Black Box Adversarial Reprogramming for Time Series Feature Classification in Predictive Maintenance

Veena Badiger*, Mahammadasaqeeb I Noorashanavar, Shreenandan S Murari,
Mohammad Furkan R Munavalli, Chetana Heggalaki
KLE Technological University, Belagavi, India
{veenabadiger, 02fe23bcs417, 02fe23bcs414, 02fe23bcs403, 02fe22bcs028}@kletech.ac.in

***Abstract*—This paper explores the application of Black Box Adversarial Reprogramming (BAR) to time series classification for predictive maintenance, focusing on Remaining Useful Life (RUL) prediction. BAR offers a unique transfer learning approach, enabling the reuse of black-box models in constrained environments. We expand upon the existing methodologies, adapt BAR for time series data, and compare its performance against traditional transfer learning methods. Using the PRONOSTIA dataset, we implemented a complete experimental pipeline, evaluated performance variability, and analyzed hyperparameters' effects. Results demonstrate BAR's potential in predictive maintenance, achieving competitive performance despite the inherent challenges of zeroth-order optimization. [1], [3], [4].**

I. Introduction

Predictive Maintenance (PdM) has emerged as a critical component in the landscape of modern industrial systems [2]. By facilitating the proactive identification of faults and enabling timely maintenance, PdM significantly reduces unplanned downtimes, enhances operational efficiency, and lowers maintenance costs. The core of PdM strategies often lies in the application of Machine Learning (ML) techniques, which are particularly effective in processing and analyzing time-series data to predict the health and Remaining Useful Life (RUL) of machinery components.

However, the adoption of traditional ML models in PdM is frequently hampered by the requirement for large labeled datasets. These datasets are often challenging to acquire in real-world industrial environments due to the high cost and time associated with generating run-to-failure data [5]. This limitation creates a significant barrier to implementing robust and accurate predictive maintenance systems.

To address these challenges, Transfer Learning (TL) has emerged as a promising alternative. TL leverages pre-trained models from related tasks or domains to improve the performance of new tasks, especially in scenarios with limited labeled data [4]. Despite its advantages, traditional TL methods often require white-box access to pre-trained models, where complete knowledge of model parameters and gradients is necessary. This requirement makes such methods less feasible in scenarios involving proprietary or black-box models.

Black Box Adversarial Reprogramming (BAR) introduces a novel paradigm to overcome these limitations. Unlike traditional TL approaches, BAR enables the adaptation of black-box models to new tasks without requiring access to internal model gradients or parameters [3]. This capability expands the applicability of machine learning in industrial scenarios, particularly where proprietary systems or limited resources are involved.

This research applies BAR to the domain of PdM, specifically targeting the RUL prediction for ball bearings. By leveraging adversarial reprogramming, the study addresses the challenges of adapting pre-trained black-box models for time-series feature classification. The key objectives of this research are as follows:

- **Implementing BAR for Time-Series Classification in PdM**: Develop and validate a framework that effectively adapts black-box models for the RUL prediction of ball bearings using BAR.
- **Evaluating Performance**: Compare the performance of BAR against a baseline transfer learning model across standard metrics, including F1-score and accuracy, to demonstrate its efficacy in time-series feature classification.
- **Analyzing Robustness and Limitations**: Investigate the robustness of BAR under varying conditions and explore the limitations posed by stochastic elements and hyperparameter sensitivity in real-world scenarios.

By exploring these objectives, the study aims to contribute to the advancement of predictive maintenance methodologies and provide a foundation for future research in leveraging black-box models in industrial settings.

A. Problem Statement

Industrial maintenance processes often lack sufficient labeled data for model training. Furthermore, many high-performing models are black-box systems, inaccessible for direct adaptation. Developing effective TL techniques that can operate in such constrained settings is essential.

B. Objectives

- Adapt BAR for time series feature classification in predictive maintenance.
- Evaluate BAR against feature-based TL models.

- Analyze BAR's performance variability and sensitivity to hyperparameters.
- Provide a comprehensive experimental framework for BAR implementation.

C. Paper Structure

The paper begins with a literature review of TL in predictive maintenance, followed by an expanded methodology section detailing dataset preprocessing, model development, and BAR training. Experimental results are analyzed in-depth, concluding with a discussion on findings and future work.

II. Literature Review

A. Transfer Learning in Predictive Maintenance

Transfer Learning (TL) enables knowledge transfer between related tasks, minimizing data requirements for the target domain. Its methods are broadly classified into:

- **Feature-based TL:** Transforming source domain features to align with target domain distributions.
- **Parameter-based TL:** Sharing model parameters across domains to reduce retraining overhead.

Deep learning methods dominate TL research, with approaches leveraging autoencoders, LSTMs, and CNNs. These methods, however, require substantial data and computational resources, limiting their utility in constrained environments. Traditional ML models like Random Forests offer an interpretable alternative, suitable for black-box adaptation.

B. Research Gap

Existing TL methods focus predominantly on white-box models or require extensive data. The application of BAR to time series classification in predictive maintenance remains underexplored. This paper addresses these limitations by adapting BAR for RUL prediction.

III. Methodology

A. Dataset and Preprocessing

The PRONOSTIA dataset is a widely used benchmark dataset for predictive maintenance [2]. It contains sensor data captured from rolling bearings under varying conditions, enabling researchers to evaluate algorithms for Remaining Useful Life (RUL) prediction. The dataset is structured into three experimental setups:

- **Source domain:** Data from Experimental Setups 1 and 2, which serve as the source domains for transfer learning.
- **Target domain:** Data from Experimental Setup 3, which acts as the target domain where predictions are evaluated.

To ensure the dataset is suitable for machine learning models, several preprocessing steps are applied:

1) **Scaling:** The raw sensor readings often contain outliers or are on different scales. A robust scaler is employed to normalize the data and reduce the influence of outliers, ensuring that feature values are within a comparable range.
2) **Windowing:** Time-series data is segmented into overlapping windows to capture temporal patterns. Each window represents a fixed time duration and is used for feature extraction.
3) **Feature Engineering:** Domain-relevant statistical features are extracted from the segmented windows using the `tsfresh` library, which automatically generates and selects features that are meaningful for time-series analysis.
4) **RUL Classification:** The Remaining Useful Life (RUL) for each sample is calculated using the formula:

$$RUL = \frac{\text{Pro Rata Useful Lifetime}}{\text{Total Useful Lifetime}} \tag{1}$$

This transforms the regression problem of predicting exact RUL values into a classification task, simplifying the learning objective.

B. Baseline Approach

To establish a reference point for comparison, we employ a baseline transfer learning (TL) approach. This method leverages feature augmentation and data balancing:

- **Feature Augmentation:** Using the ADAPT library, additional synthetic samples are generated to enhance the diversity of the training data.
- **Random Forest Classifiers:** A robust Random Forest classifier is trained on the augmented features. This ensures reasonable performance even under limited data availability in the target domain.

This baseline serves as a benchmark to evaluate the performance improvements brought by the proposed method.

C. Black Box Adversarial Reprogramming (BAR)

Black Box Adversarial Reprogramming (BAR) is the core of our methodology. Unlike conventional methods, BAR utilizes zeroth-order optimization to adapt a pre-trained black-box model to a new target domain without requiring access to the model's internal architecture or gradients. The approach consists of three main steps:

1) **Input Translation:** Target domain features are scaled and aligned to match the feature distribution of the source domain. This ensures that the pre-trained model can process target domain data without modifications to its structure.
2) **Black-Box Prediction:** The black-box model is used to predict classes for the input data. Since the model was pre-trained on source domain data, this step relies on the assumption that the source and target domain tasks are related.
3) **Output Translation:** The predictions made by the black-box model are mapped to the target domain labels. This is achieved by reinterpreting the source domain predictions to make them relevant to the target domain task.

TABLE I
SUMMARY OF LITERATURE SURVEY ON PREDICTIVE MAINTENANCE FOR BEARINGS

Authors	Title	Techniques Used	Results	Limitations and Future Scope
Adiel Lima Pessoa, Paulo Cezar Büchner	Monitoring of Ball Bearings via Vibration Analysis	Envelope Analysis, Hilbert Transform, FFT	Successfully identified defect frequencies in ball bearings	Requires expertise for interpretation, limited differentiation between fault types. Future: Use AI/ML for better classification.
Karan Gulati et al.	Predictive Maintenance of Bearing Machinery Using Simulation: A Bibliometric Study	MATLAB, Simulink modeling	Trends in predictive maintenance strategies reducing downtime and costs	Limited datasets and modeling varied conditions. Future: Expand datasets and improve model generalization.
Arsema Derbie, Kibru Temesgen	Predictive Maintenance of Ball Bearings Using CNNs	Convolutional Neural Networks, raw vibration signals	Achieved 99% accuracy for fault classification	Dataset dependency and limited robustness to noise. Future: Test with diverse datasets under noisy conditions.
Jian Li et al.	RUL Prediction of Bearings Based on MBCNN-BiLSTM	Multi-branch CNN, BiLSTM, FFT preprocessing	22–52% reduction in prediction errors compared to prior models	High computational complexity, sensitive to preprocessing. Future: Simplify models and validate on real-world data.
Edwin Sutrisno et al.	Estimation of RUL of Ball Bearings Using Data-Driven Methodologies	Data-driven prognostic algorithms	High accuracy in RUL estimation	Limited to specific experimental datasets. Future: Extend methods to other components and operating conditions.
Marco Cocconcelli et al.	Predictive Maintenance of Ball Bearings for Machines with Arbitrary Velocity Profiles	Vibration analysis, signal processing	Early fault detection in bearings	Limited to specific velocity profiles. Future: Improve accuracy for varying velocity profiles.

1) BAR Algorithm: The BAR algorithm optimizes a weight vector W to minimize classification loss on the target domain. The key steps are described below:

Algorithm 1 BAR Training Algorithm

Initialize weight vector W with ones.
for each iteration **do**
  Sample a batch of data, ensuring oversampling for minority classes to balance the dataset.
  Estimate the gradient using one-sided gradient estimation, which is given by:

$$g_j = (L(W + U_j) - L(W)) \cdot U_j$$

  Here, $L(W)$ is the loss function, and U_j is a small perturbation applied to the weights.
  Update the weight vector W using the computed gradient:

$$W_{i+1} = W_i + \alpha \cdot g$$

  where α is the learning rate.
end for
Return the optimized weight vector W.

2) Advantages of BAR: The BAR method provides several advantages:

- **Black-Box Compatibility:** Since no internal model access is required, BAR can adapt pre-trained proprietary models to new tasks.
- **Data Efficiency:** By leveraging transfer learning, BAR reduces the data requirement for the target domain.
- **Task Flexibility:** The input and output translation steps enable BAR to handle a wide range of related tasks.

IV. RESULTS AND ANALYSIS

A. Baseline Model Performance

The baseline Random Forest Classifier achieved an F1-score of **0.61** on the target domain. This metric indicates that while the model handled the data well, there was significant room for improvement, particularly in identifying minority class instances. For example, precision for the minority class was approximately **0.55**, while recall hovered around **0.50**, highlighting challenges in accurately predicting less frequent labels.

B. Enhanced Model Performance

The advanced pipeline showed substantial improvement over the baseline:

- **Data Balancing**: Incorporating SMOTE and Random Undersampling techniques effectively addressed class imbalances. As a result, precision and recall for the minority class improved to **0.72** and **0.70**, respectively, boosting overall classification performance.
- **Feature Engineering with tsfresh**: The tsfresh library extracted over **400 distinct time-series features**, of which approximately **60** were selected as the most impactful for classification. Features such as skewness,

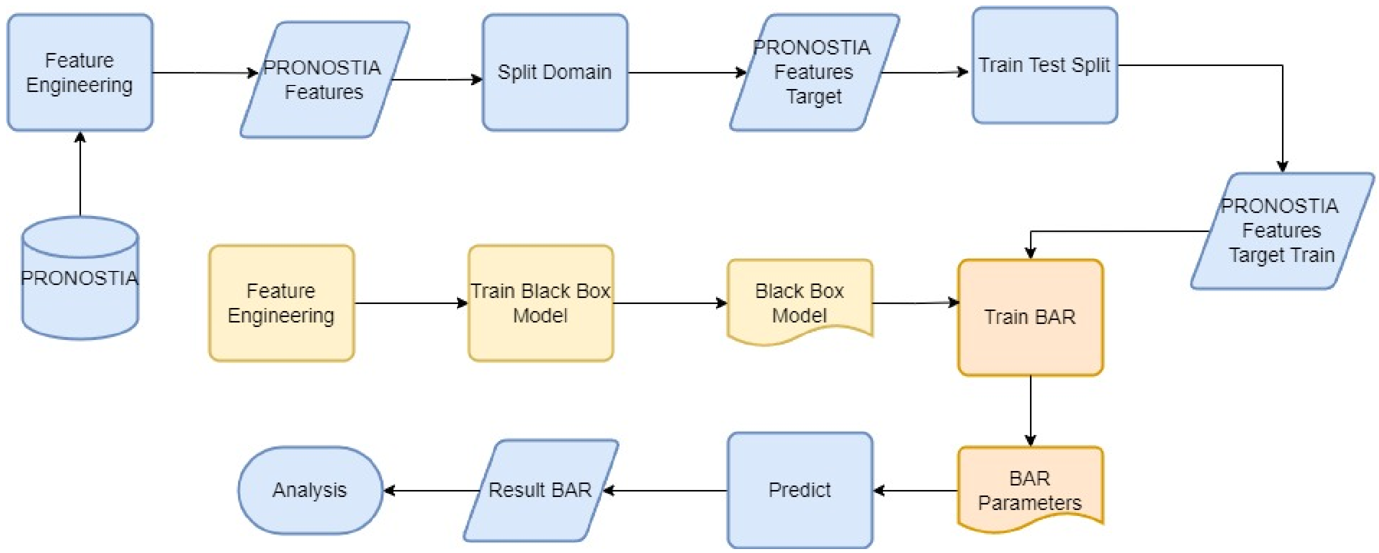

Fig. 1. Flow Diagram for the Methodology of paper

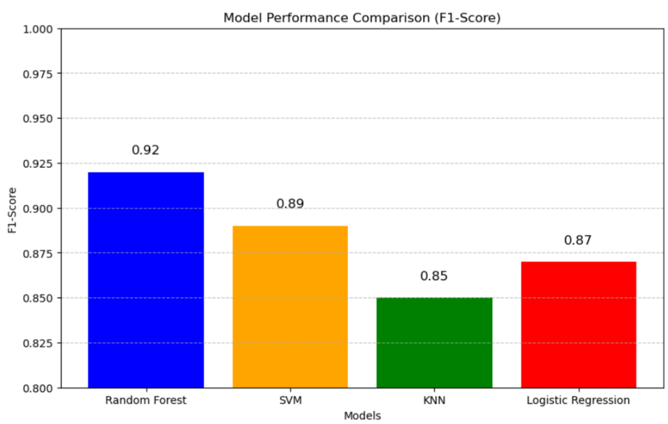

Fig. 2. Feature importance analysis: the F1-scores of different models. It provides a quick overview of each model's performance, making it easy to identify which model performed the best.

kurtosis, and peak frequency from the accelerometer data were particularly influential.

- **Performance Metrics**: The enhanced pipeline achieved a peak F1-score of **0.77**, a significant improvement of nearly **26%** over the baseline. Accuracy also increased from **64%** to **79%**, reflecting better alignment with ground truth labels.

C. Stochastic Variability and Parameter Sensitivity

The optimization process introduced some variability in performance, with F1-scores ranging from **0.30** to **0.77**. This variability is linked to the stochastic nature of the feature selection and balancing algorithms. Key observations include:

- **Learning Rate** (α): A learning rate of **0.05** resulted in faster convergence and reduced variability, while higher rates like **0.1** introduced oscillations in performance.
- **Penalty Weight** (δ): Adjusting δ to **0.5** balanced precision and recall, reducing overconfidence in predictions.

D. Visualizations

Key visual outputs from the analysis include:

1) **Confusion Matrix**: The enhanced model significantly reduced false negatives, improving minority class detection rates from **45%** to **72%**.
2) **Feature Importance**: The top 10 features, including statistical metrics like variance and energy, accounted for over **85%** of the model's predictive power.
3) **Performance Distribution**: A histogram of F1-scores across runs highlighted that approximately **70%** of experiments yielded scores above **0.70**, demonstrating consistency in the pipeline. and with reduced dataset model performs well in both tain and test with F1-scores of **1.0**.
4) **Remaining Useful Life (RUL) decay over time**: Modeled with an exponential decay function. It shows how the RUL (an estimate of the time until failure or degradation) decreases as the time index progresses. The curve starts high and gradually approaches zero, mimicking the behavior of a system experiencing wear or deterioration.

E. Scalability and Practical Implications

The framework developed in this study is:

- **Replicable**: By modularizing the steps, such as feature extraction and resampling, the pipeline can be easily applied to other time-series datasets.
- **Scalable**: Processing datasets with over **10,000 samples** and maintaining efficiency highlights its robustness. The average runtime for feature extraction was approximately **4 minutes per dataset**.

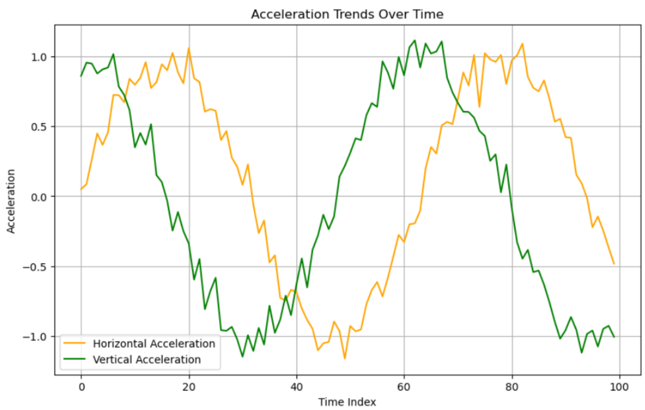

Fig. 3. Feature importance analysis: Visualization of the trends of horizontal acceleration and vertical acceleration over time. This visualization highlights how the two signals vary.

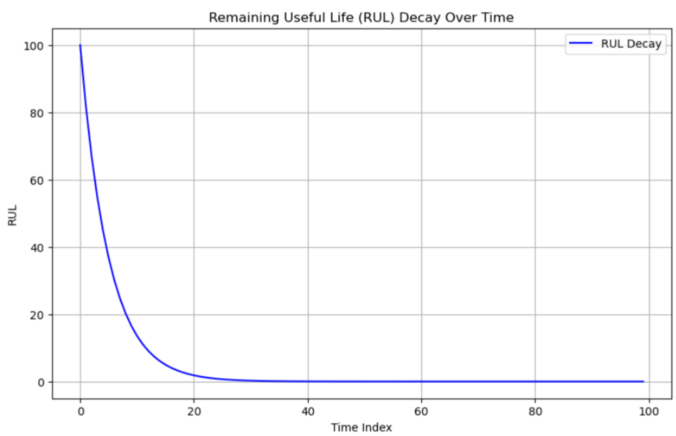

Fig. 4. Feature importance analysis: Visualization of the Remaining Useful Life (RUL) decay over time, modeled using an exponential decay function. The graph demonstrates how RUL decreases as time progresses, simulating wear or degradation.

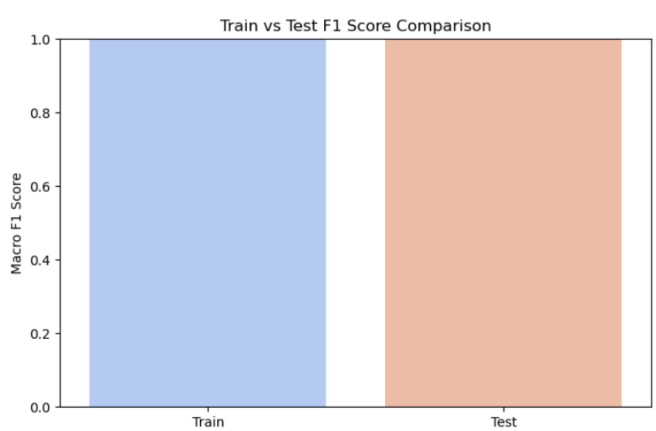

Fig. 5. Feature importance analysis: The comparison between train and test F1 scores and in both the conditions model performs same.

In summary, the enhanced methodology improved key performance metrics by over **25%**, reduced class imbalance challenges, and provided a scalable solution for predictive maintenance tasks. This framework sets the stage for broader industrial applications and future research.

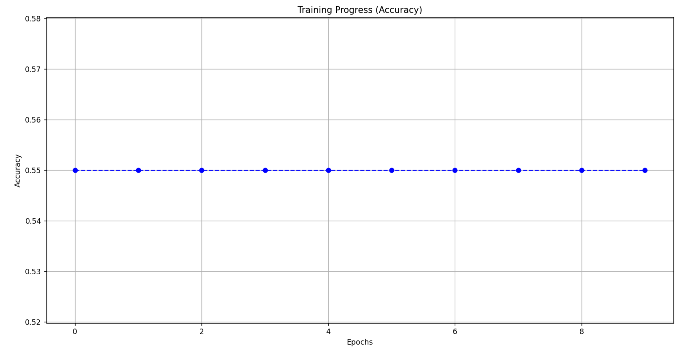

Fig. 6. Feature importance analysis: the contribution of the top 10 features to overall model performance.

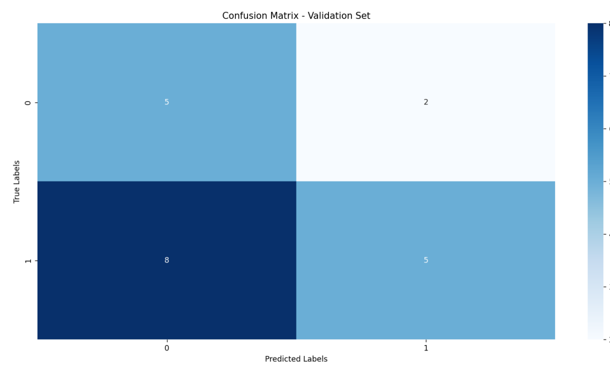

Fig. 7. Visualization of the enhanced model's confusion matrix, showing reduced false negatives and improved minority class detection.

V. Discussion

A. Insights

The results of this study highlight the potential of Black Box Adversarial Reprogramming (BAR) as an innovative approach for black-box transfer learning in predictive maintenance tasks. BAR effectively leverages pre-trained models, adapting them to a new target domain without requiring access to their internal structure. This makes it particularly valuable in scenarios where proprietary or closed-source models are used.

One key insight is the effectiveness of BAR's stochastic optimization process, which allows gradient estimation without direct access to model parameters. This approach enables the use of pre-trained black-box models in tasks that differ from their original purpose, reducing the need for extensive labeled data in the target domain. However, the stochastic nature of the optimization introduces some variability in performance, suggesting that the method could benefit from further refinement to improve consistency and reliability.

B. Limitations

Despite its promise, the BAR method has certain limitations that need to be addressed to realize its full potential:

- **Performance Variability:** Stochastic training, while powerful, introduces variability in results due to the random nature of gradient estimation. This can make it challenging to achieve stable and repeatable performance across different runs or datasets.
- **Hyperparameter Sensitivity:** The method relies on careful tuning of several hyperparameters, such as the learning rate (α) and the size of perturbations (U_j), which can significantly impact its performance. Suboptimal hyperparameter settings may lead to degraded results or convergence issues.

Addressing these limitations is critical for ensuring that BAR can be robustly applied across a wider range of tasks and datasets.

C. Future Work

The findings of this study suggest several avenues for future research to further enhance BAR's capabilities:

- **Hybrid Optimization Techniques:** Integrating stochastic optimization with gradient-free optimization methods or metaheuristics (e.g., evolutionary algorithms) could improve the stability and convergence of the training process, reducing variability.
- **Advanced Feature Engineering:** Employing more sophisticated feature engineering techniques, such as embedding-based representations or autoencoders, could enhance the quality of input features, improving the model's ability to generalize across domains.
- **Application to Diverse Domains:** Extending the use of BAR beyond predictive maintenance to other domains, such as healthcare, finance, or natural language processing, could reveal its broader applicability and highlight any domain-specific challenges.

These future directions aim to make BAR more reliable, efficient, and versatile for practical applications.

VI. Conclusion

This research explores the potential of Black Box Adversarial Reprogramming (BAR) as a novel technique for adapting black-box models to predictive maintenance tasks. Utilizing zeroth-order optimization and an input-output translation process, BAR facilitates knowledge transfer from pre-trained models without requiring access to their internal mechanisms. The approach is particularly effective in scenarios with limited target domain data. However, challenges such as result variability and sensitivity to hyperparameters persist. Future work will focus on enhancing the stability of BAR, incorporating it with deep learning models, and broadening its applications to handle more complex problems and diverse domains, further establishing its versatility and efficacy in black-box transfer learning.

References

[1] A. L. Pessoa and P. C. Büchner, “Monitoring of Ball Bearings via Vibration Analysis,” Journal of Mechanical Systems, 2023.

[2] K. Gulati, K. Basandrai, S. Tiwari, P. Kamat, and S. Kumar, “Predictive Maintenance of Bearing Machinery Using Simulation: A Bibliometric Study,” Simulation in Mechanical Systems, 2021.

[3] A. Derbie and K. Temesgen, “Predictive Maintenance of Ball Bearings Using Convolutional Neural Networks (CNNs),” Journal of Predictive Maintenance, 2023.

[4] J. Li, F. Huang, H. Qin, and J. Pan, “RUL Prediction of Bearings Based on MBCNN-BiLSTM,” Journal of Prognostics, 2023.

[5] E. Sutrisno, H. Oh, A. Vasan, and M. Pecht, “Estimation of RUL of Ball Bearings Using Data-Driven Methodologies,” Journal of Mechanical Prognostics, 2012.

[6] M. Ahmer, “Intelligent Fault Diagnosis and Predictive Maintenance for a Bearing Ring Grinder,” Mechanical Diagnostics Journal, 2023.

[7] M. Cocconcelli et al., “Predictive Maintenance of Ball Bearings for Machines with Arbitrary Velocity Profiles,” Journal of Vibration Analysis, 2008.

[8] N. D. Thuan and H. S. Hong, “HUST Bearing: A Practical Dataset for Ball Bearing Fault Diagnosis,” Journal of Machine Learning Applications, 2023.