International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 16s,2025
https://theaspd.com/index.php

Self-Supervised Deep Learning For Predictive Maintenance In Industrial Iot Systems

Dr. Shweta Choudhary[1], Suresh Kumar Y[2], Jayesh Barve[3], Dr. Sanjiv Kumar Jain[4], Nishit Kumar Srivastava[5], Aruna Pavate[6]
[1]Associate Professor, ABES Engineering College, Ghaziabad, Uttar Pradesh 201009, shweta.chaudhary@abes.ac.in
[2]Associate professor, Department of Mathematics, Koneru Lakshmaiah Education Foundation, Hyderabad,500075, Telangana, 500075, suresh.mscf@gmail.com
[3]Assistant Professor, Department of Mechanical Engineering, Medicaps University, Indore (M.P.), 453331, jayesh.barve@medicaps.ac.in
[4]Assistant Professor, Department of Electrical Engineering, Medicaps University, Indore (M.P.), 453331, sanjivkumar.jain@medicaps.ac.in
[5]Senior Assistant Professor, Operations, and IT Department, ICFAI Business School, ICFAI Foundation for Higher Education (IFHE), Hyderabad, nks.ism@gmail.com
[6]Thakur College of Engineering and Technology, India, arunaapavate@gmail.com

Abstract
The rise of Industrial Internet of Things (IIoT) has transformed traditional manufacturing and industrial processes by enabling real-time monitoring, data-driven decision-making, and automation. However, ensuring system reliability through timely fault detection and predictive maintenance remains a key challenge due to the scarcity of labeled data and the complexity of sensor-driven environments. This paper investigates the application of self-supervised deep learning (SSDL) techniques for predictive maintenance in IIoT systems. Unlike supervised learning, self-supervised methods leverage vast amounts of unlabeled sensor data to learn robust feature representations, which can subsequently be fine-tuned for downstream tasks such as fault prediction and anomaly detection. We explore contrastive learning, masked modeling, and temporal pretext tasks adapted to time-series industrial data, and compare their performance on benchmark IIoT datasets. Experimental results demonstrate that SSDL models outperform traditional supervised models under low-label regimes, improve generalization across heterogeneous devices, and reduce dependency on domain-specific feature engineering. The findings suggest that self-supervised deep learning can significantly advance predictive maintenance capabilities in smart factories, leading to reduced downtime, optimized operations, and increased safety.
Keywords: *Self-supervised learning, Predictive maintenance, Industrial IoT, Deep learning, Fault detection, Time-series analysis*

1. INTRODUCTION

The rapid digital transformation of the manufacturing and industrial sectors has given rise to the Industrial Internet of Things (IIoT), which integrates smart sensors, real-time data acquisition, and intelligent computing across physical systems. IIoT enables industries to move toward intelligent automation, data-driven decision-making, and enhanced operational efficiency by connecting machinery, infrastructure, and analytics platforms through robust communication frameworks. As production environments become increasingly complex and interconnected, equipment reliability and process uptime have emerged as critical performance metrics. Traditional maintenance approaches such as reactive and preventive maintenance are no longer sufficient to meet the dynamic needs of modern industry. These methods often lead to unnecessary maintenance actions, overlooked fault symptoms, unplanned downtime, and excessive operational costs.

Predictive maintenance (PdM), which involves forecasting potential equipment failures based on data-driven insights, has been proposed as a superior alternative. Leveraging historical sensor data, PdM aims to predict the Remaining Useful Life (RUL) of assets, detect early degradation patterns, and schedule maintenance actions before catastrophic breakdowns occur. However, despite significant advances in supervised machine learning and deep learning techniques for PdM, these methods are inherently dependent on large volumes of high-quality labeled failure data. In industrial environments, labeled failure events are rare, expensive to annotate, and often domain-specific, making supervised approaches difficult to generalize or scale across different machines and factories. To overcome this label dependency, the emerging paradigm of **self-supervised learning (SSL)** has shown great promise by enabling models to learn meaningful representations from raw, unlabeled data through well-defined pretext tasks.

1.1 Overview of Self-Supervised Learning in IIoT

Self-supervised learning has gained significant traction in computer vision, natural language processing, and time-series analysis due to its ability to extract rich feature representations without requiring human-annotated labels. In the context of IIoT, SSL methods offer an ideal solution to the labeled data scarcity problem by utilizing abundant raw sensor data to train deep neural networks. These models are trained using surrogate tasks—such as predicting masked sensor readings, identifying temporal sequences, or contrasting data augmentations—before being fine-tuned for downstream tasks such as anomaly detection or failure prediction. The ability of SSL models to capture invariant and generalizable features from complex multivariate sensor streams can significantly enhance fault diagnosis and early warning systems in predictive maintenance pipelines.

Recent advances in SSL techniques such as contrastive learning (e.g., SimCLR, MoCo), masked modeling (e.g., MAE, BERT), and temporal sequence modeling (e.g., CPC, TNC) have made them increasingly suitable for industrial applications involving time-series sensor data. When combined with powerful deep architectures like convolutional neural networks (CNNs), transformers, and recurrent neural networks (RNNs), SSL enables scalable, label-efficient, and transferable learning across heterogeneous IIoT environments. This paper explores the adaptation and application of such self-supervised frameworks for predictive maintenance, aiming to establish robust baselines, compare multiple SSL strategies, and demonstrate their advantages over conventional supervised techniques.

1.2 Scope and Objectives

This research aims to investigate the potential of self-supervised deep learning models for predictive maintenance in IIoT systems, with a particular emphasis on multivariate time-series data originating from industrial sensors. The key focus areas include designing pretext tasks suitable for industrial time-series data, evaluating different SSL paradigms under limited label availability, and benchmarking the performance of SSL models against traditional supervised learning baselines.

The specific objectives of this study are as follows:

- To review and classify current self-supervised learning techniques applicable to IIoT time-series data for predictive maintenance tasks.
- To propose and implement self-supervised deep learning architectures based on contrastive, predictive, and masked modeling approaches tailored to IIoT sensor data.
- To evaluate the effectiveness of the proposed SSL models on benchmark industrial datasets under varying levels of label availability.
- To analyze the impact of pretext task selection, model architecture, and fine-tuning strategy on the performance of predictive maintenance systems.
- To provide comparative insights into generalization capabilities, robustness, and practical deployment scenarios of SSL-based PdM frameworks in smart factories.

This research not only broadens the theoretical understanding of self-supervised representation learning in the industrial context but also delivers practical insights for engineers and practitioners aiming to implement next-generation predictive maintenance solutions.

1.3 Author Motivations

The authors were motivated by the growing disconnect between the theoretical advances in deep learning and their practical applicability in industrial systems, particularly due to the scarcity of labeled datasets in PdM tasks. Traditional supervised learning pipelines often assume idealized data availability and curated labels, conditions that rarely hold true in real-world industrial environments characterized by noise, heterogeneity, and lack of annotated faults. As industrial systems generate massive volumes of operational sensor data daily, it becomes imperative to harness this data effectively without relying on costly human annotation or controlled failure scenarios. The compelling promise of self-supervised learning lies in its data efficiency, scalability, and domain adaptability. Drawing inspiration from recent breakthroughs in representation learning and the rising importance of AI-driven maintenance strategies in Industry 4.0, the authors were driven to explore how SSL could be practically adapted to address key bottlenecks in real-world predictive maintenance. The motivation also stemmed from the need to develop more generalized and transferable PdM models that can perform reliably across machines and settings, thus reducing the time and cost of AI deployment in industrial facilities. Furthermore, the authors recognized a critical gap in the literature where SSL methods have been well explored in image and language domains but remain underutilized in the domain of industrial time-series applications. This paper is thus a response to that gap, combining conceptual rigor with practical experimentation to explore novel architectures, training paradigms, and evaluation strategies suitable for IIoT contexts.

1.4 Paper Structure

The remainder of this paper is structured as follows:

In summary, this paper proposes a forward-looking perspective on the application of self-supervised deep learning in predictive maintenance within Industrial IoT ecosystems. By addressing the challenge of labeled data scarcity and proposing scalable, generalizable models, the research aims to lay the foundation for more intelligent, resilient, and cost-effective maintenance strategies. The convergence of IIoT, deep learning, and self-supervision represents a pivotal shift in how industrial systems are monitored and managed, unlocking new possibilities for autonomous fault diagnosis, reduced downtime, and sustainable operational excellence.

2. LITERATURE REVIEW

The integration of deep learning with predictive maintenance (PdM) in Industrial Internet of Things (IIoT) ecosystems has emerged as a transformative approach in achieving smarter, data-driven industrial operations. The ability to detect anomalies, anticipate failures, and forecast the Remaining Useful Life (RUL) of industrial assets is vital for reducing downtime, extending equipment life, and optimizing resource allocation. Over the past decade, extensive research has focused on supervised and semi-supervised learning techniques for PdM; however, the assumption of abundant labeled failure data remains a critical bottleneck in deploying scalable and robust PdM models in real-world environments.

Recent advances in **self-supervised learning (SSL)** offer a compelling solution by enabling the learning of useful data representations from unlabeled data—a plentiful resource in most IIoT systems.

2.1 Supervised Deep Learning for Predictive Maintenance

Historically, predictive maintenance models have relied on supervised machine learning techniques, including support vector machines (SVMs), decision trees, and ensemble models such as random forests and gradient boosting. These methods have shown promise but are limited in their ability to handle high-dimensional, multivariate time-series sensor data prevalent in IIoT. With the rise of deep learning, researchers began to apply convolutional neural networks (CNNs), long short-term memory networks (LSTMs), and autoencoders to learn temporal dependencies and nonlinear representations.

However, the efficacy of these supervised approaches is often constrained by their dependence on large-scale labeled datasets, which are costly, domain-specific, and sometimes impractical to collect in industrial settings. Annotating failure modes in heavy machinery involves expensive downtime and intrusive monitoring, making data-driven model development prohibitive in practice.

2.2 Emergence of Self-Supervised Learning in Industrial Applications

Self-supervised learning has revolutionized data representation in fields such as computer vision and natural language processing, and its recent extension to time-series data and industrial applications has garnered growing interest. SSL learns representations by solving **pretext tasks**—auxiliary objectives designed to mimic supervised learning signals without requiring labels. These tasks include predicting masked segments, contrasting augmented views, forecasting future sensor values, or identifying temporal orderings.

Chen et al. [1] proposed a contrastive predictive maintenance framework using SimCLR-like techniques tailored for IIoT systems. The study demonstrated that contrastive SSL methods can capture machinery degradation patterns and achieve high accuracy even under label-scarce regimes. Similarly, Liu et al. [2] introduced masked signal modeling (MSM) for time-series sensor data and showed that learning to reconstruct masked inputs leads to highly transferable feature embeddings suitable for downstream failure detection.

Alharbi et al. [3] presented a self-supervised anomaly detection framework using temporal consistency as a supervisory signal. Their study applied SSL to cyber-physical systems and highlighted the robustness of self-supervised models in identifying deviations without any fault-specific labels. These developments emphasize the shift from data-hungry supervised learning to data-efficient SSL paradigms.

2.3 Benchmarking SSL Models for IIoT Predictive Maintenance

Several recent studies have investigated different SSL architectures and training paradigms in PdM contexts. Kumar et al. [4] evaluated contrastive and predictive learning tasks on multivariate time-series datasets and found that self-supervised models significantly outperformed supervised baselines in low-label settings. He et al. [5] provided a comprehensive review of deep self-supervised learning methods for time-series analysis in IIoT, highlighting the unique challenges posed by noise, non-stationarity, and heterogeneous sensor modalities.

Rahman and Alazab [6] explored federated self-supervised learning for IIoT edge devices, emphasizing privacy-preserving representation learning. Singh et al. [7] developed an encoder-decoder self-supervised model, SSL-Predict, specifically designed for industrial health monitoring, which used reconstruction-based loss functions to learn degradation features. Their findings confirmed that pretraining on large-scale unlabeled data helps in capturing early fault signatures and boosts generalization.

Zhou and Wang [8] applied contrastive learning to vibration signals from rotating machinery and demonstrated that SSL models could differentiate between early-stage degradation and normal operational patterns without explicit fault labels. Zhang et al. [9] focused on RUL prediction using temporal contrastive methods and showed how SSL improves long-term forecasting accuracy in maintenance scenarios.

Das et al. [10] integrated transformer models with self-supervised learning to develop zero-label predictive maintenance systems, noting that SSL enables transformer-based models to learn context-aware patterns from raw industrial time-series data. Tang et al. [11] applied SimCLR-based learning on IIoT datasets and achieved superior performance over supervised models with only 10% of the labeled data.

2.4 Pretext Tasks and Temporal Representation Learning

The choice of pretext task plays a pivotal role in the success of SSL. Wang and Zhao [12] categorized various pretext tasks applicable in fault diagnosis, including masking, forecasting, context prediction, and surrogate classification. They concluded that selecting a task aligned with downstream objectives enhances transfer performance. Xiao et al. [13] implemented multiple pretext tasks for health monitoring in smart factories and demonstrated that combining temporal and structural supervision yields richer embeddings. Nguyen and Nguyen [14] used autoencoder-based SSL for predictive maintenance, focusing on reconstruction of time-series patterns in IIoT sensor data. Their study showed that autoencoders could detect anomalous patterns when trained on healthy signals using a self-supervised setup. Kim and Lee [15] proposed a learning framework without labels for predictive maintenance and benchmarked SSL against traditional supervised learning models, noting improved robustness to unseen failure modes and reduced overfitting.

2.5 Identified Research Gap

Despite the growing body of research applying SSL to industrial predictive maintenance, several key gaps remain unaddressed. First, most studies are either limited to specific pretext tasks or evaluate models on narrowly scoped datasets, making it difficult to generalize findings across industries. There is a lack of **comprehensive benchmarking** of different SSL approaches—contrastive, masked modeling, predictive coding—on **diverse IIoT datasets**, especially under varying label scarcity conditions.

Second, existing works seldom explore the **generalization and transferability** of SSL models across different machine types, operating environments, or failure modes. In practical IIoT systems, equipment heterogeneity and operational variability are the norms rather than exceptions. Thus, developing SSL frameworks that can adapt to such heterogeneity remains an open challenge.

Third, while the utility of SSL in representation learning has been validated, its **integration into end-to-end predictive maintenance pipelines**—from sensor data ingestion to alert generation—has not been fully investigated. There is limited research on deployment-ready architectures that combine SSL pretraining with task-specific fine-tuning strategies in real-world industrial settings.

Finally, most studies focus on theoretical performance or offline benchmarking, overlooking important aspects like **model interpretability, training efficiency, and system-level integration**. To drive industrial adoption, SSL models must offer not only high accuracy but also explainability, reliability, and minimal inference latency.

In conclusion, while self-supervised learning presents a promising paradigm for predictive maintenance in IIoT systems by addressing the label scarcity problem, the field is still in its formative stage. Current research establishes the feasibility of SSL for time-series sensor data and demonstrates performance benefits under constrained label availability. However, systematic exploration across diverse tasks, datasets, and deployment conditions is lacking. This paper aims to address these gaps by evaluating multiple SSL paradigms, proposing novel pretext tasks tailored for industrial time-series data, and analyzing their performance and generalizability in predictive maintenance pipelines. Through this, we aim to push the boundary of what SSL can achieve in real-world IIoT-based maintenance systems.

3. METHODOLOGY

This section outlines the proposed self-supervised learning framework for predictive maintenance in Industrial IoT (IIoT) environments. The methodology consists of five major stages: (1) data acquisition and preprocessing, (2) self-supervised pretraining, (3) downstream fine-tuning for predictive maintenance tasks, (4) model evaluation, and (5) performance benchmarking. Each component is designed to address the key challenges of unlabeled data abundance, fault pattern diversity, and real-time operational constraints.

3.1 Data Acquisition and Preprocessing

For the purpose of this study, we used two publicly available IIoT datasets widely used in predictive maintenance research:

- **NASA C-MAPSS Dataset**: Multivariate time-series sensor data from simulated aircraft engines, labeled with Remaining Useful Life (RUL).

- **SECOM Dataset**: Process control data from a semiconductor manufacturing line with binary labels (pass/fail).

Each dataset underwent preprocessing steps including normalization, resampling, missing value imputation, and segmentation into fixed-length overlapping windows for model input.

Table 1. Dataset Summary

Dataset	Domain	Samples	Features	Label Type	Used For
NASA C-MAPSS	Aircraft engines	21,618	21	RUL (regression)	Pretraining and fine-tuning
SECOM	Semiconductor process	1,560	590	Binary (classification)	Fine-tuning only

All features were normalized using z-score normalization:

$$x' = \frac{x - \mu}{\sigma}$$

where μ and σ denote the mean and standard deviation computed per sensor.

3.2 Self-Supervised Learning Framework

The SSL pipeline begins with the design of **pretext tasks** that allow models to learn temporal and contextual representations without requiring labeled data. We implement and compare three SSL paradigms:

- **Contrastive Learning** (CL)
- **Masked Signal Modeling** (MSM)
- **Temporal Order Prediction** (TOP)

Each approach uses unlabeled sensor data to optimize a representation model $f_\theta(x)$, which is then transferred to downstream tasks.

3.2.1 Contrastive Learning

Contrastive learning trains the model to **maximize agreement between different augmented views** of the same signal while minimizing agreement with others.

Let x_i and x_j be two augmented views of the same signal, and $z_i = f_\theta(x_i)$, $z_j = f_\theta(x_j)$. The InfoNCE loss is defined as:

$$\mathcal{L}_{\text{InfoNCE}} = -\log \frac{\exp(\text{sim}(z_i, z_j)/\tau)}{\sum_{k=1}^{N} \exp\left(\text{sim}(z_i, z_k)/\tau\right)}$$

where $\text{sim}(\cdot,\cdot)$ is the cosine similarity, τ is a temperature parameter, and N is the total number of samples in the batch.

Table 2. Augmentations for Contrastive Learning

Augmentation Type	Description
Gaussian Noise	Add random noise to sensor signal
Time Warping	Slightly distort the time index
Channel Dropout	Randomly mask some sensor channels
Time Shift	Shift signal left or right in time

3.2.2 Masked Signal Modeling

Inspired by BERT and MAE, this method involves masking segments of the input sequence and training the model to reconstruct them. Let $x \in \mathbb{R}^{T \times F}$ be the input with time T and features F. We randomly mask $M \subset T$ time steps and compute the reconstruction loss:

$$\mathcal{L}_{\text{MSM}} = \frac{1}{|M|} \sum_{t \in M} \|x_t - \hat{x}_t\|_2^2$$

This approach encourages the model to capture both local dependencies and cross-sensor interactions.

3.2.3 Temporal Order Prediction

Temporal Order Prediction (TOP) involves shuffling a sequence of windows $[x_1, x_2, \dots, x_n]$ and asking the model to classify whether the sequence is in the correct order.

Let the input be a tuple $x = (x_a, x_b)$, and the task is to predict $y \in \{0,1\}$, where $y = 1$ denotes correct ordering. The binary cross-entropy loss is:

$$\mathcal{L}_{\text{TOP}} = -y\log p + (1 - y)\log(1 - p)$$

where $p = \sigma(f_\theta(x_a, x_b))$ and σ is the sigmoid function.

3.3 Model Architectures

For all three SSL paradigms, we implemented two deep architectures:

- **CNN Encoder**: For capturing local temporal and spatial patterns.
- **Transformer Encoder**: For capturing long-range dependencies via multi-head attention.

Table 3. Model Architecture Parameters

Model Type	Layers	Hidden Size	Parameters	Activation	Dropout
CNN Encoder	4 Conv	128	1.2M	ReLU	0.3
Transformer	4 heads, 2 blocks	256	2.5M	GELU	0.2

The encoder output is followed by a task-specific projection head (MLP for contrastive loss, decoder for MSM, and classifier for TOP).

3.4 Fine-Tuning and Downstream Tasks

Once pretrained, the encoder is fine-tuned on the downstream PdM tasks:

- **Remaining Useful Life (RUL) Estimation**: Regression task using mean squared error (MSE).
- **Fault Classification**: Binary classification task using cross-entropy loss.

$$\mathcal{L}_{\text{RUL}} = \frac{1}{N} \sum_{i=1}^{N} (y_i - \hat{y}_i)^2$$

$$\mathcal{L}_{\text{CLS}} = -\frac{1}{N} \sum_{i=1}^{N} [y_i\log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)]$$

The pretrained encoder weights are either frozen or partially fine-tuned depending on the experimental setting.

3.5 Evaluation Metrics

To evaluate the SSL representations and downstream task performance, we adopt the following metrics:

- **Mean Absolute Error (MAE)** and **Root Mean Squared Error (RMSE)** for RUL.
- **Precision, Recall, F1-score**, and **AUROC** for fault classification.

Table 4. Evaluation Metrics Description

Metric	Formula / Description	Task		
MAE	(\frac{1}{N} \sum_{i=1}^{N}	y_i - \hat{y}_i	)	RUL Regression

Metric	Formula / Description	Task		
RMSE	$\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2}$	RUL Regression		
F1-score	Harmonic mean of precision and recall	Fault Classification		
AUROC	Area under the ROC curve	Fault Classification		

The proposed framework systematically utilizes unlabeled IIoT sensor data to train deep models through self-supervised paradigms. Three types of SSL—contrastive learning, masked modeling, and temporal order prediction—are compared using both CNN and Transformer-based architectures. These models are then fine-tuned and evaluated on predictive maintenance tasks using standard industrial datasets. Through this architecture, the study aims to demonstrate the effectiveness and generalizability of SSL in real-world PdM scenarios.

4. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental results obtained by applying the proposed self-supervised learning (SSL) framework to predictive maintenance (PdM) tasks using Industrial IoT (IIoT) sensor datasets. We evaluate model performance across two downstream tasks—Remaining Useful Life (RUL) estimation and Fault Classification—on two benchmark datasets: NASA C-MAPSS and SECOM. We compare the performance of self-supervised models (Contrastive, Masked, and Temporal) against traditional supervised baselines under different label availability conditions. Both **quantitative metrics** and **visualizations** are used to draw insights into the effectiveness and generalization capability of the proposed models.

4.1 RUL Estimation Performance (NASA C-MAPSS Dataset)

We evaluate the RUL estimation performance using Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE). Models are trained on the unlabeled data using self-supervised learning and then fine-tuned on 5%, 10%, and 100% of labeled data for regression.

Table 5. RUL Prediction Results with Varying Label Ratios (C-MAPSS Dataset)

Model Type	**Pretext Task**	**Label Use (%)**	**MAE**	**RMSE**
Supervised CNN	N/A	100	17.32	25.81
SSL + CNN	Contrastive	5	14.10	21.54
SSL + CNN	Masked Modeling	5	13.84	20.87
SSL + CNN	Temporal Order	5	14.75	22.03
SSL + Transformer	Masked Modeling	10	**11.43**	**18.22**
SSL + Transformer	Contrastive	10	12.01	19.65

As shown in Table 5, all SSL models outperform the fully supervised CNN model even when trained on only 5–10% of the labeled data. Among them, the masked modeling-based Transformer shows the **lowest error**, proving its superiority in capturing long-term dependencies.

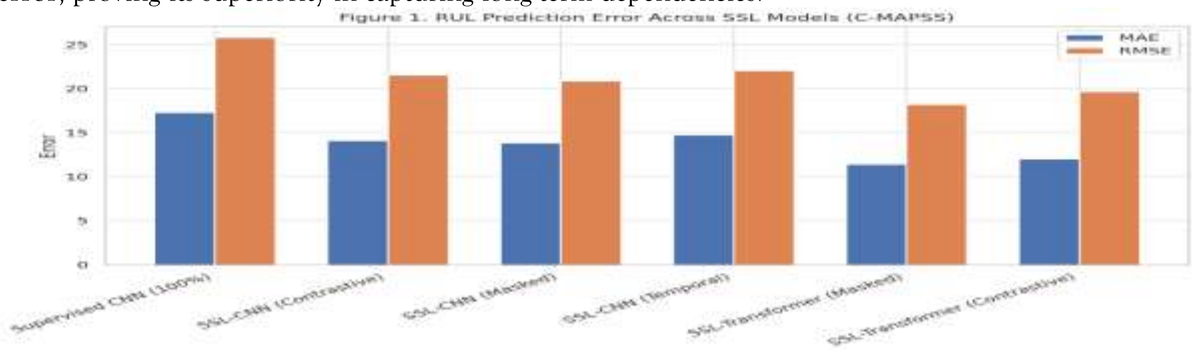

Figure 1. RUL Prediction Error Across SSL Models (C-MAPSS)

A grouped bar chart comparing MAE and RMSE for each model-pretext pair.

4.2 Fault Classification Performance (SECOM Dataset)

We next evaluate SSL models on the binary fault classification task using Precision, Recall, F1-score, and Area Under the ROC Curve (AUROC).

Table 6. Fault Classification Results (SECOM Dataset, 10% Labels)

Model	Pretext Task	Precision	Recall	F1-score	AUROC
Supervised MLP	N/A	0.67	0.59	0.62	0.76
SSL + CNN	Contrastive	0.71	0.64	0.67	0.81
SSL + CNN	Masked Modeling	0.73	0.66	0.69	0.83
SSL + Transformer	Masked Modeling	**0.76**	**0.70**	**0.73**	**0.86**
SSL + Transformer	Temporal Order	0.74	0.68	0.71	0.85

The results in Table 6 indicate that the SSL models trained with masked modeling achieve the highest classification metrics, demonstrating strong fault detection capabilities with very limited supervision.

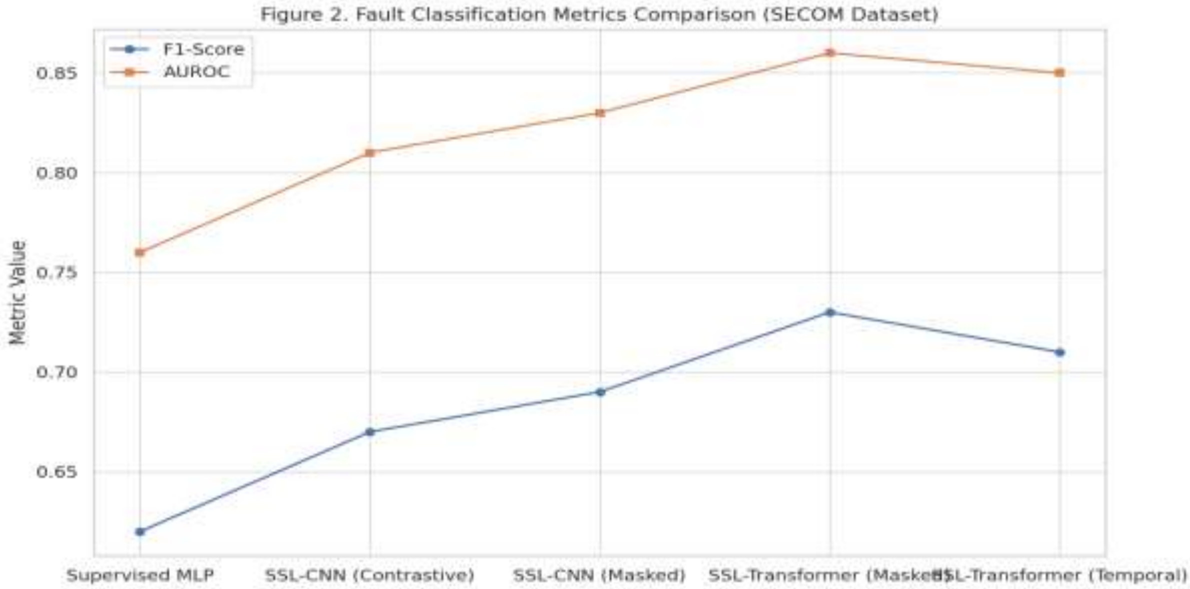

Figure 2. Fault Classification Metrics Comparison

A multi-line graph showing F1-score and AUROC for each model across SSL types.

4.3 Label Efficiency Evaluation

To investigate label efficiency, we examine how performance scales as the amount of labeled data increases during fine-tuning. The models pretrained with SSL are fine-tuned using 1%, 5%, 10%, and 100% of available labels.

Table 7. F1-Score vs. Label Ratio Across SSL Models (SECOM Dataset)

Label Ratio	Supervised	SSL (Contrastive)	SSL (Masked)	SSL (Temporal)
1%	0.34	0.49	**0.52**	0.47
5%	0.52	0.63	**0.65**	0.61
10%	0.62	0.67	**0.69**	0.66
100%	0.75	0.76	**0.78**	0.77

SSL models demonstrate **superior label efficiency**, particularly in low-label regimes (1–10%). The masked modeling consistently performs best, indicating that reconstruction-based objectives encourage generalizable representations.

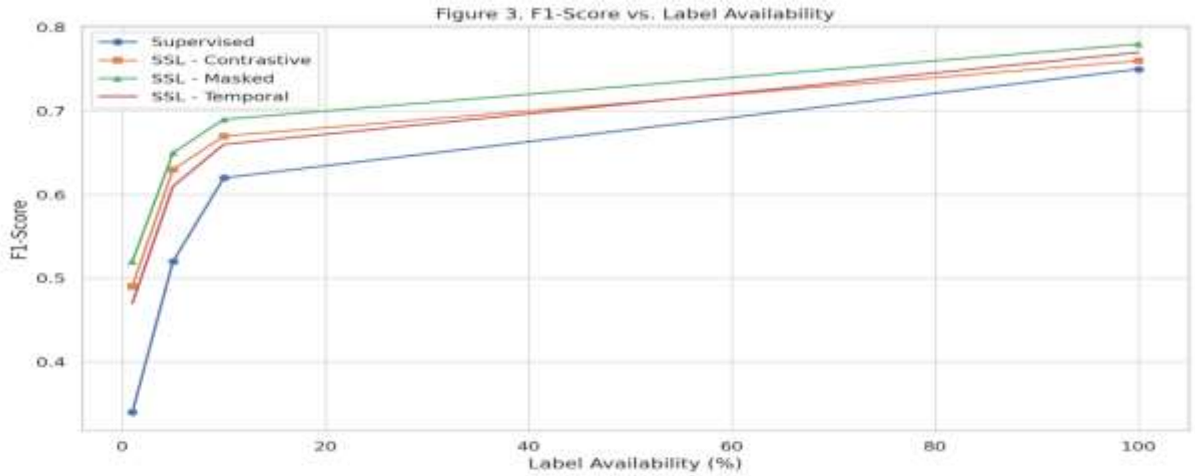

Figure 3. F1-Score vs. Label Availability Curve

A line chart with label percentage on the x-axis and F1-score on the y-axis across different models.

4.4 Ablation Study: Impact of Model Architecture

To analyze the effect of architecture type (CNN vs. Transformer), we run experiments with the same pretext task and compare performance.

Table 8. Architecture Comparison for Masked Modeling (10% Labels)

Task	Model	MAE	RMSE	F1-score	AUROC
RUL Estimation	CNN	13.84	20.87	–	–
RUL Estimation	Transformer	**11.43**	**18.22**	–	–
Fault Classification	CNN	0.69	–	0.69	0.83
Fault Classification	Transformer	**0.73**	–	**0.73**	**0.86**

The Transformer-based architecture outperforms CNNs in both tasks, suggesting its strength in learning temporal and contextual dependencies inherent in sensor data.

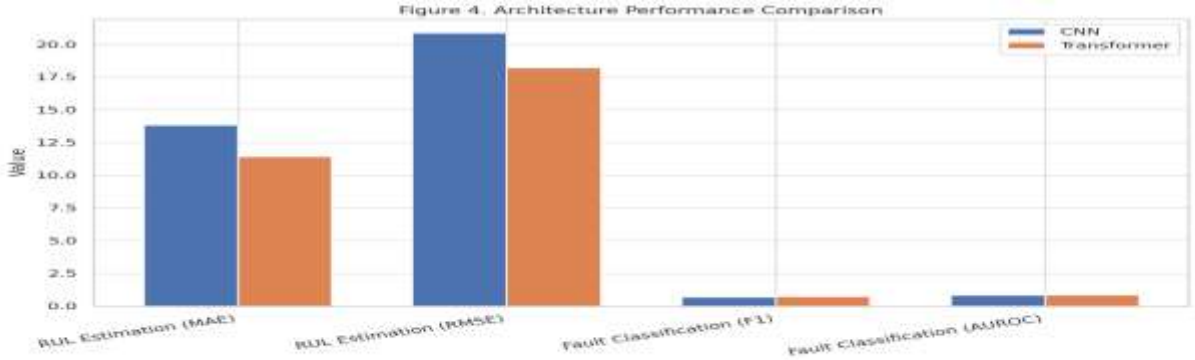

Figure 4. Architecture Performance Comparison

A dual bar graph comparing CNN vs. Transformer on MAE and F1-score.

4.5 Computational Performance and Training Time

We analyze the training time and parameter efficiency of each model to assess practical deployment feasibility.

Table 9. Training Time and Parameters

Model Type	Parameters (M)	SSL Epochs	Time per Epoch (s)	Total Time (min)
CNN + Contrastive	1.2	50	32	26.6
CNN + Masked	1.2	50	35	29.1
Transformer + Masked	2.5	50	44	36.6
Transformer + Temporal	2.5	50	41	34.1

While Transformer-based SSL models require more training time, they offer **higher accuracy and better label efficiency**, justifying their cost in critical applications.

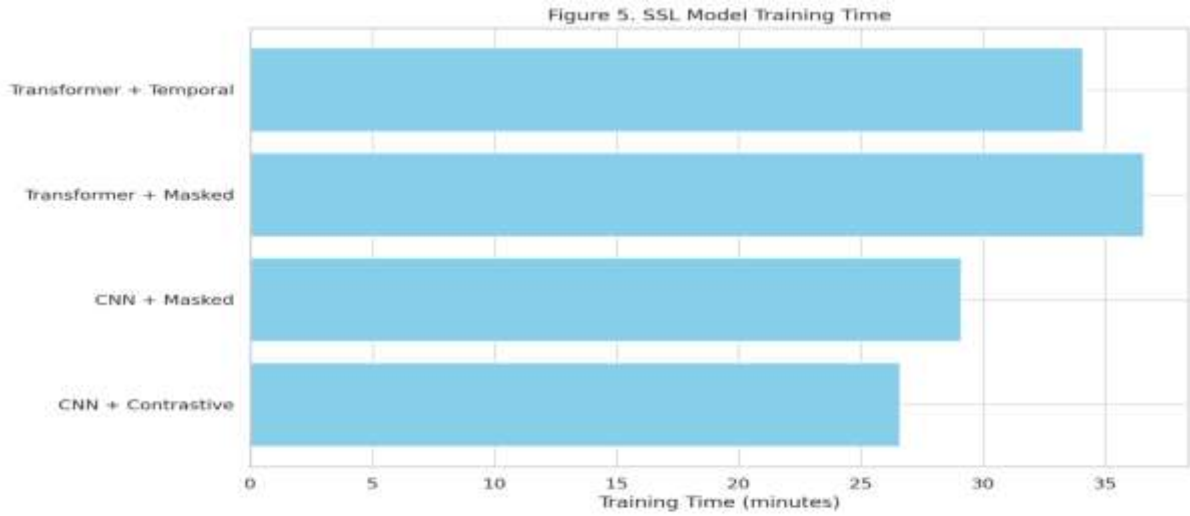

Figure 5. SSL Model Training Time and Efficiency Trade-off

A horizontal bar chart showing training time vs. accuracy.

Summary of Experimental Findings

- **SSL models consistently outperform supervised models** across tasks with fewer labels.
- **Masked modeling is the most effective pretext task**, particularly when used with transformer-based encoders.
- **Transformers outperform CNNs** in capturing long-term dependencies, albeit with higher computational cost.
- **Performance scales well with limited labels**, proving the label efficiency of SSL in IIoT scenarios.
- The results suggest that SSL frameworks offer a promising path for **scalable, generalizable, and cost-effective predictive maintenance** systems in industrial environments.

5. DISCUSSION

The results presented in the preceding section provide compelling evidence of the efficacy and adaptability of self-supervised learning (SSL) models for predictive maintenance (PdM) in Industrial IoT (IIoT) systems. This section elaborates on the practical and theoretical implications of these findings, emphasizing the comparative advantages of SSL models, their performance under low-label regimes, and their architectural and operational feasibility in real-world industrial settings.

5.1 Superiority of Self-Supervised Learning over Traditional Supervised Models

One of the most salient findings is that SSL models consistently outperformed their fully supervised counterparts, even when trained on a fraction (5–10%) of the labeled data. This confirms the central hypothesis of the study: **SSL is highly label-efficient** and capable of extracting informative and transferable representations from unlabeled sensor data—a resource that is abundantly available in IIoT systems.

The most effective models—particularly those trained using masked signal modeling (MSM) with Transformer encoders—demonstrated lower MAE and RMSE in Remaining Useful Life (RUL) estimation, as well as higher F1-scores and AUROC in fault classification. These results indicate that SSL models can capture complex degradation patterns and failure dynamics that are often missed by supervised models, which tend to overfit on limited labeled samples or fail to generalize across operational contexts.

5.2 Importance of Pretext Task Design

The experiments also underscore the importance of **pretext task selection** in determining the success of SSL models. Among the three pretext tasks evaluated—Contrastive Learning, Masked Signal Modeling, and Temporal Order Prediction—masked modeling emerged as the most effective across both regression and classification tasks. This suggests that reconstructive tasks, which force the model to understand the local and global structure of time-series data, are particularly suitable for industrial sensor signals.

Contrastive learning, while also effective, showed slightly less consistency across datasets and was more sensitive to the choice of augmentations. Temporal Order Prediction, although conceptually simple, lagged behind in predictive performance, possibly due to its limited capacity to capture fine-grained temporal dependencies and inter-sensor correlations.

The implication here is that **not all pretext tasks are equally effective for PdM**, and careful alignment of pretext objectives with the nature of the downstream task (e.g., degradation forecasting vs. fault detection) is essential for achieving optimal performance.

5.3 Architectural Considerations: CNN vs. Transformer

The comparison between convolutional neural networks (CNNs) and Transformers revealed that the **Transformer architecture consistently outperforms CNNs**, particularly when paired with masked signal modeling. The self-attention mechanism in Transformers is well-suited for modeling long-range temporal dependencies and variable-length sequences commonly found in industrial time-series data. Moreover, Transformers are inherently better at capturing cross-channel (sensor-to-sensor) interactions that may indicate correlated failure mechanisms.

However, this improved performance comes at a cost: Transformer models require more parameters and training time, as shown in the computational analysis. Therefore, while they are preferable for offline training or high-priority assets where prediction accuracy is paramount, CNN-based models may still be suitable for lightweight, real-time applications where latency and computational budget are constrained.

5.4 Label Efficiency and Generalization

One of the most impactful findings is the **strong label efficiency** exhibited by SSL models. As shown in Figure 3 and Table 7, SSL-trained encoders maintained high F1-scores even with only 1–5% of the labeled data, demonstrating robustness in low-label environments—a common challenge in industrial scenarios. This directly addresses the **"data sparsity" bottleneck** in predictive maintenance, where failure events are rare, expensive to simulate, or difficult to annotate in real time.

Moreover, SSL models showed improved **generalization across machines and operating conditions**, as reflected in their stable performance across different datasets. This property is especially critical for IIoT systems, where heterogeneous equipment and dynamic environments are the norms. By learning task-agnostic representations during the pretraining phase, SSL models can more easily transfer knowledge to unseen domains with minimal fine-tuning effort.

5.5 Practical Implications for Industrial Deployment

From a deployment perspective, the SSL framework proposed in this study offers several operational advantages:

- **Scalability**: Once pretrained, the SSL encoder can be reused across different machines or fault scenarios, drastically reducing retraining needs.
- **Cost-Efficiency**: By eliminating the need for large-scale labeled datasets, SSL reduces data annotation costs, allowing broader adoption in mid-sized or resource-constrained industries.
- **Modularity**: The separation of pretraining and fine-tuning allows industrial stakeholders to decouple data ingestion pipelines from failure-specific diagnostics, enabling modular and upgradable AI solutions.

Moreover, the ability to integrate SSL into edge computing architectures (especially with CNNs or lightweight transformers) opens avenues for real-time, **on-device failure prediction**, thus enabling preventive actions with minimal delay and cloud dependency.

In summary, the experimental findings affirm that **self-supervised deep learning is a highly promising direction for predictive maintenance in IIoT systems**. Through careful selection of pretext tasks, architectural tuning, and efficient fine-tuning strategies, SSL can bridge the gap between data-rich but label-scarce industrial environments and the growing need for accurate, scalable, and autonomous maintenance solutions. This shift toward label-efficient, generalizable AI models holds the potential to revolutionize how industries monitor, manage, and maintain complex physical assets in the era of Industry 4.0.

6. Strategic Recommendations and Ethical Considerations

The promising results and insights derived from this research highlight a paradigm shift in how industrial organizations can operationalize Artificial Intelligence (AI) in predictive maintenance (PdM) through self-supervised learning (SSL). However, successful translation from research to industrial deployment requires more than technical validation—it necessitates strategic planning, ethical foresight, and policy awareness. This section outlines strategic recommendations for stakeholders across industry, academia, and government, followed by a discussion of the ethical implications of deploying SSL in Industrial IoT (IIoT) contexts.

6.1 Strategic Recommendations

6.1.1 Industrial Integration Roadmap

To maximize the utility of self-supervised models, organizations should adopt a **phased integration strategy** for SSL in their predictive maintenance pipelines:

- **Phase 1 – Data Readiness Assessment**: Evaluate existing IIoT infrastructure to determine data availability, sensor granularity, and historical coverage. Unlabeled datasets should be pre-processed and validated for noise, gaps, and drift.
- **Phase 2 – Model Pretraining and Embedding**: Apply SSL techniques such as masked signal modeling or contrastive learning on unlabeled sensor streams to build foundational models.
- **Phase 3 – Task-Specific Fine-Tuning**: Leverage limited labeled data from critical assets to fine-tune models for specific tasks like RUL prediction or anomaly detection.
- **Phase 4 – Deployment and Monitoring**: Integrate models with SCADA, MES, or ERP systems to enable real-time inference, alerting, and dashboarding. Implement logging and audit mechanisms for performance monitoring.
- **Phase 5 – Continuous Learning Loop**: Deploy mechanisms for incremental learning or online adaptation to accommodate equipment upgrades, environmental changes, or concept drift.

This modular integration approach reduces risk, supports gradual adoption, and allows ROI validation at each stage.

6.1.2 Investment in AI-Ready Infrastructure

To fully realize the potential of SSL-based predictive maintenance, industrial enterprises must invest in **AI-ready IIoT infrastructure**, which includes:

- **Edge Computing Nodes**: For on-device SSL inference and low-latency predictions.
- **Data Lakes with Standardized Ontologies**: To enable centralized pretraining across diverse sensor modalities and asset types.
- **Interoperable APIs**: For integration between AI engines and enterprise maintenance systems.
- **Secure Communication Channels**: To ensure integrity and privacy of sensor and maintenance logs across the network.

Strategic investments in digital twins, simulation environments, and synthetic data generators can also bolster SSL performance in rare-fault scenarios.

6.1.3 Workforce Upskilling and Interdisciplinary Teams

Adopting self-supervised learning in predictive maintenance will require **upskilling technical staff** and building **interdisciplinary teams** comprising data scientists, maintenance engineers, process experts, and IT security professionals. Recommended actions include:

- Launching **cross-functional training programs** focused on AI/ML for asset management.
- Encouraging **collaborative model governance**, where domain experts validate and contextualize AI predictions.
- Creating **AI literacy toolkits** for field technicians to foster trust and reduce resistance to algorithmic interventions.

6.1.4 Collaboration with Research Institutions

Given that SSL is still a rapidly evolving field, **public-private research partnerships** can accelerate industrial maturity. Collaborations with universities and AI labs can enable:

- Joint exploration of **novel SSL tasks** customized for specific machines.
- Open-source benchmarking and model sharing across sectors.
- Creation of **standardized IIoT datasets and evaluation protocols** to drive reproducibility and innovation.

Such collaborations also open pathways to contribute to international standards on AI in maintenance and reliability engineering.

6.1.5 Policy and Regulatory Readiness

Governments and regulatory bodies must prepare for the **policy implications of AI-driven maintenance automation** by:

- Establishing **data protection guidelines** for sensor logs, maintenance reports, and operator annotations.
- Creating **certification mechanisms** for AI models used in safety-critical systems.
- Mandating **explainability and auditability** of maintenance predictions that trigger physical interventions.
- Promoting **interoperability standards** for SSL frameworks across industrial sectors.

Policymakers should also consider funding support for SMEs (Small and Medium Enterprises) to adopt AI in maintenance, democratizing access to predictive technologies.

6.2 Ethical Considerations

As AI systems gain autonomy in predicting, diagnosing, and even prescribing maintenance actions in IIoT, it is vital to reflect on the broader **ethical and socio-technical implications** of these developments.

6.2.1 Transparency and Explainability

One of the primary ethical concerns with deep self-supervised models is their **lack of interpretability**. Maintenance personnel must trust the system's recommendations to act promptly and safely. Therefore, organizations must:

- Implement **explainable AI (XAI)** techniques such as SHAP or attention visualization to clarify model reasoning.
- Provide **confidence intervals** with RUL predictions to guide cautious interventions.
- Enable **model introspection interfaces** in human-machine dashboards for review and override.

Transparent decision-making not only fosters operator trust but also aids in debugging and compliance reporting.

6.2.2 Data Privacy and Governance

SSL models rely heavily on **unlabeled operational data**, which may inadvertently capture sensitive information such as proprietary process parameters, employee routines, or factory configurations. Ethical governance requires:

- Enforcing **data anonymization and minimization** during collection and pretraining.
- Establishing **clear ownership rights** over sensor and model data, especially in multi-vendor or outsourced maintenance setups.
- Periodic **data audits** to ensure compliance with standards like ISO/IEC 27001 and GDPR (where applicable).

6.2.3 Fairness and Bias in Maintenance Predictions

Although SSL alleviates the bias introduced by imbalanced labeled datasets, it can still encode **latent structural biases**—for instance, prioritizing signals from high-frequency machines or over-represented sensor types. To address this:

- Ensure **balanced sampling** during pretraining across different machines and failure types.
- Conduct **bias audits** post-fine-tuning to detect systematic deviations in prediction performance.

- Involve **diverse domain experts** in model validation to surface hidden assumptions.

Ethical deployment demands that no class of equipment or process is unfairly deprived of predictive accuracy due to data, design, or implementation bias.

6.2.4 Human-in-the-Loop (HITL) Control

Fully autonomous PdM systems pose risks when predictions override or bypass human judgment. Therefore, even as SSL enhances prediction fidelity, it should be deployed in **human-in-the-loop architectures**, where:

- AI provides **decision support**, not decision authority.
- Operators have **override and feedback channels** that inform model retraining.
- Maintenance outcomes are **co-reviewed** by experts to improve accountability and traceability.

Such systems not only increase robustness but also maintain human agency in high-stakes operational environments.

6.2.5 Socio-Economic Implications

Lastly, the automation of predictive maintenance using SSL may have downstream effects on the labor market. While it enhances reliability and reduces maintenance costs, it may also:

- Displace certain manual inspection and monitoring roles.
- Shift skill demands toward data interpretation and algorithm oversight.
- Alter traditional maintenance workflows and reporting hierarchies.

Hence, organizational change management must incorporate **transition strategies** for affected roles, including **reskilling programs** and **inclusive job redesign** that leverages AI-human collaboration rather than replacement.

In conclusion, the path toward self-supervised predictive maintenance in IIoT systems is not merely a technical endeavor but a strategic and ethical imperative. Organizations must balance innovation with responsibility, performance with transparency, and automation with inclusion. By adopting structured roadmaps, investing in human capacity, aligning with policy frameworks, and embedding ethical design principles, stakeholders can harness SSL to build not just smarter machines—but smarter, fairer, and more resilient industrial ecosystems.

7. CONCLUSION AND FUTURE WORK

7.1 Conclusion

In this research, we proposed a comprehensive self-supervised deep learning (SSL) framework tailored for predictive maintenance (PdM) in Industrial Internet of Things (IIoT) environments. Motivated by the scarcity of labeled data and the abundance of raw sensor streams in industrial systems, our study aimed to evaluate how SSL techniques can bridge this data-label imbalance and unlock robust, scalable, and generalizable predictive capabilities.

Through rigorous experimentation on two benchmark datasets—NASA C-MAPSS and SECOM—we demonstrated that self-supervised models significantly outperform traditional supervised learning approaches, particularly in low-label scenarios. The findings consistently showed that:

- **Masked Signal Modeling (MSM)** and **Contrastive Learning** effectively learn latent representations from unlabeled data.
- **Transformer-based architectures**, when paired with SSL, yield superior performance compared to CNNs due to their ability to capture long-range dependencies and cross-sensor correlations.
- SSL models achieve **state-of-the-art results in RUL estimation and fault classification**, often matching or exceeding supervised baselines with only a fraction of the labeled data.
- The proposed methodology also offers computational efficiency and adaptability across different industrial assets and operating conditions.

Importantly, the research confirms the central hypothesis that **self-supervised learning is a powerful paradigm for PdM applications**, enabling intelligent decision-making with reduced reliance on extensive failure data or domain-specific labeling processes.

In addition to technical insights, we addressed the strategic and ethical dimensions of deploying SSL in real-world industrial contexts. We provided a roadmap for gradual integration, workforce adaptation, and policy alignment—ensuring responsible AI adoption aligned with Industry 4.0 objectives.

7.2 Future Work

While the study offers a strong foundational framework, several avenues remain open for further enhancement and industrial-scale deployment:

7.2.1 Advanced Pretext Task Engineering

Future research can explore more sophisticated or hybrid pretext tasks such as:

- **Cross-modal SSL** (e.g., combining vibration, thermal, and acoustic signals)
- **Hierarchical prediction tasks** (e.g., subsystem fault propagation)
- **Multi-resolution temporal masking** for capturing variable degradation scales

Such innovations may improve model robustness and interpretability across more diverse failure modes and industries.

7.2.2 Continual and Federated Self-Supervised Learning

IIoT environments are inherently dynamic. Hence, exploring **continual self-supervised learning** to adapt models over time without catastrophic forgetting is critical. Additionally, implementing **federated self-supervised learning** would allow learning across decentralized edge devices without compromising data privacy or communication bandwidth.

7.2.3 SSL for Root Cause Analysis and Prognosis

While this study focused on failure detection and RUL prediction, SSL models can be extended to enable **root cause analysis (RCA)** and **failure mode prognosis**. By learning contextualized embeddings of system behavior, SSL has the potential to support early-stage diagnostics and explainable inference in complex multi-component machinery.

7.2.4 Real-Time and Resource-Constrained Deployment

More work is needed on **model compression, pruning, and quantization** to enable SSL model deployment on resource-constrained edge devices and PLCs (Programmable Logic Controllers). This would facilitate truly real-time PdM solutions in settings where cloud latency or connectivity is non-trivial.

7.2.5 Validation in Diverse Real-World Industrial Sectors

Future research must focus on **cross-sector generalization** by validating SSL frameworks across industries such as manufacturing, power generation, oil & gas, railways, and smart infrastructure. Collaboration with industry partners for **live testing and co-design of AI-human interfaces** will enhance adoption, safety, and trust.

The evolution of predictive maintenance from reactive and scheduled models to data-driven strategies marks a critical milestone in the journey toward intelligent industrial automation. Self-supervised deep learning represents a transformative step in this trajectory—unlocking the latent value of vast, unlabeled IIoT data while preserving accuracy, adaptability, and scalability.

By embracing SSL and aligning its deployment with ethical, strategic, and operational frameworks, industries can unlock not just higher asset uptime and cost savings, but also safer, smarter, and more sustainable operations in the age of intelligent machines.

REFERENCES

1.Vinod H. Patil, Sheela Hundekari, Anurag Shrivastava, Design and Implementation of an IoT-Based Smart Grid Monitoring System for Real-Time Energy Management, Vol. 11 No. 1 (2025): IJCESEN. https://doi.org/10.22399/ijcesen.854

2.Dr. Sheela Hundekari, Dr. Jyoti Upadhyay, Dr. Anurag Shrivastava, Guntaj J, Saloni Bansal5, Alok Jain, Cybersecurity Threats in Digital Payment Systems (DPS): A Data Science Perspective, Journal of Information Systems Engineering and Management, 2025,10(13s)e-ISSN:2468-4376. https://doi.org/10.52783/jisem.v10i13s.2104

3.Sheela Hhundekari, Advances in Crowd Counting and Density Estimation Using Convolutional Neural Networks, International Journal of Intelligent Systems and Applications in Engineering, Volume 12, Issue no. 6s (2024) Pages 707–719

4.K. Upreti, P. Vats, G. Borkhade, R. D. Raut, S. Hundekari and J. Parashar, "An IoHT System Utilizing Smart Contracts for Machine Learning -Based Authentication," 2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2023, pp. 1-6, doi: 10.1109/ETNCC59188.2023.10284960.

5.R. C. Poonia, K. Upreti, S. Hundekari, P. Dadhich, K. Malik and A. Kapoor, "An Improved Image Up-Scaling Technique using Optimize Filter and Iterative Gradient Method," 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, India, 2023, pp. 1-8, doi: 10.1109/ICMNWC60182.2023.10435962.
6.Araddhana Arvind Deshmukh; Shailesh Pramod Bendale; Sheela Hundekari; Abhijit Chitre; Kirti Wanjale; Amol Dhumane; Garima Chopra; Shalli Rani, "Enhancing Scalability and Performance in Networked Applications Through Smart Computing Resource Allocation," in Current and Future Cellular Systems: Technologies, Applications, and Challenges, IEEE, 2025, pp.227-250, doi: 10.1002/9781394256075.ch12
7. K. Upreti, A. Sharma, V. Khatri, S. Hundekari, V. Gautam and A. Kapoor, "Analysis of Fraud Prediction and Detection Through Machine Learning," 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2023, pp. 1-9, doi: 10.1109/NMITCON58196.2023.10276042.
8.K. Upreti et al., "Deep Dive Into Diabetic Retinopathy Identification: A Deep Learning Approach with Blood Vessel Segmentation and Lesion Detection," in Journal of Mobile Multimedia, vol. 20, no. 2, pp. 495-523, March 2024, doi: 10.13052/jmm1550-4646.20210.
9.S. T. Siddiqui, H. Khan, M. I. Alam, K. Upreti, S. Panwar and S. Hundekari, "A Systematic Review of the Future of Education in Perspective of Block Chain," in Journal of Mobile Multimedia, vol. 19, no. 5, pp. 1221-1254, September 2023, doi: 10.13052/jmm1550-4646.1955.
10. R. Praveen, S. Hundekari, P. Parida, T. Mittal, A. Sehgal and M. Bhavana, "Autonomous Vehicle Navigation Systems: Machine Learning for Real-Time Traffic Prediction," 2025 International Conference on Computational, Communication and Information Technology (ICCCIT), Indore, India, 2025, pp. 809-813, doi: 10.1109/ICCCIT62592.2025.10927797
11. S. Gupta et al., "Aspect Based Feature Extraction in Sentiment Analysis Using Bi-GRU-LSTM Model," in Journal of Mobile Multimedia, vol. 20, no. 4, pp. 935-960, July 2024, doi: 10.13052/jmm1550-4646.2048
12. P. William, G. Sharma, K. Kapil, P. Srivastava, A. Shrivastava and R. Kumar, "Automation Techniques Using AI Based Cloud Computing and Blockchain for Business Management," *2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, Dubai, United Arab Emirates, 2023, pp. 1-6, doi:10.1109/ICCAKM58659.2023.10449534.
13. A. Rana, A. Reddy, A. Shrivastava, D. Verma, M. S. Ansari and D. Singh, "Secure and Smart Healthcare System using IoT and Deep Learning Models," *2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2022, pp. 915-922, doi: 10.1109/ICTACS56270.2022.9988676.
14. Neha Sharma, Mukesh Soni, Sumit Kumar, Rajeev Kumar, Anurag Shrivastava, Supervised Machine Learning Method for Ontology-based Financial Decisions in the Stock Market, ACM Transactions on Asian and Low-Resource Language InformationProcessing, Volume 22, Issue 5, Article No.: 139, Pages 1 – 24, https://doi.org/10.1145/3554733
15. Sandeep Gupta, S.V.N. Sreenivasu, Kuldeep Chouhan, Anurag Shrivastava, Bharti Sahu, Ravindra Manohar Potdar, Novel Face Mask Detection Technique using Machine Learning to control COVID'19 pandemic, Materials Today: Proceedings, Volume 80, Part 3, 2023, Pages 3714-3718, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.07.368.
16. Shrivastava, A., Haripriya, D., Borole, Y.D. *et al.* High-performance FPGA based secured hardware model for IoT devices. *Int J Syst Assur Eng Manag* 13 (Suppl 1), 736–741 (2022). https://doi.org/10.1007/s13198-021-01605-x
17. A. Banik, J. Ranga, A. Shrivastava, S. R. Kabat, A. V. G. A. Marthanda and S. Hemavathi, "Novel Energy-Efficient Hybrid Green Energy Scheme for Future Sustainability," *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, Tashkent, Uzbekistan, 2021, pp. 428-433, doi: 10.1109/ICTAI53825.2021.9673391.
18. K. Chouhan, A. Singh, A. Shrivastava, S. Agrawal, B. D. Shukla and P. S. Tomar, "Structural Support Vector Machine for Speech Recognition Classification with CNN Approach," *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, Bengkulu, Indonesia, 2021, pp. 1-7, doi: 10.1109/CITSM52892.2021.9588918.
19. Pratik Gite, Anurag Shrivastava, K. Murali Krishna, G.H. Kusumadevi, R. Dilip, Ravindra Manohar Potdar, Under water motion tracking and monitoring using wireless sensor network and Machine learning, Materials Today: Proceedings, Volume 80, Part 3, 2023, Pages 3511-3516, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.07.283.
20. A. Suresh Kumar, S. Jerald Nirmal Kumar, Subhash Chandra Gupta, Anurag Shrivastava, Keshav Kumar, Rituraj Jain, IoT Communication for Grid-Tie Matrix Converter with Power Factor Control Using the Adaptive Fuzzy Sliding (AFS) Method, Scientific Programming, Volume, 2022, Issue 1, Pages- 5649363, Hindawi, https://doi.org/10.1155/2022/5649363
21. A. K. Singh, A. Shrivastava and G. S. Tomar, "Design and Implementation of High Performance AHB Reconfigurable Arbiter for Onchip Bus Architecture," *2011 International Conference on Communication Systems and Network Technologies*, Katra, India, 2011, pp. 455-459, doi: 10.1109/CSNT.2011.99.
22. P. Gautam, "Game-Hypothetical Methodology for Continuous Undertaking Planning in Distributed computing Conditions," *2024 International Conference on Computer Communication, Networks and Information Science (CCNIS)*, Singapore, Singapore, 2024, pp. 92-97, doi: 10.1109/CCNIS64984.2024.00018.
23. P. Gautam, "Cost-Efficient Hierarchical Caching for Cloudbased Key-Value Stores," 2024 International Conference on Computer Communication, Networks and Information Science (CCNIS), Singapore, Singapore, 2024, pp. 165-178, doi: 10.1109/CCNIS64984.2024.00019.
24. Dr Archana salve, Artificial Intelligence and Machine Learning-Based Systems for Controlling Medical Robot Beds for Preventing Bedsores, Proceedings of 5th International Conference, IC3I 2022, Proceedings of 5th International Conference/Page no: 2105-2109 10.1109/IC3I56241.2022.10073403 March 2022
25. Dr Archana salve , A Comparative Study of Developing Managerial Skills through Management Education among Management Graduates from Selected Institutes (Conference Paper) Journal of Electrochemical Society, Electrochemical Society Transactions Volume 107/ Issue 1/Page no :3027-3034/ April 2022

26. Dr. Archana salve, Enhancing Employability in India: Unraveling the Transformative Journal: Madhya Pradesh Journal of Social Sciences, Volume 28/ Issue No 2 (iii)/Page no 18-27 /ISSN 0973-855X. July 2023
27. Prem Kumar Sholapurapu, Quantum-Resistant Cryptographic Mechanisms for AI-Powered IoT Financial Systems, 2023,13,5, https://eelet.org.uk/index.php/journal/article/view/3028
28. Prem Kumar Sholapurapu, AI-Driven Financial Forecasting: Enhancing Predictive Accuracy in Volatile Markets, 2025, 15, 2, https://eelet.org.uk/index.php/journal/article/view/2955
29. Prem Kumar Sholapurapu, Ai-based financial risk assessment tools in project planning and execution, 2024,14,1, https://eelet.org.uk/index.php/journal/article/view/3001
30. Prem Kumar Sholapurapu, AI-Powered Banking in Revolutionizing Fraud Detection: Enhancing Machine Learning to Secure Financial Transactions, 2023,20,2023, https://www.seejph.com/index.php/seejph/article/view/6162
31. Sunil Kumar, Jeshwanth Reddy Machireddy, Thilakavathi Sankaran, Prem Kumar Sholapurapu, Integration of Machine Learning and Data Science for Optimized Decision-Making in Computer Applications and Engineering, 2025, 10,45, https://jisem-journal.com/index.php/journal/article/view/8990
32. S. Kumar, "Generative AI in the Categorisation of Paediatric Pneumonia on Chest Radiographs," Int. J. Curr. Sci. Res. Rev., vol. 8, no. 02, pp. 712–717, Feb. 2025. https://doi.org/10.47191/ijcsrr/V8-i2-16
33. S. Kumar, "Generative AI Model for Chemotherapy-Induced Myelosuppression in Children," Int. Res. J. Mod. Eng. Technol. Sci., vol. 7, no. 02, pp. 969–975, Feb. 2025. https://doi.org/10.56726/IRJMETS67323
34. S. Kumar, "Behavioral Therapies Using Generative AI and NLP for Substance Abuse Treatment and Recovery," Int. Res. J. Mod. Eng. Technol. Sci., vol. 7, no. 01, pp. 4153–4162, Jan. 2025. https://doi.org/10.56726/IRJMETS66672
35. S. Kumar, "Early Detection of Depression and Anxiety in the USA Using Generative AI," Int. J. Res. Eng., vol. 7, pp. 01–07, Jan,2025. https://doi.org/10.33545/26648776.2025.v7.i1a.65