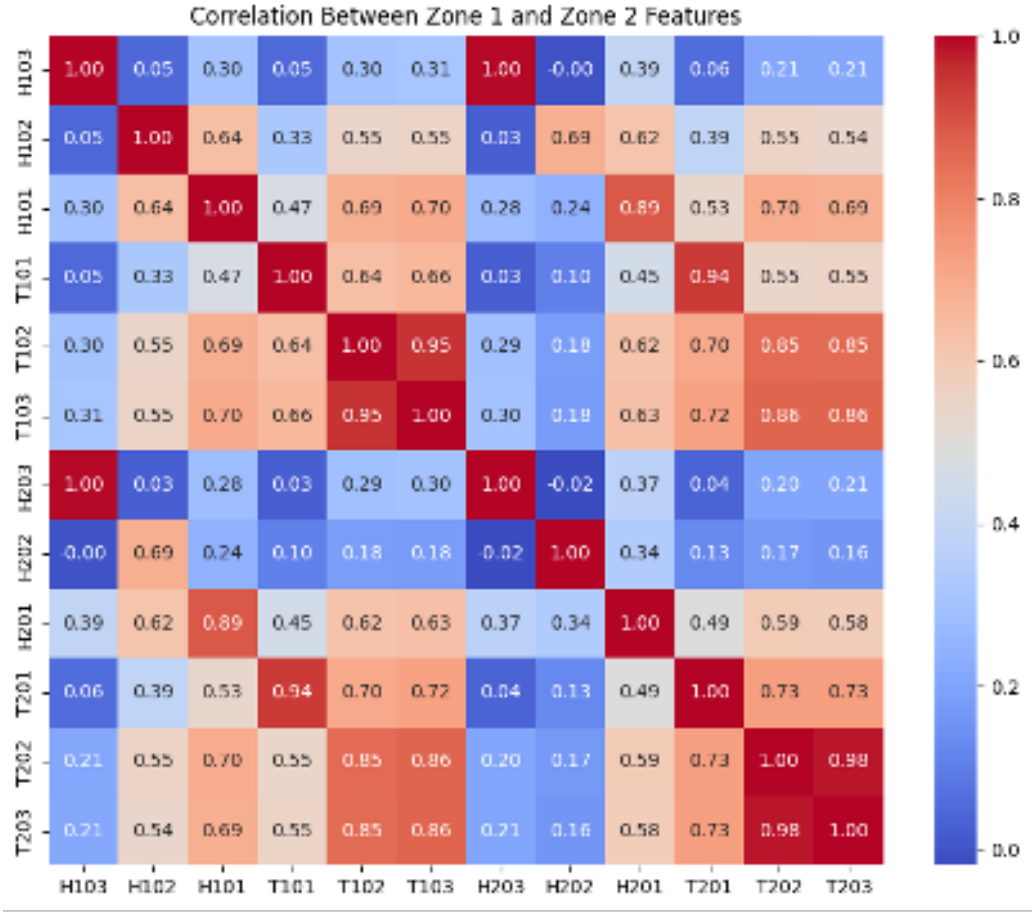

FIGURE 4. The heatmaps illustrate the correlations among features relevant to Zone 1 and Zone 2.

anomalous temporal patterns, whereas overly long windows increased noise and computational complexity. Therefore, $n_{\text{steps}} = 10$ was selected to achieve a balance between effective temporal feature learning and computational efficiency.

3.6. **The main model.**

3.6.1. *Introduction to the Model.* To address the challenges of anomaly detection in industrial ovens, particularly under conditions of highly imbalanced data collected from IoT-enabled sensors, this study proposes a Stacking Ensemble–based learning framework. The proposed method combines the strengths of multiple base learners and employs a meta-learner to enhance detection accuracy, robustness, and generalization capability. In addition, the ADASYN technique is applied to balance the training data, while hyperparameters are systematically optimized to achieve stable performance across datasets of different sizes.

Four datasets covering different time spans (15, 30, 60, and 180 days), as summarized in Table 2, were used to train and evaluate the proposed model. These datasets exhibit severe class imbalance, with anomalous samples accounting for less than 1% of the total data. To mitigate this issue, the Adaptive Synthetic Sampling (ADASYN) technique [18] was employed. Unlike conventional oversampling methods that merely replicate minority-class samples, ADASYN generates synthetic samples in regions where the classifier has difficulty distinguishing anomalous patterns. This approach enables the model to learn rare anomaly characteristics more effectively while reducing the risk of overfitting to the original dataset.

3.6.2. *Model Architecture.* The proposed model employs a Stacking Ensemble framework for anomaly detection. Figure 5 illustrates the overall architecture, which comprises the following components. The proposed model employs a Stacking Ensemble approach for anomaly detection. The base learners consist of a Random Forest algorithm, which constructs multiple decision trees and combines their predictions,

TABLE 2. The dataset statistics across collection periods

Dataset Period	Normal Samples	Abnormal Samples	Percentage Abnormal (%)
15 Days	514,018	4,626	0.89%
30 Days	1,027,123	4,715	0.46%
60 Days	2,060,838	6,668	0.32%
180 Days	6,334,816	26,370	0.42%

and an XGBoost algorithm, known for its ability to capture complex patterns and achieve high accuracy. A Logistic Regression model serves as the meta-learner, combining the predictions of the base learners to produce a final classification. A threshold of 0.5 is used to determine the presence of an anomaly, balancing the trade-off between sensitivity and precision. Figure 5 illustrates our proposed method for anomaly detection.

3.6.3. *Hyperparameter fine-turning.* We conducted extensive hyperparameter tuning to optimize the performance of both the base learners and the meta learner. Table 3 summarizes the ranges and optimal hyperparameters for each dataset duration.

TABLE 3. The developed Stacking Ensemble algorithm's hyperparameter ranges and optimal architecture for different dataset periods.

Component	Hyper-parameter	Range	Optimal Value (All Periods)
Window Size	Size	[5, 10, 15, 20]	10
Random Forest	Number of Trees	[50, 100, 200]	100
XGBoost	Learning Rate	[0.01, 0.1, 0.2]	0.1
	Subsample	[0.6, 0.8, 1.0]	0.8
Meta-Learner	Regularization (C)	[0.1, 1, 10]	1
Output	Probability Threshold	[0.4, 0.5, 0.6]	0.5

3.6.4. *Algorithm Description.* Algorithm 1 applies the proposed Stacking Ensemble approach to predict anomaly events in time-series data using a sliding window mechanism. The proposed model offers several key advantages for identifying anomalies in time-series data:

(1) Sliding window mechanism: The sliding window mechanism enables the model to focus on local temporal features within the time series, thereby improving the accuracy of anomaly detection.

(2) Ensemble learning: The Stacking Ensemble strategy enhances model performance by leveraging the complementary strengths of multiple base learners and a meta-learner.

(3) Flexible threshold adjustment: The proposed model allows flexible adjustment of the decision threshold to balance sensitivity and specificity, enabling adaptation to different operational requirements.

(4) Ability to handle large datasets: The proposed algorithm efficiently processes large-scale time-series datasets with moderate computational complexity. By performing computations on individual sliding windows, the overall computational cost is effectively reduced.

3.7. **Evaluation model.** In real-time anomaly detection, the data are highly imbalanced, as anomalous events occur rarely. Under this setting, accuracy can be misleading, since a model may achieve high accuracy by predominantly predicting the normal class. Therefore, this study does not rely on accuracy but instead focuses on four evaluation metrics that are more appropriate for imbalanced data and operational requirements: precision, recall, F1-score, and AUC. Precision measures the proportion of correct alarms among all issued alarms, while recall quantifies the proportion of true anomalies that are successfully detected. As these two objectives are often conflicting, the F1-score is adopted as a harmonic mean to provide a single balanced measure between false-alarm reduction and anomaly miss minimization. In the experiments, decision thresholds are optimized by maximizing the F1-score on the validation set. Model performance is reported using precision, recall, F1-score, and AUC, with F1-score serving as the primary

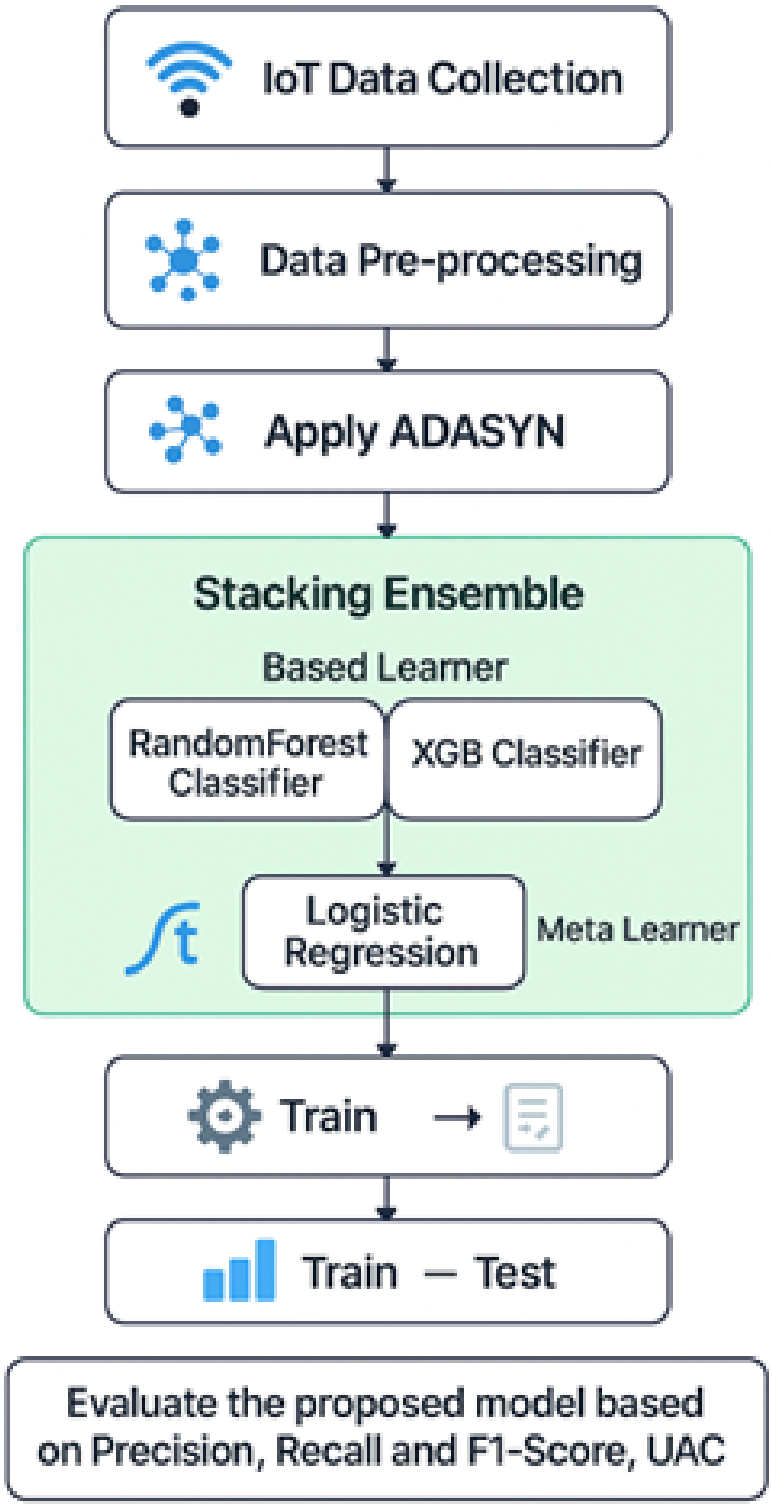

FIGURE 5. Overview of the proposed Stacking Ensemble–based anomaly detection method using IoT data.

metric for model comparison. All metrics are computed per variable and averaged to provide an overall performance assessment.

Based on the literature review, the proposed Stacking Ensemble model was compared with several existing approaches [15], [16], [17] that also employ AI and IoT technologies for anomaly detection. Such a comprehensive comparison helps to clarify the relative performance of the proposed model with respect

Algorithm 1 Proposed scheme for Anomaly Detection using Stacking Ensemble

Input:
- $X = (x_1, x_2, \ldots, x_M)$: Time series data.
- T: Length of the sliding window.
- Φ: Trained Stacking Ensemble model.
- θ: Decision threshold for anomaly detection.

Output:
- $A_M = [a_1, a_2, \ldots, a_M]$: Binary sequence indicating anomaly status (0: normal, 1: anomalous) at each time point.

Initialization: $A_M = [0, 0, \ldots, 0]$
for each time point t from 1 to M **do**
  if $t < T$ **then**
    $a_t \leftarrow a_{t-1}$
  else
    $X_t \leftarrow (x_{t-T+1}, \ldots, x_t)$
    Preprocess X_t: Normalize and reshape X_t to fit the input format of Φ.
    Compute $\hat{y}_t \leftarrow \Phi(X_t)$
    if $\hat{y}_t > \theta$ **then**
      $a_t \leftarrow 1$
    else
      $a_t \leftarrow 0$
    end if
  end if
end for
return A_M

FIGURE 6. Pseudocode of the proposed Stacking Ensemble–based anomaly detection algorithm.

to state-of-the-art methods and to identify potential areas for further improvement. The algorithms used for comparison are summarized as follows:

- **XGBoost:** A gradient boosting algorithm known for its ability to efficiently handle large-scale datasets. It has been widely applied in various domains, including anomaly detection, due to its strong predictive performance.
- **Transformer:** An advanced deep learning model that employs an attention mechanism to detect anomalies in time-series data through contextual modeling.
- **CNN + LSTM:** A hybrid architecture that combines Convolutional Neural Networks (CNNs) for spatial feature extraction with Long Short-Term Memory (LSTM) networks for capturing temporal dependencies, thereby improving anomaly detection performance in time-series data.

3.8. **Hardware configuration used.** To execute our experiment, we selected the Kaggle platform because of its ability to configure and deploy easily and quickly. The configuration used for the training model is an Intel Xeon with a CPU @ 2.20GHz, 2 cores, 4 threads, and 31 GiB RAM, which supports virtualization technology (KVN). With this capacity, we will ensure model training with large data in a 180-day dataset.

4. Experimental result and conclusion.

4.1. **Experimental results.** The study assesses how well the machine learning models perform using four different datasets, each covering a different time span: 15 days, 30 days, 60 days, and 180 days. This allows researchers to see how the models handle varying amounts of data and timeframes.

The experimental results presented in Tables 4 and 5 show that the proposed Stacking Ensemble model consistently outperforms all other models across a variety of datasets and evaluation metrics. The model achieves an average precision of 0.97, recall of 0.96, F1-score of 0.96, and an AUC of 1.00, demonstrating its strong ability to balance the detection of minority-class patterns while minimizing false

TABLE 4. Performance comparison of anomaly detection models on datasets with different time spans.

Model	Dataset	Precision	Recall	F1-Score	AUC
XGBoost	15 days	0.99	1.00	0.99	1.0000
	30 days	0.98	0.99	0.99	0.9999
	60 days	0.95	0.96	0.95	1.0000
	180 days	0.33	0.90	0.48	0.9970
CNN - LSTM	15 days	0.41	1.00	0.58	0.9969
	30 days	0.27	0.98	0.42	0.9967
	60 days	0.22	1.00	0.36	0.9983
	180 days	0.21	0.98	0.35	0.9951
Transformer	15 days	0.92	0.94	0.93	0.9998
	30 days	0.69	0.74	0.71	0.9986
	60 days	0.36	0.77	0.49	0.9975
	180 days	0.41	0.84	0.55	0.9976
Stacking Ensemble (Proposed Model)	15 days	1.00	1.00	1.00	1.0000
	30 days	1.00	0.99	1.00	0.9968
	60 days	1.00	0.99	0.99	0.9925
	180 days	0.86	0.84	0.85	0.9997

TABLE 5. Average performance metrics of anomaly detection models across all datasets.

Model	Precision	Recall	F1-Score	AUC
XGBoost	0.81	0.96	0.85	1.00
CNN – LSTM	0.28	0.99	0.43	1.00
Transformer	0.60	0.82	0.67	1.00
Stacking Ensemble (Proposed Model)	0.97	0.96	0.96	1.00

positives. Notably, the Stacking Ensemble maintains high performance across all datasets, including the challenging 180-day dataset, where it achieves an F1-score of 0.85, which is significantly higher than that of the second-best model, Transformer, which attains an F1-score of only 0.55. Compared with traditional machine learning methods (e.g., XGBoost) and deep learning models (e.g., CNN–LSTM and Transformer), the Stacking Ensemble leverages the strengths of multiple base learners to achieve better generalization and effectively address the challenges posed by imbalanced data. Its adaptability and robustness make it well suited for long-term time-series analysis, particularly under highly imbalanced data conditions. These results confirm the effectiveness of the proposed Stacking Ensemble as a reliable and high-performance approach for anomaly detection and classification tasks.

To further validate the performance of the proposed model, the results obtained from the 15-day dataset are visualized using temperature-based time-series data, as illustrated in Figures 6 and 7. Figure 6 provides an overview of anomalous events occurring between 2024-04-01 and 2024-04-15, where ground-truth anomalies are indicated by red markers and the predicted anomaly regions are highlighted in green. The proposed model successfully identifies two days with anomalous events, demonstrating the capability of the Stacking Ensemble to detect steam valve leakage in industrial ovens. Figure 7 presents a more detailed view of a specific anomalous event, including the actual and predicted start and end times. These visualizations further confirm the accuracy of the proposed model in detecting anomalies over short time horizons and highlight its potential for reliable anomaly prediction in long-term monitoring scenarios.

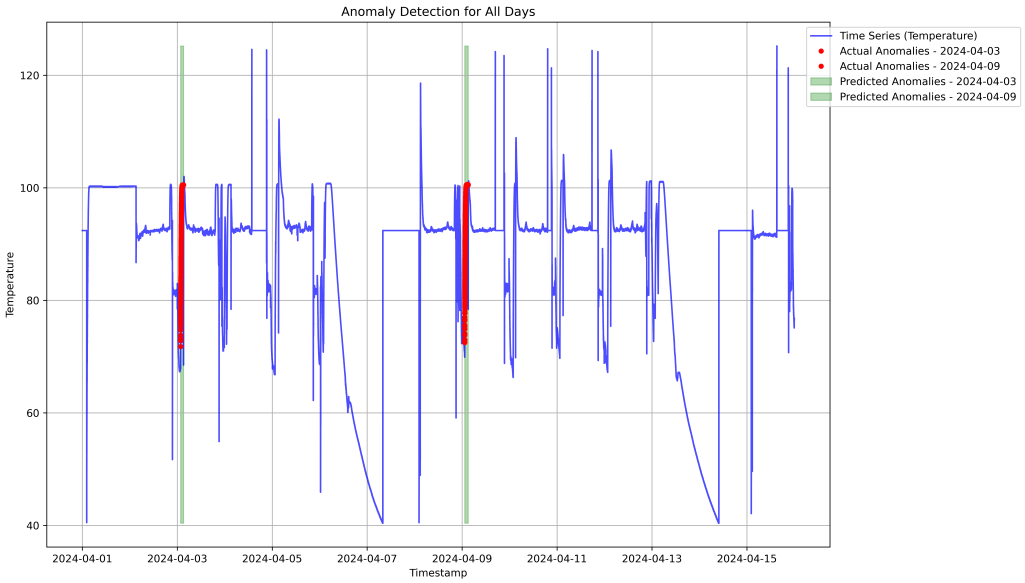

FIGURE 7. Visualization of predicted anomalies based on 15 days of data.

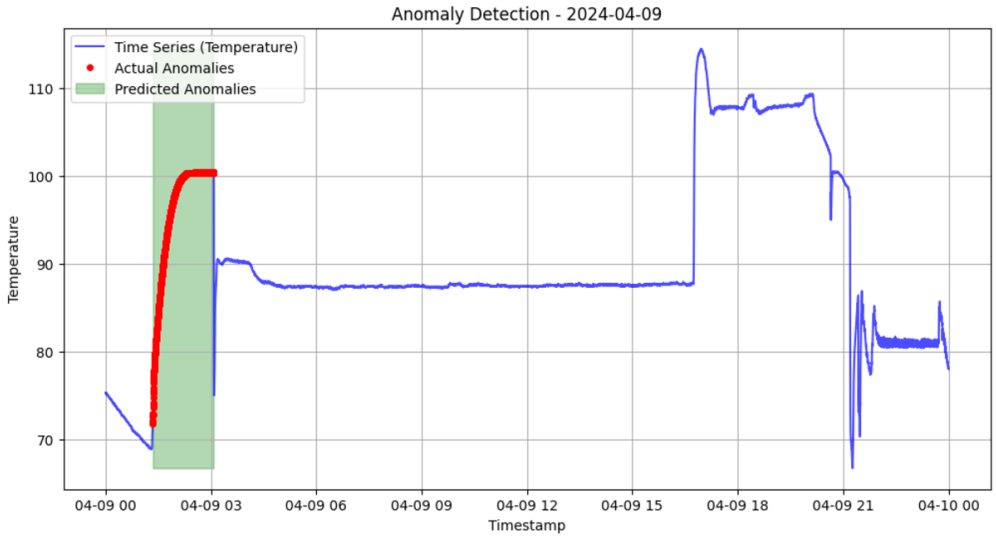

FIGURE 8. Illustrates the predicted anomalies and the duration of steam valve leakage for a single day.

4.2. **Conclusion.** The experimental results demonstrate that the proposed model is an effective approach for anomaly detection in industrial oven systems. The proposed method not only outperforms traditional machine learning techniques but also achieves superior performance compared with state-of-the-art deep learning models. The strength of the proposed model lies in its ability to effectively balance high precision in identifying anomalies, including rare events, while minimizing false alarms. Performance is evaluated using key metrics such as precision, recall, F1-score, and AUC (Area Under the ROC Curve), as reported in detail in Table 5.

In addition, the proposed model demonstrates stable performance across all datasets, particularly in long-term analyses. Notably, the model achieves an F1-score of 85% on the 180-day dataset, outperforming competing approaches, including XGBoost and Transformer. These results confirm the capability of the Stacking Ensemble to detect anomalies effectively while handling large-scale and complex industrial time-series data.

By combining the strengths of multiple base learners, the Stacking Ensemble model provides robust and reliable performance for time-series analytics in industrial environments. This ensemble strategy

enhances model adaptability to complex data distributions, severe class imbalance, and long-term monitoring scenarios, while improving robustness and mitigating the limitations of individual component models. Furthermore, the flexibility of the Stacking Ensemble facilitates the integration of new models and supports evolving data analytics requirements. Consequently, the application of the proposed approach for anomaly detection has the potential to improve reliability, safety, and operational efficiency in industrial production processes.

Despite the promising results, this study has several limitations. First, anomaly labeling relies on expert knowledge, which may introduce subjectivity and limit scalability when deploying the framework across different industrial environments. Second, the current study focuses on a single failure mode, namely steam valve leakage, under standby operating conditions. The proposed framework has not yet been validated for other fault types or operational states of industrial ovens. Third, the approach is based on supervised learning and requires labeled anomaly data, which may be scarce in real-world industrial settings. Finally, the model is trained offline and does not currently incorporate online learning or concept drift adaptation, which may affect long-term robustness under changing operating conditions. These limitations highlight important directions for future research and practical deployment.

5. **Future research.** This section outlines potential research directions to further improve the proposed system in real-world applications.

Future research will focus on deploying the anomaly detection system in real-world industrial environments, with particular emphasis on real-time monitoring of industrial ovens. To achieve this objective, the Stacking Ensemble model will be integrated with streaming platforms such as Azure Stream Analytics and Apache Kafka. These platforms are responsible for collecting and processing continuous data streams from sensors installed on industrial ovens. After preprocessing, the data will be transmitted to the Stacking Ensemble model for real-time analysis, enabling immediate anomaly detection. This solution is expected to improve the reliability, safety, and operational performance of industrial ovens, thereby contributing to enhanced productivity.

In addition, future research will explore the application of online learning techniques to enhance the adaptability of the anomaly detection model. Online learning allows the model to automatically update its parameters based on incoming data streams, ensuring sustained accuracy and reliability under changing operating conditions. Key advantages of this approach include rapid adaptation to new data, effective detection of previously unseen anomalies, and improved utilization of computational resources. The adoption of online learning is therefore expected to significantly enhance the performance and flexibility of anomaly detection systems in industrial environments.

Overall, these research directions are expected to contribute to the development of intelligent monitoring systems for industrial ovens, support the optimization of maintenance processes, and reduce operational risks in food production facilities.

6. **Acknowledgements.** This research was supported by The VNUHCM-University of Information Technology's Scientific Research Support Fund. The data used in this study were provided by Marel company under confidentiality agreements and are not publicly available.

7. **Data availability.** The data that has been used is confidential.

REFERENCES

[1] "Anomaly Detection Market Size, Share & Industry Trends Analysis Report By Deployment, By Technology, By Component." Accessed: Oct. 09, 2025. [Online]. Available: `https://www.researchandmarkets.com/reports/5869061/anomaly-detection-market-size-share-and-industry`

[2] R. Kabore, A. Kouassi, R. N'goran, O. Asseu, Y. Kermarrec, and P. Lenca, "Review of Anomaly Detection Systems in Industrial Control Systems Using Deep Feature Learning Approach," *ENG*, vol. 13, no. 1, pp. 30–44, 2021, doi: 10.4236/eng.2021.131003.

[3] R. P. Singh, M. B. Sorte, and M. M. Jagtap, "Capturing Steam Energy Leaks in the Steam Distribution Network Using an Integrated Method: A Case Study of a Petroleum Refinery," *J. Inst. Eng. India Ser. C*, vol. 103, no. 3, pp. 509–518, Jun. 2022, doi: 10.1007/s40032-021-00793-6.

[4] P. Yan *et al.*, "A Comprehensive Survey of Deep Transfer Learning for Anomaly Detection in Industrial Time Series: Methods, Applications, and Directions," *IEEE Access*, vol. 12, pp. 3768–3789, 2024, doi: 10.1109/ACCESS.2023.3349132.

[5] M. A. Belay, S. S. Blakseth, A. Rasheed, and P. Salvo Rossi, "Unsupervised Anomaly Detection for IoT-Based Multivariate Time Series: Existing Solutions, Performance Analysis and Future Directions," *Sensors*, vol. 23, no. 5, p. 2844, Mar. 2023, doi: 10.3390/s23052844.

[6] M. H. Ho *et al.*, "Ensemble Learning for Multi-Label Classification with Unbalanced Classes: A Case Study of a Curing Oven in Glass Wool Production," *Mathematics*, vol. 11, no. 22, p. 4602, Nov. 2023, doi: 10.3390/math11224602.

[7] N. Alghanmi, R. Alotaibi, and S. M. Buhari, "Machine Learning Approaches for Anomaly Detection in IoT: An Overview and Future Research Directions," *Wireless Personal Communications*, vol. 122, no. 3, pp. 2309–2324, Feb. 2022, doi: 10.1007/s11277-021-08994-z.

[8] A. Abusitta *et al.*, "Deep learning-enabled anomaly detection for IoT systems," *Internet of Things*, vol. 21, p. 100656, Apr. 2023, doi: 10.1016/j.iot.2022.100656.

[9] M. Pota, G. De Pietro, and M. Esposito, "Real-time anomaly detection on time series of industrial furnaces: A comparison of autoencoder architectures," *Engineering Applications of Artificial Intelligence*, vol. 124, p. 106597, Sep. 2023, doi: 10.1016/j.engappai.2023.106597.

[10] T.-X.-H. Nguyen *et al.*, "AI-Driven Security Solutions for Industrial IoT: Challenges and Future Directions," *J. Inf. Hiding Multimedia Signal Process.*, vol. 16, no. 3, pp. 1002–1011, Sep. 2025.

[11] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 15:1–15:58, Jul. 2009, doi: 10.1145/1541880.1541882.

[12] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," *Internet of Things*, vol. 19, p. 100568, Aug. 2022, doi: 10.1016/j.iot.2022.100568.

[13] G. Pang *et al.*, "Deep Learning for Anomaly Detection: A Review," *ACM Computing Surveys*, vol. 54, no. 2, pp. 1–38, Mar. 2022, doi: 10.1145/3439950.

[14] P. Malhotra *et al.*, "Long Short-Term Memory Networks for Anomaly Detection in Time Series," *Computational Intelligence*, 2015.

[15] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," *IEEE Access*, vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.

[16] T. Nguyen-Da, P. Nguyen-Thanh, and M.-Y. Cho, "Real-time AIoT anomaly detection for industrial diesel generator based on efficient deep learning CNN–LSTM in Industry 4.0," *Internet of Things*, vol. 27, p. 101280, Oct. 2024, doi: 10.1016/j.iot.2024.101280.

[17] S. Tuli, G. Casale, and N. R. Jennings, "TranAD: Deep Transformer Networks for Anomaly Detection in Multivariate Time Series Data," arXiv:2201.07284, 2022, doi: 10.48550/arXiv.2201.07284.

[18] J. Lind, "A Work Project presented as part of the requirements for the award of a Master's degree in Business Analytics," Nova School of Business and Economics.

[19] D. H. Tran *et al.*, "Self-Supervised Learning for Time-Series Anomaly Detection in Industrial Internet of Things," *Electronics*, vol. 11, no. 14, p. 2146, Jul. 2022, doi: 10.3390/electronics11142146.

[20] D. L. Whaley, "The Interquartile Range: Theory and Estimation," p. 1030, 2005.

[21] H. He *et al.*, "ADASYN: Adaptive Synthetic Sampling Approach for Imbalanced Learning," in *Proc. IEEE IJCNN*, Jun. 2008, pp. 1322–1328, doi: 10.1109/IJCNN.2008.4633969.