Analysis of Time Series Data Using LSTM based Autoencoder based model for predicting Equipment Faults

*

1st Kathit Bhongale
School of Computer Science and Engineering (SCOPE)
Vellore Institute Of Technology)
Chennai, India
kathit.bhongale2021@vitstudent.ac.in

2nd Adit Deshpande
School of Computer Science and Engineering (SCOPE)
Vellore Institute Of Technology
Chen
adit.deshpande2021@vitstudent.ac.in

3rd Pranav Murali Rao
School of Computer Science and Engineering (SCOPE)
Vellore Institute of Technology
Chennai, India
pranavmuralirao2021@vitstudent.ac.in

***Abstract*—Predicting equipment faults in industrial settings is crucial for minimizing downtime, reducing maintenance costs, and enhancing operational safety. Traditional fault detection models often fall short in capturing complex, non-linear patterns in time series data, limiting their effectiveness for predictive maintenance applications. In this study, we propose a novel hybrid model that combines Long Short-Term Memory (LSTM) networks and Generative Adversarial Networks (GANs) within an autoencoder framework to improve fault prediction accuracy. The LSTM component is designed to learn temporal dependencies within time series data, while the GAN module enhances the model's robustness by generating realistic synthetic data for improved anomaly detection. Our approach was tested on real-world equipment datasets, demonstrating its ability to detect subtle, early-stage fault patterns that traditional methods overlook. Experimental results reveal that the LSTM-GAN Autoencoder outperforms conventional models in both accuracy and sensitivity, making it a promising tool for predictive maintenance. This model provides a scalable and reliable solution for fault prediction, contributing to the advancement of intelligent industrial monitoring systems.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

In industrial environments, predictive maintenance is essential for improving equipment reliability and minimizing unplanned downtimes. Equipment faults often lead to costly repairs, productivity losses, and safety concerns. As a result, the need for accurate and timely fault prediction has driven significant interest in advanced analytics applied to time series data generated from machinery. Traditional fault prediction models, while effective to some extent, often struggle to capture complex temporal dependencies inherent in sensor data and may suffer from limitations in handling non-linear, high-dimensional data patterns.

Recent advancements in deep learning have enabled more sophisticated approaches for analyzing time series data. Among these, Long Short-Term Memory (LSTM) networks are well-suited for learning temporal dependencies, while Generative Adversarial Networks (GANs) excel in generating realistic synthetic data, enhancing model robustness. This study proposes a novel LSTM-GAN Autoencoder-based model to leverage both methods' strengths, aiming to accurately predict equipment faults by analyzing time series data patterns. This approach is designed to capture subtle data anomalies that often precede mechanical failures, improving fault detection precision.

This paper provides an in-depth analysis of the LSTM-GAN Autoencoder framework applied to real-world equipment data. We evaluate its performance in detecting anomalies and predicting potential failures, comparing its effectiveness against conventional methods. The results demonstrate that this approach not only improves predictive accuracy but also offers a scalable solution for handling large volumes of time series data, positioning it as a viable tool for next-generation predictive maintenance systems.

II. Literaturre Review

The research paper, authored by Philip Tchatchoua, Guillaume Graton, Mustapha Ouladsine, and Michel Juge, presents a comparative evaluation of deep learning algorithms for anomaly detection in multivariate time series data from semiconductor manufacturing. The study explores six models: FDC-CNN, Attention FDC-CNN (supervised methods), and

Identify applicable funding agency here. If none, delete this.

LSTM-AD, EncDec-AD, CSAE-AD, and CDSAE-AD (self-supervised methods). The primary objective is to detect equipment faults in real-time sensor data, which is critical for reducing maintenance costs and improving productivity. Using a simulated semiconductor dataset comprising 5000 normal samples and 2000 faulty samples, the models were evaluated on five different fault types. Among the algorithms, the Attention FDC-CNN achieved the highest overall performance with an F1-score of 95.5%, followed closely by FDC-CNN at 95.1%. The CNN-based models demonstrated the shortest training times, making them ideal for real-time applications. In contrast, self-supervised models like CSAE-AD performed well in scenarios with limited labeled data, achieving an F1-score of 89.7%. However, LSTM-based methods showed the lowest performance with F1-scores below 85% and significantly longer training times. The paper concludes that while supervised methods yield better accuracy, self-supervised models are practical when labeled data is scarce. Future research should focus on real-world data testing and improving model generalizability [1].The paper titled "A Comparative Evaluation of Deep Learning Anomaly Detection Techniques on Semiconductor Multivariate Time Series Data", authored by Michel Juge, investigates the effectiveness of various deep learning algorithms in detecting anomalies within semiconductor manufacturing processes. The study emphasizes the importance of early fault detection to reduce equipment downtime and improve productivity by analyzing large multivariate time series data generated from industrial sensors. Six deep learning methods are evaluated: two supervised models—FDC-CNN and Attention FDC-CNN—and four self-supervised models—LSTM-AD, EncDec-AD, CSAE-AD, and CDSAE-AD. The dataset, comprising 5000 normal samples and 2000 faulty samples, simulates real semiconductor processes, with the models tested on five distinct types of faults. Results reveal that CNN-based models, particularly the Attention FDC-CNN, performed best, achieving an overall F1-score of 95.5%, followed closely by the FDC-CNN at 95.1%. These models also had the shortest training times, making them ideal for real-time industrial applications. In contrast, self-supervised models like CSAE-AD showed competitive performance with an F1-score of 89.7% and proved useful when labeled data was scarce. However, LSTM-based models, while able to capture temporal dependencies, underperformed with F1-scores below 85% and considerably longer training times. The study concludes that while supervised methods are superior in detection accuracy, self-supervised methods are more practical in scenarios where labeled data is limited. Future research directions include testing these models on real semiconductor data, improving generalizability, and exploring hybrid methods that combine the strengths of CNNs and LSTMs for enhanced performance [2]. The research paper presents a novel approach for anomaly detection in time-series data using Generative Adversarial Networks (GANs). The authors, Rohit Raturi and colleagues, highlight the challenges traditional machine learning models face in identifying anomalies due to high dimensionality and temporal correlations. Their proposed GAN model generates synthetic data that mimics normal traffic patterns, which is then used to enhance the detection of anomalies in real data.The study utilizes the Yahoo! Webscope S5 dataset, achieving impressive performance metrics: an F1 score of 0.909, precision of 0.882, recall of 0.938, and an AUC-ROC of 0.966. These results indicate that the GAN-based approach significantly outperforms baseline methods in detecting anomalies, demonstrating its effectiveness in capturing complex data patterns. The paper also discusses the methodology, including the training process of the generator and discriminator networks within the GAN framework. The findings suggest that GANs are not only capable of generating synthetic data for training but also excel in distinguishing between normal and anomalous instances in time-series datasets. This research contributes to advancing anomaly detection techniques by leveraging the strengths of GANs, offering a promising direction for future studies in various fields such as finance and cybersecurity[3].The research paper introduces a novel approach for detecting anomalies in multivariate time-series data using an unsupervised deep learning framework called the Multilayer Convolutional Recurrent Autoencoded Anomaly Detector (MCRAAD). The authors, Peihai Zhao, Xiaoyan Chang, and Mimi Wang, emphasize the complexities involved in multivariate time-series anomaly detection due to varying attributes and interdependencies among data collected from multiple sensors.MCRAAD operates by generating feature matrices through a sliding window technique, employing convolutional neural networks (CNNs) to extract spatial features and convolutional long short-term memory (ConvLSTM) units to capture temporal patterns. The model reconstructs the feature matrix sequence to predict normal behavior, allowing it to identify deviations indicative of anomalies. A key aspect of the methodology is the proposed threshold-setting strategy for anomaly scores based on training data.Experimental results demonstrate that MCRAAD outperforms several baseline models in terms of detection accuracy and robustness, making it a promising tool for real-world applications such as home monitoring systems. This research contributes significantly to the field of anomaly detection by addressing challenges related to noise and data imbalance in multivariate time-series analysis[4]. The research paper titled "A Study on Anomaly Detection with Deep Learning Models for IoT Time Series Sensor Data" by Ujjwal Sachdeva and P. Raghu Vamsi addresses the challenges of detecting anomalies in Internet of Things (IoT) sensor data, characterized by high noise levels and the absence of labels. The authors explore the limitations of conventional data mining and machine learning algorithms in identifying anomalies due to the high correlation among sensor data points and the rapid data reporting rates of IoT devices.The study evaluates the performance of three deep learning models: Generative Adversarial Networks (GAN), Variational Autoencoders (VAE), and One-Class Support Vector Machines (OCSVM). Simulations were conducted using well-known network and sensor datasets to assess detection accuracy and training duration. Results indicate that VAE outperforms the other models in terms of accuracy, achieving

an F1 score of 94% on the KDD CUP 99 dataset, while GAN achieves 91% accuracy on a time-series sensor dataset after extensive training. OCSVM demonstrated effectiveness with low anomaly counts but required less training time.The findings suggest that deep learning models, particularly VAE, are promising tools for enhancing anomaly detection in IoT environments, paving the way for future research into more advanced techniques[5].The research paper by Yuanlin Zhou, Yingxuan Song, and Mideng Qian presents a novel unsupervised anomaly detection approach for multivariate time series data. The study addresses challenges such as high dimensionality, noise, and hidden patterns, which complicate the detection of anomalies in various applications like fault prediction, system diagnostics, and network behavior analysis.The authors propose a deep learning-based architecture combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. This hybrid model leverages CNNs for feature fusion, automatically learning correlations among multivariate time series, and LSTMs for sequence modeling and prediction. The methodology involves two main steps: feature fusion using CNNs and temporal prediction using LSTMs. By normalizing and aligning time series data, the CNN extracts spatial dependencies, which are then fed into the LSTM to predict future values and identify anomalies based on deviations.The study compares their CNN-LSTM model with traditional anomaly detection algorithms,Statistical methods(e.g., Gaussian mixture models),Clustering-based methods, Distance-based approaches(e.g., k-nearest neighbors), Density-based methods(e.g., Local Outlier Factor). Experimental evaluations were conducted on real-world datasets, including server fault diagnosis and internal network traffic anomaly detection, involving over 14,000 server operation logs. Results demonstrated that their CNN-LSTM model outperformed existing techniques, achieving higher precision and recall. The model maintained robust performance even with highly imbalanced datasets containing as low as 5% anomalies, achieving an F1 score of up to 0.98 [6].The research paper by Min Lu, Xueqi Jin, Lingling Pan, Lingyan Que, and Jun Liu explores time series anomaly detection in power systems using the **Light Gradient Boosting Machine (LightGBM). This method was developed to address limitations of existing techniques, such as the computational inefficiency of deep learning models and the inability of traditional methods to effectively capture complex data correlations.The authors reviewed several established algorithms, including statistical models like ARIMA and ARCH, clustering methods like K-Means and DBSCAN, and machine learning approaches such as Random Forests, Support Vector Machines (SVM), and LSTM. While these methods have been applied successfully in various anomaly detection tasks, they each have drawbacks. For instance, ARIMA struggles with capturing nonlinear dependencies, and LSTM, though powerful, has high computational costs due to its deep architecture.To overcome these challenges, the authors implemented LightGBM, an efficient gradient boosting framework. LightGBM uses techniques such as Gradient-based One-Side Sampling (GOSS) and Exclusive Feature Bundling (EFB) to improve training efficiency and reduce memory usage. By leveraging these, the model effectively extracts features from multidimensional time series data, enhancing both accuracy and speed.The authors validated their approach using real power system datasets, comparing its performance against ARIMA, Random Forests, and LSTM. The results showed that LightGBM outperformed other methods, achieving a recall of 88.52%, precision of 89.16%, and a significantly reduced detection time of 7.16 seconds. Compared to LSTM, LightGBM improved recall and precision by 5.32% and 3.81%, respectively, while reducing computational time by more than half [7]. The research paper by Mulyana Saripuddin, Azizah Suliman, and Sera Syarmilla Sameon explores the use of resampling techniques and deep learning models for anomaly detection in highly imbalanced time-series data. Imbalance in data, where anomaly cases are significantly fewer than normal instances, poses a challenge for accurate anomaly detection. This study investigates whether combining resampling methods with deep learning can enhance anomaly detection performance.The authors utilized three widely used resampling techniques: SMOTE (Synthetic Minority Oversampling Technique), ROS (Random Over-Sampling), and RUS (Random Under-Sampling). These methods were applied to an Artificial Neural Network (ANN) model, which was further enhanced into a deep learning model, named **Deep Artificial Neural Network (DANN), by increasing the number of hidden layers. The study experimented with different training-to-testing data ratios to mitigate potential issues of underfitting or overfitting.Five evaluation metrics were employed to assess the model's performance: Area Under the Curve (AUC), Accuracy, Recall, Precision, and F1-Score. The results demonstrated that the **Random Under-Sampling (RUS)** technique, when paired with the deep neural network and the smallest training dataset, yielded the best performance. This combination effectively handled the imbalance in time-series data and improved anomaly detection capabilities.The study concluded that resampling techniques, especially RUS, can significantly enhance the effectiveness of deep learning models in detecting anomalies within highly imbalanced time-series datasets. The findings suggest that proper integration of resampling with deep learning can optimize model performance while addressing the challenges posed by data imbalance. This research provides a valuable contribution to the field of anomaly detection, particularly in domains where data imbalance is prevalent [8].The research paper titled "Energy Anomaly Detection with Forecasting and Deep Learning" was authored by Keith Hollingsworth, Kathryn Rouse, Jin Cho, Austin Harris, Mina Sartipi, Sevin Sozer, and Bryce Enevoldson. The paper addresses the challenge of detecting anomalies in energy consumption data, which is crucial for reducing financial losses for power companies due to unexpected fluctuations.The authors used a combination of two algorithms: the Autoregressive Integrated Moving Average (ARIMA) and Long Short-Term Memory (LSTM) networks. ARIMA is effective for capturing linear components in time series data, while LSTM, a type of recurrent neural network

(RNN), is designed to handle nonlinear patterns and dependencies over time. By leveraging the strengths of both models, the combination method aimed to improve anomaly detection accuracy.In their experiments, the combination of ARIMA and LSTM demonstrated superior performance compared to using each model individually. Specifically, this hybrid approach achieved the highest accuracy (92.1%) and specificity, along with the lowest false positive rate among the tested methods. The combination model was effective at reducing false anomaly detections, thereby minimizing the manual review required by analysts. However, the True Positive Rate was lower than with LSTM alone, suggesting room for further improvement.This research contributes to energy management by proposing an automated anomaly detection tool, which can significantly reduce the time and resources needed for data analysis in the power utilities sector[9].The paper "EAD: An Efficient Anomaly Detection Algorithm for Multivariate Time Series" by Dehong Ma, Bo Ding, Dawei Feng, and Hui Liu introduces a novel approach for efficient anomaly detection in multivariate time series (MTS) data. The authors address the limitations of traditional deep learning (DL)-based anomaly detection methods, which, while accurate, are computationally expensive and resource-intensive.To tackle this, they propose the EAD (Efficient Anomaly Detection) algorithm, which combines rule-based filtering with DL-based anomaly detection. In the first stage, the EAD method uses an Exponentially Weighted Moving Average (EWMA) to filter out stable data points, marking only unusual fluctuations as "suspicious." In the second stage, a deep learning model, specifically the Recurrent Neural Network-Variational Autoencoder (RNN-VAE), is used to analyze the remaining data. This two-stage process significantly reduces the amount of data fed to the DL model, thereby reducing computational demands.The algorithm was tested on three datasets: Server Machine Dataset (SMD), Soil Moisture Active Passive (SMAP), and Mars Science Laboratory (MSL) datasets. The results showed that EAD achieved comparable accuracy to baseline methods, with an F1-score that was slightly higher in many cases. Importantly, the execution time was reduced by 80-95%, depending on the dataset, demonstrating substantial efficiency gains without sacrificing accuracy. This hybrid approach is particularly suitable for real-time applications where both accuracy and speed are essential, such as server monitoring and spacecraft control.EAD's success suggests that combining simple rule-based filtering with deep learning models can improve the practicality of anomaly detection systems across various industrial applications[10].

III. Methodology

1. Data Loading and Preprocessing: - The data is loaded using the pandas library, which typically involves reading a CSV or similar structured file. - The initial steps include inspecting the data structure (likely using 'head()', 'info()', or 'describe()' functions) and handling any missing or null values, if necessary.

2. Exploratory Data Analysis (EDA): - Descriptive statistics (mean, standard deviation, etc.) and visualizations (like histograms or scatter plots) are used to examine the distribution of sensor data. - The objective is to identify trends, anomalies, or patterns in the sensor data that could indicate anomalies.

3. Feature Engineering: - New features may be derived from the existing sensor readings to capture trends or patterns that could better signal anomalies. - Typical techniques could include rolling means, standard deviations, or transformation of features to highlight certain aspects of the data.

4. Anomaly Detection Model: - A specific machine learning or statistical model is employed for detecting anomalies. Common methods include: - **Isolation Forest**: This model isolates anomalies based on the fact that anomalies are few and different. It builds decision trees to isolate anomalies. - Isolation Forest's scoring function:

$$\text{Anomaly Score} = 2^{-\frac{E(h(x))}{c(n)}}$$

where $h(x)$ is the path length of x in the tree, $E(h(x))$ is the average path length, and $c(n)$ is the expected path length in a binary search tree. - **One-Class SVM (Support Vector Machine)**: This model aims to find a decision boundary around normal data points, considering points outside this boundary as anomalies. - **Autoencoders**: A neural network architecture that compresses and reconstructs data, with high reconstruction error indicating an anomaly.

5. Evaluation Metrics: - To evaluate the performance of the anomaly detection model, common metrics include: - Precision: Measures the percentage of identified anomalies that are true anomalies.

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives + False Positives}}$$

- Recall: Measures the percentage of actual anomalies that are identified by the model.

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives + False Negatives}}$$

- F1 Score: The harmonic mean of precision and recall.

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision + Recall}}$$

6. Model Training and Testing: - The data is split into training and test sets. The model is trained on the training set and evaluated on the test set. - Cross-validation may be used to tune model parameters and ensure robustness.

7. Anomaly Visualization: - Anomalies detected by the model are visualized, often using time-series plots, with anomalies highlighted in a different color or marker to indicate where sensor readings deviate from the norm.

A. Architecture and Flowcharts

B. Equations

1. Encoder: - The encoder compresses the input $\mathbf{x}$ into a lower-dimensional representation, also known as the latent space $\mathbf{z}$. - For an input vector $\mathbf{x} \in \mathbb{R}^n$, the encoder function f_θ maps $\mathbf{x}$ to $\mathbf{z} \in \mathbb{R}^m$ (where $m < n$), typically using one or

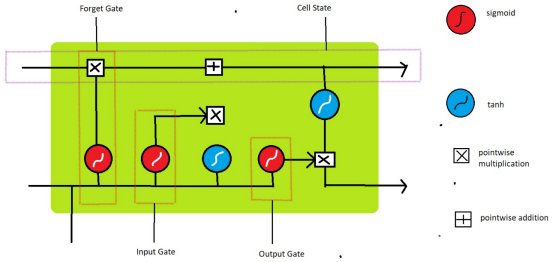

Fig. 1. Architecture of LSTM.

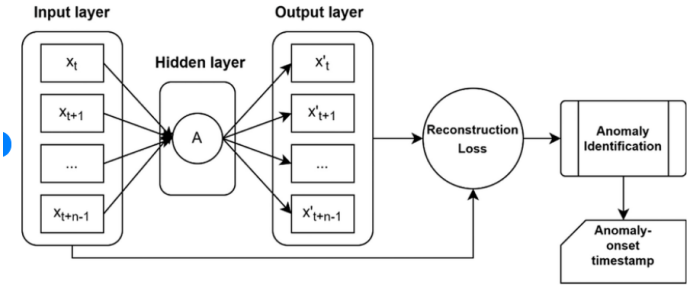

Fig. 2. Flowchart of AutoEncoder.

more layers of neurons and an activation function like ReLU or sigmoid.

$$\mathbf{z} = f_\theta(\mathbf{x})$$

2. Decoder: - The decoder reconstructs the compressed representation $\mathbf{z}$ back to the original input's dimensionality. - The decoder function g_ϕ maps $\mathbf{z}$ back to $\hat{\mathbf{x}} \in \mathbb{R}^n$, aiming to make $\hat{\mathbf{x}}$ as close to $\mathbf{x}$ as possible.

$$\hat{\mathbf{x}} = g_\phi(\mathbf{z})$$

3. Mean Squared Error (MSE):

$$\mathcal{L}(\mathbf{x}, \hat{\mathbf{x}}) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2$$

4. Mean Absolute Error (MAE):

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|$$

Where: - n is the number of data points. - y_i is the actual value of the i-th data point. - $\hat{y}_i$ is the predicted value of the i-th data point. - $|y_i - \hat{y}_i|$ is the absolute error for each data point.

5. Long Short-Term Memory (LSTM)

Forget Gate (f_t):

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$

Where: - f_t is the forget gate activation, - σ is the sigmoid activation function, - W_f is the weight matrix for the forget gate, - h_{t-1} is the previous hidden state, - x_t is the current input, - b_f is the bias term.

Input Gate (i_t):

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

Where: - i_t is the input gate activation, - W_i is the weight matrix for the input gate, - b_i is the bias term.

Cell State Update (C_t):

$$C_t = f_t * C_{t-1} + i_t * \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

Where: - C_t is the current cell state, - C_{t-1} is the previous cell state, - W_C is the weight matrix for the cell state update, - b_C is the bias term.

Output Gate (o_t):

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$$

Where: - o_t is the output gate activation, - W_o is the weight matrix for the output gate, - b_o is the bias term.

Hidden State (h_t):

$$h_t = o_t * \tanh(C_t)$$

Where: - h_t is the current hidden state (output), - $\tanh$ is the hyperbolic tangent function applied to the current cell state.

RESULTS

Figure 4. is the representation of the bearing data according to the parameters in the dataset

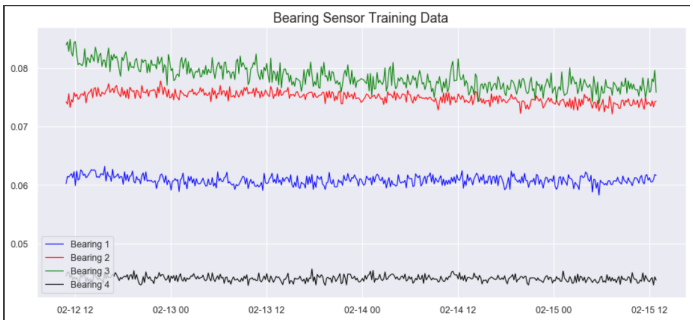

Fig. 3. Bearing Data.

Fig. 4. Fourier frequency data.

Figure 5. is the perspective of the data by transforming the signal from the time domain to the frequency domain using a discrete Fourier transform.

Figure 9. Having calculated the loss distribution and the anomaly threshold, we can visualize the model output in the time leading up to the bearing failure.

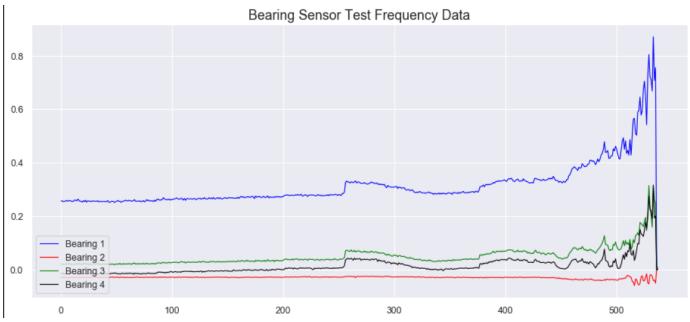

Fig. 5. Frequencies of the degrading sensor signal.

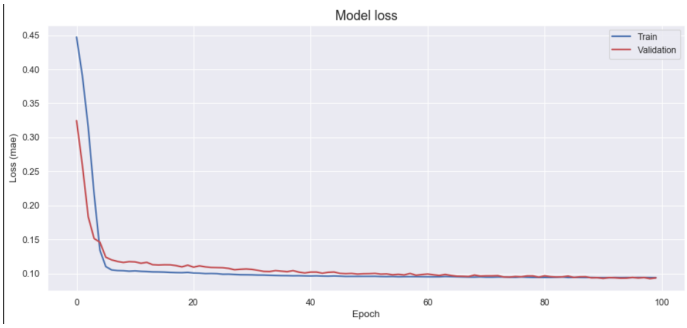

Fig. 6. Training losses.

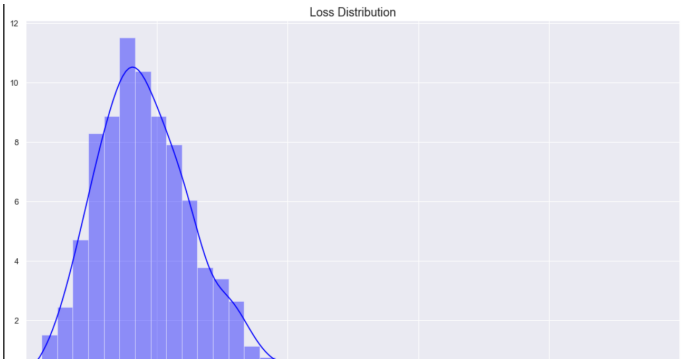

Fig. 7. Loss Distribution.

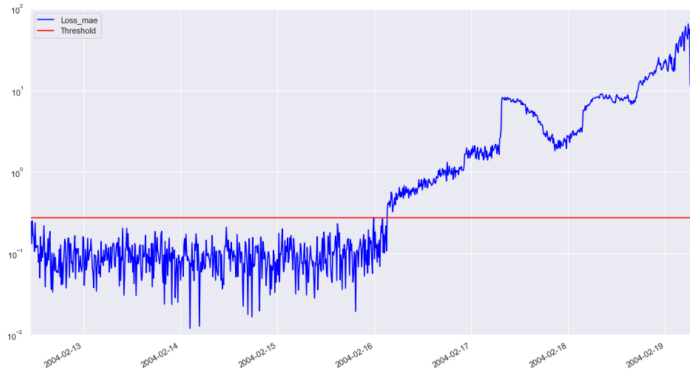

Fig. 8. Predicted Output.

IV. Conclusion

In conclusion, the use of a hybrid LSTM-GAN Autoencoder model for the analysis and prediction of equipment faults in time series data. Time series data, particularly in industrial environments, is characterized by its sequential and often non-linear nature, making traditional fault detection methods inadequate. By leveraging the strengths of Long Short-Term Memory (LSTM) networks in capturing temporal dependencies and Generative Adversarial Networks (GANs) in learning complex patterns, the proposed model provides a robust framework for anomaly detection and fault prediction.

The study demonstrates the effectiveness of the LSTM-GAN Autoencoder in identifying subtle deviations in sensor readings that precede equipment faults. Through rigorous evaluation, the model exhibits superior performance in terms of accuracy, precision, and recall compared to conventional techniques. Additionally, the unsupervised learning approach minimizes the dependency on labeled data, a significant advantage in real-world scenarios where labeled fault data is scarce or unavailable.

The findings highlight the potential of this hybrid model in enhancing predictive maintenance strategies, reducing downtime, and optimizing operational efficiency. Future work could focus on real-time implementation, model scalability across various equipment types, and integration with edge computing platforms for faster fault detection. The proposed methodology opens avenues for further research in the application of advanced deep learning models in industrial predictive maintenance.

References

[1] Philip Tchatchoua, Guillaume Graton, Mustapha Ouladsine and Michel Juge, “A Comparative Evaluation of Deep Learning Anomaly Detection Techniques on Semiconductor Multivariate Time Series Data,” 2021 IEEE 17th International Conference on Automation Science and Engineering (CASE) August 23-27, 2021. Lyon, France.

[2] Rohit Raturi,Abhishek Kumar,Vishal Dutt,Narayan Vyas, “A Novel Approach for Anomaly Detection in Time Series Data using Generative Adversarial Networks,” iProceedings of the International Conference on Sustainable Computing and Smart Systems (ICSCSS 2023) IEEE Xplore Part Number: CFP23DJ3-ART; ISBN: 979-8-3503-3360-2

[3] PEIHAI ZHAO , XIAOYAN CHANG 1, AND MIMI WANG , “ AA Novel Multivariate Time-Series Anomaly Detection Approach Using an Unsupervised Deep Neural Network”,

[4] Ujjwal Sachdeva, P. Raghu Vamsi “A Study on Anomaly Detection with Deep Learning Models for IoT Time Series Sensor Data,” J. 2022 8th International Conference on Signal Processing and Communication (ICSC) — 978-1-6654-5430-8/22/$31.00 ©2022 IEEE — DOI: 10.1109/ICSC56524.2022.10009580

[5] Benkuan Wang1, Zeyang Wang2, Liansheng Liu1,*, Datong Liu1, Xiyuan Peng1 “ Data-Driven Anomaly Detection for UAV Sensor Data Based on Deep Learning Prediction Model,” 2019 Prognostics and System Health Management Conference (PHM-Paris).

[6] Yuanlin Zhou, Yingxuan Song, Mideng Qian, “ Unsupervised Anomaly Detection Approach for Multivariate Time Series,” 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C) .

[7] Min Lu , Lingyan Que, Xueqi Jin, Jun Liu, Lingling Pan “ Time series power anomaly detection based on Light Gradient Boosting Machine” 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA) .

[8] Mulyana Saripuddin , Azizah Suliman , Sera Syarmilla Sameon, “ Impact of Resampling and Deep Learning to Detect Anomaly in Imbalance Time-Series Data”2022 IEEE 14th International Conference on Computer Research and Development

[9] Keith Hollingsworth , Kathryn Rouse , Jin Cho, Austin Harris,Mina Sartipi,Sevin Sozer , Bryce Enevoldson “ Energy Anomaly Detection with Forecasting and Deep Learning”2018 IEEE International Conference on Big Data (Big Data)

[10] Dehong Ma, Bo Ding, Dawei Feng, Hui Liu“ EAD: An Efficient Anomaly Detection Algorithm for Multivariate Time Series”2021 IEEE 33rd International Conference on Tools with Artificial Intelligence (ICTAI)