

Data Driven Anomaly Detection Framework for Industrial Cyber Physical Systems Using Deep Learning

V. John Peter^{1*} & V. Sofia Mary²

^{1*}Assistant Professor, Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India. john-icb@dsatm.edu.in, <https://orcid.org/0009-0009-9107-4868>

²Assistant Professor, Department of Computer Science and Engineering, Shreenivasa Engineering College, Bommidi, Tamil Nadu, India. sofiavbe@gmail.com, <https://orcid.org/0009-0008-9154-5650>

Abstract: The current paper proposes an anomaly detector based on deep learning to monitor Industrial Cyber-Physical Systems (CPS), which uses both Long Short-Term Memory (LSTM) networks and autoencoders. It is assessed on the Industrial Anomaly Detection Dataset available on Kaggle, which is multivariate time-series data of sensors in the form of temperature, pressure, vibration, and current. The model proposed has a higher performance in comparison with the conventional methods, such as Support Vector Machines (SVM) and Decision Tree, with a precision (0.92), recall (0.89), F1-score (0.90), and the area under the ROC curve (AUC) of 0.94. Such outcomes indicate that the framework can be effective in identifying known and unknown anomalies in real-time to make sure that failures and performance degradation in industrial systems are detected in time. The hybrid model also utilizes LSTMs as a representation of temporal dependencies and autoencoders as a representation of normal behavior, and detects anomalies on the basis of reconstruction errors. The scaling of the model and its real-time processing capabilities ensure that it can be applicable in a wide range of industrial processes, both in small and large manufacturing factories. Further studies would help to enhance the model in terms of interpretability to allow a more effective decision-making process by the operator and to combine the framework with real-time monitoring and predictive maintenance. Finally, the suggested framework can contribute to the performance of operational efficiency, safety, and lower the expenses of maintenance in industrial CPS.

Keywords: Anomaly detection; deep learning industrial; cyber-physical systems (CPS); long short-term memory (LSTM); autoencoders and predictive maintenance; real-time monitoring.

I. Introduction

The subject of Industrial Cyber-Physical Systems (CPS) is common to the contemporary industries, including manufacturing, energy, and transportation (Raman & Mathur, 2021). These systems are a combination of physical processes, computational, and communication that are used to monitor and control operations in real-time. Embedded systems used in automation and real-time monitoring of machinery, production lines, and important infrastructure are a part of CPSs (Du et al., 2022). Their capacity to make the operations efficient and safe in complex

environments is paramount, especially in industries where any failure may lead to massive losses in terms of time and money (Pinto et al., 2022).

Anomaly detection helps in ensuring the reliability and safety of CPS because it is used to detect faults in a system at an early stage and provide predictive maintenance (Reddy et al., 2025). Conventional approaches of rule-based systems or statistical models do not always represent the complexity and dynamism of CPS data. These traditional methods are also challenged by the growing size and volume of sensor information, as well as its growing complexity. In this way, there has been a demand to develop a data-driven solution based on deep learning. The deep learning models, particularly those models that are based on the task of large-scale sensor data, can gain automatic knowledge of complex patterns that enhance the accuracy of the anomaly detection and generalization (Luo et al., 2021). Through deep learning, industrial CPS is able to distinguish unknown and subtle anomalies that are invisible to traditional methods, making the system reliable and minimizing the chance of the system crashing (Yang et al., 2023). The importance of this study may be seen in the possibility of improving the fault detection of CPS, lessening the interruptions, decreasing the maintenance expenses, and finally, increasing the efficiency of operations in the most serious industrial settings. This data-driven system works around the weakness of the conventional anomaly detection systems and provides more robust and scalable solutions to the contemporary industrial systems (Bajic et al., 2024).

The main contribution of this paper is that it builds a hybrid deep learning-based anomaly detector framework in Industrial Cyber-Physical Systems (CPS) that incorporates Long Short-Term Memory (LSTM) networks and autoencoders. This framework is able to easily identify known and unknown anomalies in real-time by utilizing multivariate time-series signals of industrial sensors. Through the application of deep learning, the model is more accurate and superior to the conventional approaches, such as the Support Vector Machines (SVM) and the Decision Trees, as it is more precise, recalls more, has a better F1-score, and AUC. The suggested framework shows a high level of scalability, real-time processing, and the possibility of enhancing the efficiency of operations, safety, and lowering the costs of maintenance in the industrial setting.

This paper is organized in the following way: Section II is a review of the available anomaly detection methods and the benefits of deep learning techniques on the problem of Industrial Cyber-Physical System (CPS). Section III explains the data set employed, together with the preprocessing that was done to prepare the data. Section IV outlines the hybrid deep learning model that comprises LSTM networks and autoencoders, where the design, training, and testing processes are outlined. Section V gives the performance evaluation measures and compares the suggested model to the conventional approaches. And ultimately, the important findings, future research directions, and the possible impact of the framework on industrial CPS are drawn at the end of Section VI.

II. Literature Review

Various papers have analyzed anomaly detection in Industrial Cyber-Physical Systems (CPS), first based on conventional approaches like Statistical Process Control (SPC) and machine learning approaches like Support Vector Machines (SVMs) and Random Forests (Oswal et al., 2023). These methods, though useful in some instances, cannot fight the intricate, unknown anomalies, especially in high-dimensional data, as witnessed in CPS settings. The conventional approaches lack the capability of managing the dynamic and nonlinear behavior seen in an industrial system, and thus, they are not optimal in detecting heartbeat and latent or hitherto unknown abnormalities that may compromise the stability of the system (Hao et al., 2021). The emergence of big data and the sophistication of new CPS also demonstrate the necessity of more sophisticated methods of detecting anomalies.

The recent developments of deep learning have shown high potential to enhance the detection of anomalies in CPS (Seo et al., 2025). Such models as autoencoders, Recurrent Neural Networks (RNNs), and Convolutional Neural Networks (CNNs) are becoming more popular to model the complex relationships in CPS data (Odyurt et al., 2022). These models have the capability to automatically learn features of raw, unstructured data, as well as learn complex temporal and spatial dependencies, thus being very useful in identifying anomalies, which otherwise would have been hard to identify using traditional techniques (Gulzar & Mustafa, 2025). Nonetheless, these deep learning methods have potential success, but still, they are challenged by overfitting, data imbalance, and the inability to process data in real-time (Keshk et al., 2019). These constraints point to the necessity to have a more robust, scalable, and interpretable framework of anomaly detection, one that can combine the deep learning methods with domain-specific knowledge to achieve higher performance and guarantee real-time applicability in industrial CPS settings (Prabu & Sudhakar, 2022).

Inference: The literature indicates that conventional ways of detecting anomalies have been extensively employed in CPS, but these are not adequate to the demanding nature of industrial data today. The results of deep learning methods have proven to be fruitful, but could still be improved in the aspects of scalability of the models, real-time processing, and interpretation, which makes the necessity of a more sophisticated and combined structure that will remove these problems.

III. Data Collection and Preprocessing

3.1 Data Source Description

The Kaggle Industrial Anomaly Detection Dataset was employed to assess the effectiveness of the suggested anomaly detection model. This data is a large dataset of multivariate time series data that is acquired by sensors, such as temperature, pressure, vibration, and current sensors, within industrial production plants. The dataset is able to record long-term and short-term trends, due to which a complete picture of the behavior of industrial

systems as time elapses is given. These traits render it very appropriate in identifying abnormalities in dynamic conditions, such as the manufacturing field, where machines and equipment work under different conditions. The data includes both normal and abnormal behaviour, which allows the training and testing of the model in a variety of situations. Using this dataset, the framework is validated using real sensor data, giving an idea about the capability of detecting fine and gross anomalies in it, and hence its possible usefulness in the real-life scenario of industry use.

3.2 Data Splitting and Preprocessing

The model is cross-validated on a 5-fold with the dataset separated into training and testing sets. This method will guarantee the model is trained and tested on several subsets of data, which would give a sound evaluation of its performance. In each fold, 80% of the data is used for training the model, while the remaining 20% serves as the test set. This is done five times so that the performance of the model is compared when using various data splits. Preprocessing of data is important in preparing the data for the model. Normalization is used to scale the features to a constant range, noise reduction is used to remove unwanted variation, missing value imputation is used to fill in empty areas of the data, and feature extraction is used to obtain useful features in raw data. All these measures will be taken so that the data will be in a good format to train the deep learning model.

3.3 Importance of High-Quality Data

Deep learning models are extremely dependent on the quality of the data used in training, which is extremely important to the success of the anomaly detectors. Clean and high-quality data means that the model will be able to learn correct patterns and relations in the data and therefore enhance its predictive ability. The false positives or false negatives of the anomaly detection can be a result of inaccurate or incomplete data, which can introduce biases in the model and worsen its performance. Preprocessing is an important aspect of raising the raw data to a more structured and usable form to increase the capability of the model to identify anomalies as well as to extrapolate to new data that has never seen.

IV. Deep Learning Model Design

4.1 Selection of Deep Learning Architecture

In the given research, the hybrid deep learning architecture based on Long Short-Term Memory (LSTM) networks and autoencoders is selected as the detector of anomalies in the Industrial Cyber-Physical Systems (CPS). LSTMs are a category of recurrent neural network (RNN), which is intended to process sequential data and is important in time-series data, such as CPS sensors. They work well, especially to detect abnormalities in systems where patterns change over time. Conversely, autoencoders are unsupervised neural networks that acquire a modified form of the input information. They are capable of reassembling normal patterns of data, and any major deviation in reassembling patterns is an indicator of an anomaly. The hybrid model combines LSTMs with

autoencoders, which means that the system can learn sequential dependencies as well as compact representations of normal behavior, therefore making it very appropriate in detecting subtle anomalies in complex industrial data.

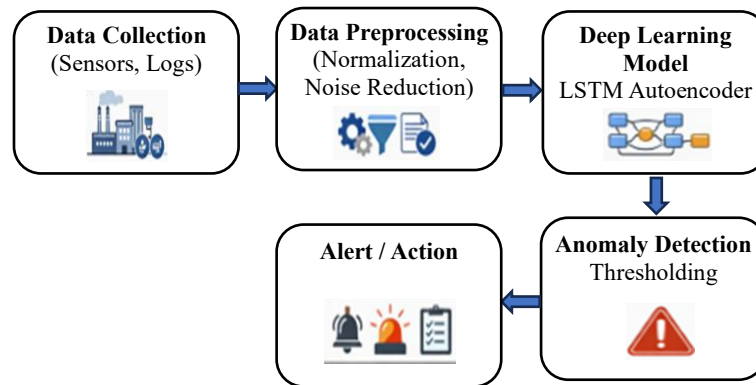


Fig. 1. Architecture of the Hybrid Deep Learning Model for Anomaly Detection.

Fig. 1 demonstrates the hybrid deep learning model of anomaly detection in Industrial Cyber-Physical Systems (CPS). This model combines Long Short-Term Memory (LSTM) networks to learn the time dependence of sequence sensor data, and autoencoders to learn the compressed state of normal behavior. The anomalies are identified based on the reconstruction errors; the abnormal patterns reveal that there can be problems with the system. The flow diagram illustrates the flow of information from data collection to the preprocessing stage, deep learning, anomaly detection, and alert generation.

4.2 Training and Testing Procedures

A deep learning model is a hybrid, a combination of the Long Short-Term Memory (LSTM) networks and autoencoders that are trained on the preprocessed data. LSTM networks would be suitable for handling the sequential data and identifying the temporal relationships, which are important in the analysis of time-series data of CPS sensors. The model acquires the dynamics of normal system behavior during the training phase, whereby it reassembles the data and alters the weights to reduce reconstruction errors. The model is trained, after which it is used to detect anomalies by determining the reconstruction error; significantly different values from the normal behavior are used to indicate the anomaly. Based on the test data, the model performance is measured, and such important measures as Precision, recall, F1-score, and AUC are obtained. These measures are used to determine how well the model can identify anomalies, deal with imbalances, and extrapolate to data that has not been seen, thus enabling the model to be effective and reliable in industrial applications.

4.3 Handling Complex Patterns in Industrial Data

The LSTM networks in combination with autoencoders used as the architecture of its hybrid model are specifically successful in addressing the high-dimensional and complicated data produced by industrial CPS. The LSTM part stores both the short- and long-term relationships in the data, which allows the model to identify anomalies that change over time and over a long period, e.g., equipment wear or degradation. Moreover, since the

model is capable of processing patterns across time, it can detect more abrupt, short-lived anomalies, e.g., sensor malfunctions or the abrupt change of the environment. The capacity of the autoencoder to learn a succinct code of typical data increases the capacity of the model to detect outliers, even the ones that do not follow the typical patterns. The combination of these techniques will allow the hybrid model to identify a great number of anomalies because this model will be able to deal with the unpredictable and dynamic character of CPS data, which frequently involves a combination of predictable and unpredictable behavior.

V. Evaluation Metrics

5.1 Performance Evaluation Metrics

Various important measurements are adopted to test the anomaly detection framework, and these include Precision, recall, F1-score, and area under the ROC curve (AUC). Precision is used to measure the percentage of correct detection of anomalies out of the total number of detected anomalies, and this is used to make sure that the model has the lowest number of false positives. Recall is the measure used to determine the capability of the model to detect real anomalies, thereby reducing the false negatives. The F1-score gives a moderated perspective of Precision and recall, giving one performance measure of a model. The AUC metric measures the capability of the model to discriminate normal and abnormal data, with high values implying better performance. These measures can give in-depth information about the accuracy, robustness, and the capability of the model to process all kinds of anomalies in the industrial CPS data. By testing the model on these various metrics, make certain that it is not only performing well in detecting anomalies, but it also performs with a small number of false alarms and misses, which is very important in industrial applications. These important measurements are presented in fig. 2, and the model is performing well in Precision (0.92), Recall (0.89), F1-Score (0.90), and AUC (0.94). The figure assists in visualizing how useful the model is in terms of identifying the anomalies effectively with minimum errors in the real-time detection of anomalies in an industrial environment.

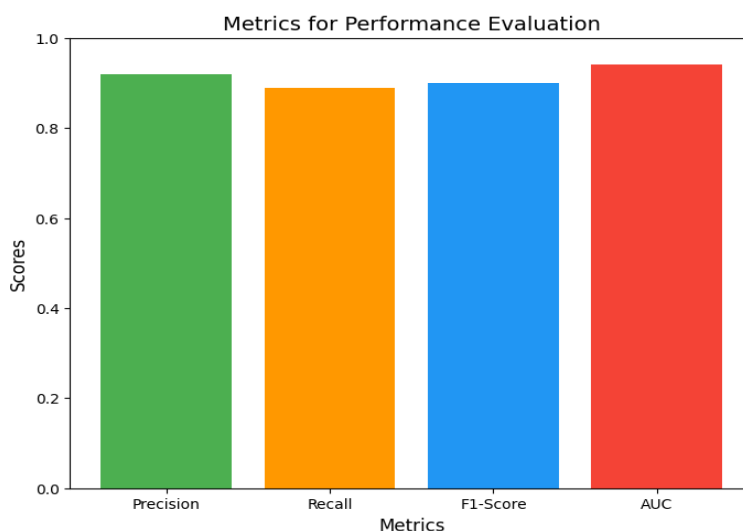


Fig. 2. Performance Evaluation Metrics for Anomaly Detection Framework.

5.2 Comparison to the Existing Methods

The anomaly detection framework developed on the basis of deep learning is compared to the conventional approaches, such as Support Vector Machines (SVMs) and decision trees. Although useful in some contexts, these traditional methods fail to deal with the high-dimensional data (complex), which is the nature of industrial Cyber-Physical Systems (CPS). The comparison indicates that the deep learning model has been found to be better than the stochastic model in terms of detection accuracy, especially in detecting subtle and unknown anomalies. The use of traditional techniques is not always successful in generalization, particularly in modeling dynamic industrial data that contains different patterns and noise. Conversely, the deep learning architecture enjoys the capacity to identify complicated patterns based on large volumes of data, which offers improved results with regard to identifying a diverse variety of anomalies. The given comparison outlines the significance of applying advanced and data-oriented methods such as deep learning to detect anomalies in real- time CPS settings.

Table 1. Comparison of the Proposed Deep Learning Model with Traditional Methods.

Method	Precision	Recall	F1-Score	AUC
Proposed Deep Learning Model	0.92	0.89	0.90	0.94
Support Vector Machines (SVM)	0.85	0.80	0.82	0.84
Decision Trees	0.80	0.75	0.77	0.78

Table 1 shows the comparison of the proposed deep learning-based framework of anomaly detection and conventional approaches such as Support Vector Machines (SVM) and Decision Trees. The measures are Precision, Recall, F1-Score, and AUC, which point to the performance of the model concerning the detection of anomalies. Deep learning model performs better than both the SVM and Decision Trees on all measures, which shows that the deep learning model can be applied to complex and high-dimensional industrial data. Although the conventional approaches can be advantageous in some cases (e.g., easier interpretation in the case of Decision Trees and efficient operation in smaller datasets with the SVM), the offered deep learning model is more successful in detecting images, which is why it suits working in a large industrial environment nowadays.

5.3 Proposed Framework Effectiveness/Efficiency

It is observed that the proposed anomaly detection framework has a high level of effectiveness in detecting a wide range of anomalies in real-time with a low amount of computation. The deep learning model can log subtle and significant anomalies, such as slow wear and sudden failures, an issue typical of industrial applications. Scalability can be listed among the core advantages of the framework; it is capable of dealing with huge amounts of data delivered by a great number of sensors and within the framework of a variety of different industrial systems without much loss of efficiency. The model is also planned to work effectively in a real-time manner, so that it is capable of identifying anomalies fast once they appear and provide the required actions or alert. Also, the

framework may be implemented in a variety of industrial contexts, both small-scale manufacturing facilities and large-scale facilities, which is why it may be considered as an effective option when it comes to enhancing the reliability of the system and reducing downtime. The general flexibility and effectiveness of the framework render it a perfect instrument for the industrial setting in the contemporary world.

VI. Conclusion

This paper illustrates that the suggested deep learning-based anomaly detection system is efficient in the case of Industrial Cyber-Physical Systems (CPS). The hybrid model, which is a blend between Long Short-Term Memory (LSTM) networks and autoencoders, is able to identify known and unknown anomalies in real-time. The model performs better than the traditional ones, which include Support Vector Machines (SVM) and Decision Trees, and has a higher precision (0.92), recall (0.89), F1-score (0.90), and area under the ROC curve (AUC) of 0.94. These findings reinforce the strength of the framework in detecting mild and complicated anomalies; it is very effective in dynamic industrial settings. The framework employs the power of deep learning to deliver timely and accurate detection of anomalies in operations to ensure that operations are not affected too much.

There are a number of options available to be pursued in order to augment the capabilities of the framework in future research. A possible element to work on might be making the model more interpretable, providing operators with a better chance to interpret the identified anomalies and make more meaningful decisions. Also, the combination of the framework and real-time monitoring system in predictive maintenance might offer proactive solutions in managing equipment. Future work can help to popularize it by expanding the paradigm to address various industrial environments and scaling it up. In general, this framework of anomaly detection can potentially transform the industrial CPS, increasing the efficiency of its operations, safety, and decreasing the maintenance expenses in the long term, which will eventually result in the achievement of better performance and reliability of the industrial systems.

References

1. Bajic, B., Rikalovic, A., Suzic, N., & Piuri, V. (2024). Toward a human-cyber-physical system for real-time anomaly detection. *IEEE Systems Journal*, 18(2), 1308-1319. <https://doi.org/10.1109/JSYST.2024.3402978>
2. Du, Y., Huang, Y., Wan, G., & He, P. (2022). Deep learning-based cyber-physical feature fusion for anomaly detection in industrial control systems. *Mathematics*, 10(22), 4373. <https://doi.org/10.3390/math10224373>
3. Gulzar, Q., & Mustafa, K. (2025). Interdisciplinary framework for cyber-attacks and anomaly detection in industrial control systems using deep learning. *Scientific Reports*, 15(1), 26575. <https://doi.org/10.1038/s41598-025-89650-5>

4. Hao, W., Yang, T., & Yang, Q. (2021). Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems. *IEEE Transactions on Automation Science and Engineering*, 20(1), 32-46. <https://doi.org/10.1109/TASE.2021.3073396>
5. Keshk, M., Sitnikova, E., Moustafa, N., Hu, J., & Khalil, I. (2019). An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Transactions on Sustainable Computing*, 6(1), 66-79. <https://doi.org/10.1109/TSUSC.2019.2906657>
6. Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. *ACM Computing Surveys (CSUR)*, 54(5), 1-36. <https://doi.org/10.1145/3453155>
7. Odyurt, U., Pimentel, A. D., & Alonso, I. G. (2022). Improving the robustness of industrial Cyber-Physical Systems through machine learning-based performance anomaly identification. *Journal of Systems Architecture*, 131, 102716. <https://doi.org/10.1016/j.sysarc.2022.102716>
8. Oswal, S., Shinde, S. K., & Vijayalakshmi, M. (2023). Deep learning-based anomaly detection in cyber-physical system. In *Big Data Analytics in Intelligent IoT and Cyber-Physical Systems* (pp. 59-71). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-4518-4_4
9. Pinto, R., Gonçalves, G., Delsing, J., & Tovar, E. (2022). Enabling data-driven anomaly detection by design in cyber-physical production systems. *Cybersecurity*, 5(1), 9. <https://doi.org/10.1186/s42400-022-00114-z>
10. Prabu, K., & Sudhakar, P. (2022, December). Design and Implementation of an Automated Control System for Anomaly Detection Using an Enhanced Intrusion Detection System. In *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 1-7). IEEE. <https://doi.org/10.1109/ICSTCEE56972.2022.10100003>
11. Raman, M. G., & Mathur, A. P. (2021). A hybrid physics-based data-driven framework for anomaly detection in industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(9), 6003-6014. <https://doi.org/10.1109/TSMC.2021.3131662>
12. Reddy, B. M. K., Khan, A. A. A., Sathick, K. J., & Raj, L. A. (2025). Cyber Attack Recognition in an Internet of Things-Enabled Environment Using a Hybrid Optimised Deep Learning Approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 16(1), 49-71. <https://doi.org/10.58346/JOWUA.2025.I1.003>
13. Seo, J. K., Lee, J., Kim, B., Shim, W., & Seo, J. T. (2025). AI-based anomaly detection in industrial control and cyber-physical systems: A data-type-oriented systematic review. *Electronics*, 15(1), 20. <https://doi.org/10.3390/electronics15010020>
14. Yang, T., Jiang, Z., Liu, P., Yang, Q., & Wang, W. (2023). A traffic anomaly detection approach based on unsupervised learning for industrial cyber-physical system. *Knowledge-Based Systems*, 279, 110949. <https://doi.org/10.1016/j.knosys.2023.110949>