



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Secure AI-Enabled Cyber-Physical Framework for Integrated Fluid, Mechanical, and Electrical Systems

Dr. Pravin Prakash Adivarekar¹, Bibhuprasad Mohanty², Dr Jaksan D Patel³, Dr. Suman Mehta⁴, Prerana Kulkarni⁵, Binod Kumar Pattanayak⁶

¹Associate Professor, University -A.P.Shah Institute of Technology, Mumbai University, ppadivarekar@apsit.edu.in

²Professor, Department of Electronics and Communication Engineering Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India, E-mail: bibhumohanty@soa.ac.in

³Professor, Merchant Engineering College, Basna, Gujarat Mail ID -jaksanpatelmec1986@gmail.com

⁴Assistant Professor & Head of the Department Department of Computer Science and Engineering Millia Institute of Technology, Rambagh, Pune. Pin code – 854302 ORCID- 0009-0003-4661-3021 Mail ID - smehtacs@gmail.com

⁵Asst. Professor, Pillai University, New Panvel, Maharashtra, preranakulkarni@mes.ac.in, <https://orcid.org/0009-0008-1486-6549>

⁶Professor, Department of Computer Science and Engineering, Institute of Technical Education and Research Siksha O Anusandhan Deemed to be University Bhubaneswar, Odisha, India, Email: binodpattanayak@soa.ac.in

Abstract

The growing use of fluid, mechanical, and electrical elements in modern industrial systems creates a complex cyber-physical ecosystem in which an anomaly in one area can trigger subsequent issues throughout the other areas. Traditional monitoring practices typically operate in isolation and, as a result, may be ill-suited to detecting coupled faults, cyber-attacks, and incipient performance degradation. This article proposes a secure artificial intelligence (AI)-enabled cyber-physical framework for fluid, mechanical, and electrical systems. The framework leverages Internet of Things (IoT) sensing, secure edge/fog computing, cross-domain feature engineering, ensemble artificial intelligence, digital-twin-assisted monitoring, and coordinated supervisory control. Fluid pressure, flow rate, and temperature, mechanical speed, torque, and vibration, and electrical voltage, current, frequency, and power factor are continuously acquired and processed. Cross-domain residual indicators are proposed to capture physically inconsistent information and enhance the discrimination of equipment faults from malicious data tampering. A reproducible synthetic digital-twin dataset comprising 10,500 operating instances was constructed, representing normal conditions, fluid, mechanical, electrical faults, and cyber-attacks. Random Forest, Gradient Boosting, Support Vector Machine, Logistic Regression, and a soft-voting ensemble were evaluated. The ensemble achieved an overall accuracy of 91.43%, a weighted precision of 91.59%, a recall of 91.43%, and an F1-score of 91.37%. Cross-domain consistency features improved the overall ensemble accuracy from 89.08% to 91.43% and the recall of cyber-attack from 69.50% to 76.50%. The study reveals that the combination of AI-based condition assessment and secure fog processing with cross-domain consistency can form a tripartite foundation for building a resilient monitoring and intelligent control paradigm of multidisciplinary industrial systems.

Keyword: Artificial intelligence; cyber-physical systems; IoT; fog computing; fluid systems; mechanical systems; electrical systems; cybersecurity; anomaly detection; predictive maintenance; digital twin.

Introduction

Nowadays, various types of industrial equipment are considered integrated systems of fluid, mechanical, electrical, computational, and communication functions. Pump aggregates, hydro-systems, compressors, turbines, automated technological complexes, engineering plants, air-cooling systems, and power machines are a part of such objects. In these examples, electrical motors are used to produce rotational motion, mechanical elements transmit this movement, and fluid machines transform it into a pressure difference and flow. Therefore, in the interaction of their elements, any deviation from the norm is not only a local phenomenon.

The expansion of Internet of Things (IoT) has enabled the development of continuous sensing and distributed monitoring technologies. Swain et al. [3] demonstrated that heterogeneous technologies of sensors can be incorporated into IoT to identify real-time physical field data and facilitate machine learning-enabled predictions. The study by Swain et al. [3] also revealed that multiple sensor categories can be combined to enhance the representation capacity of a given system beyond the reach of a single channel.

Cloud-only architectures can be inappropriate and ineffective for applications requiring the rapid execution of control acts as data would have to move from physical devices into remote platforms and vice versa. Pati et al. [4] describe fog computing as an approach distributed towards the edge of the network to which data processing and computation are shifted, thus diminishing reliance on centralized processing, while also addressing privacy, security, and communication concerns. Similarly, HeartFog is also about exploiting IoT, cloud, and fog resources

for the sake of real-time decision support while evaluating latency, execution time, and power consumption alongside predictive performance [1].

Security becomes a critical concern when communication networks are directly connected to industrial actuators. A wrong pressure value, an incorrect motor-speed command, a fake voltage value, and a spoofed controller can lead to wrong decisions made by AI models even if physical equipment works properly. HeartFog utilizes FogBus, which unifies the concept of IoT, cloud, and fog with blockchain-based approaches to security, privacy, and data integrity [1]. Such ideas can be used to design secure distributed systems for industrial cyber-physical systems.

Machine learning can be used in practice for solving problems related to the identification of nonlinear dependencies with multiple variables. Rath et al. [2] discuss popular algorithms, including support vector machines, decision trees, neural networks, and Random Forest, and note the importance of choosing the right set of features and optimizing the set for performance. The use of ensemble learning is applicable when the behavior of individual algorithms is different in the case of noise, nonlinear changes in working conditions, and overlapping of fault symptoms.

However, the existing studies tend to apply AI-IoT-fog architectures in a specific application or data domain. This paper aims to provide a framework in which fluid, mechanical, electrical, AI, cybersecurity, and communication layers are analyzed together.

2. Research Problem and Objectives

A major limitation of conventional industrial monitoring is the independent analysis of individual subsystems. Take an electrically driven centrifugal pump as an example. Reduced flow could be due to pipe leakage, valve malfunction, cavitation, reduced shaft speed, motor electrical degradation, excessive mechanical load or deliberately manipulated sensor information. Monitoring only the flow sensor cannot reliably distinguish between these conditions.

Similarly, abnormal motor current could be caused by an electrical fault or increased mechanical torque due to obstruction of the fluid flow path. A cybersecurity mechanism monitoring only network packets could miss a physically feasible malicious command. The main question to be answered in this research is: How can AI, physical-systems relations, secure IoT communication, and distributed fog computing be combined to identify fluid, mechanical, electrical, and cyber-related anomalies in real-time?

2.1 Research Objectives

1. Develop an integrated cyber-physical architecture connecting fluid, mechanical, and electrical subsystems.
2. Design cross-domain features capable of identifying physical inconsistency among coupled variables.
3. Develop an ensemble AI mechanism for equipment-fault and cyber-attack classification.
4. Incorporate security mechanisms into sensing, communication, fog, and control layers.
5. Evaluate the proposed methodology using a reproducible synthetic digital-twin dataset.

3. Related Work

Fog-enabled AI architectures provide several concepts that can be transferred to industrial cyber-physical systems. HeartFog combines IoT, cloud, and fog computing while incorporating FogBus for distributed processing and communication protection [1]. The framework shows that a real-time AI application can be partitioned across physical devices, fog resources, and cloud resources while taking into account both the accuracy of predictions and network-level metrics.

Pati et al. [4] extend similar principles to an IoT and deep-transfer-learning environment in which fog nodes perform distributed processing. Their design includes gateway-based authentication, protected fog-node communication, resource monitoring, cloud resources, and AI inference. The same study discusses iFogSim as a tool for estimating latency, congestion, energy consumption, network use, and cost in IoT-fog environments [4].

Sensor diversity is also paramount. Swain et al. [3] present a solution which employs an IoT-based framework and utilizes machine learning algorithms to analyze the data received from several sensors in real time. Although the former's application is related to livestock monitoring, the general concept of using multiple readings to gather more information about the state of the monitored object remains the same.

The machine-learning literature also indicates the possibility of effective individual models. Rath et al. [2] address supervised learning models including SVM, Decision Trees, Neural Networks, and Random Forest as well as optimization approaches to improve the prediction. The above-mentioned sources encourage the application of the ensemble strategy in the current research.

3.1 Identified Research Gap

The content of the articles provided covers a significant amount of theoretical information related to distributed IoT-fog-cloud computing, real-time sensor processing, AI-based prediction and ensemble methods, security aspects, integrity, and latency. However, none of them offer a particular model for the secure observation of fluid, mechanical, and electrical physical processes. The present research aims to address this problem since the combined consideration of these aspects is the major challenge.

4. Proposed Secure AI-Enabled Cyber-Physical Framework

The framework under consideration includes six levels ranging from physical process sensing and secure communication means, through fog layer inference functions and artificial intelligence algorithms, to digital twin analytics functions and supervisory decision-making capabilities.

Table 1. Layered architecture of the proposed framework

Layer	Main Components	Primary Functions
1. Physical Process	Pumps, compressors, pipes, valves, shafts, bearings, motors, drives	Represents fluid, mechanical, and electrical energy conversion and process behavior.
2. Sensing and Actuation	Flow, pressure, temperature, speed, torque, vibration, voltage, current, frequency, power factor, valve position	Captures real-time process condition and applies authorized control actions.
3. Secure Edge/Fog	Industrial gateway, local compute node, authentication, encrypted communication	Performs filtering, feature extraction, security checks, local AI inference, and rapid alarms.
4. AI Intelligence	Fault classifier, anomaly detector, ensemble model, confidence estimator	Distinguishes normal operation, equipment faults, and cyber-related anomalies.
5. Digital Twin and Cloud	Historical database, model retraining, digital twin, fleet analytics	Supports long-term learning, simulation, expected-state estimation, and model management.
6. Supervisory Decision	HMI, PLC/safety logic, maintenance dashboard	Presents state, fault class, confidence, security status, and recommended action.

4.1 Multidomain Sensing

Table 2. Principal variables used by the cyber-physical monitoring framework

Domain	Measured / Derived Parameters
Fluid	Flow rate, pressure, temperature, valve position, estimated hydraulic power
Mechanical	Shaft speed, RMS vibration, torque, bearing or housing temperature
Electrical	Voltage, current, frequency, power factor, electrical input power
Cyber / Communication	Authentication state, timestamp consistency, command sequence, communication anomalies

5. Mathematical Representation and Cross-Domain Features

5.1 Fluid Model

For valve-controlled incompressible flow, a simplified relation can be expressed as:

$$Q = C_d A_v \sqrt{(2\Delta P / \rho)}$$

where Q is the flow, C_d is the discharge coefficient, A_v is the effective area of the valve, ΔP is the pressure difference, and ρ is the density of the fluid. For a centrifugal pump, the head rise can be approximated as a function of the speed of rotation and the flow:

$$H_p = a\omega^2 - bQ^2$$

5.2 Mechanical Model

Rotational dynamics are represented by:

$$J(dw/dt) = \tau_m - \tau_L - B\omega - \tau_f$$

where J is the rotational inertia, τ_m is the motor torque, τ_L is the load torque, B is the viscous friction, and τ_f is the additional torque that represents the fault. The vibration intensity is defined using the root-mean-square acceleration:

$$V_{RMS} = \sqrt{[(1/N) \sum (a_i^2)]}$$

5.3 Electrical Model

For a balanced three-phase system, electrical input power can be approximated as:

$$P_e = \sqrt{3} \cdot V \cdot I \cdot \cos\phi$$

Mechanical shaft power is:

$$P_m = \tau_m \cdot \omega$$

and the energy conversion efficiency is $\eta = P_m / P_e$. The relationships can be used to verify electrical quantities against mechanical loading and fluid demand.

5.4 Cross-Domain Residual Features

Rather than using the actual value of the sensor reading, the framework produces residuals, which are the disagreements between observed sensor reading and the reading that physically should have been observed.

$$r_Q = Q_{\text{measured}} - Q_{\text{hat}}(\omega, u_v, \Delta P)$$

$$r_I = I_{\text{measured}} - I_{\text{hat}}(\tau, \omega, V, \cos\phi)$$

$$r_E = P_e - P_m - P_h$$

These residuals can be especially valuable in distinguishing between equipment faults and sensor manipulations by an adversary. For instance an adversary could report a normal flow value whereas the shaft speed, valve state and pressure imply that such a flow value is physically impossible. A conventional threshold monitor may accept the value, but a cross-domain residual could pick up on the discrepancy.

6. Security Architecture

Security is implemented in the entire architecture instead of just the cloud level. The design is inspired by the distributed security concepts described in HeartFog and the IoT-fog framework of Pati et al. [1,4].

- Unique device identities and mutual authentication
- Encrypted sensor-to-gateway and gateway-to-fog communication
- Secure boot and digitally signed firmware
- Role-based access to control commands and configuration
- Network segmentation and command whitelisting
- Timestamp verification and replay-attack detection
- Tamper-evident event logging
- AI-assisted anomaly detection combined with physical consistency checks

A combined security-risk score can be constructed from AI-based attack probability, normalized physical residuals, and authentication or communication abnormalities:

$$S_t = \alpha P_{AI} + \beta Z(r_Q) + \gamma Z(r_I) + \delta Z(r_E) + \lambda A_t$$

7. Experimental Methodology

The data that was provided with the PDFs do not form a dataset of an integrated fluid-mechanical-electrical plant. Because of this, the empirical part of the current manuscript is based on a reproducible synthetic digital-twin dataset that was produced for the purposes of framework validation. The simulation was produced using a fixed random seed (42) to allow for repeatability. The values that resulted are not measurements taken from any of the provided studies.

7.1 Dataset Design

Table 3. Distribution of simulated operating states

Operating State	Samples
Normal	2,500
Fluid fault	2,000
Mechanical fault	2,000
Electrical fault	2,000
Cyber-attack	2,000
Total	10,500

The variables generated include the flow rate, pressure, fluid temperature, shaft speed, RMS vibration, torque, voltage, current, power factor, frequency, valve position, flow residual, current residual, and the cross-domain power balance. The measurement noise, variable load, and overlapping fault severity have been added to the data to prevent unrealistically perfect class separation. The data have been split into 70:30 stratified train/test, resulting in 7,350 and 3,150 samples, respectively.

7.2 AI Models and Evaluation Metrics

Four individual classifiers were considered, including Logistic Regression, Gradient Boosting, Random Forest, and radial-basis-function Support Vector Machine (SVM-RBF). A soft-voting ensemble learning technique was performed on the majority of the classifiers, whereby the weights were distributed as an increase for the SVM component due to its superior results during the validation set. Accuracy, weighted average of precision, recall, and F1-score were taken into consideration for final selection.

8. Results

8.1 Overall Model Performance

Table 4. Classification performance on the synthetic test set

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	80.89%	80.92%	80.89%	80.74%
Gradient Boosting	89.97%	90.09%	89.97%	89.90%
Random Forest	89.75%	89.81%	89.75%	89.67%
SVM-RBF	91.21%	91.46%	91.21%	91.11%
Soft Voting Ensemble	91.43%	91.59%	91.43%	91.37%

The nonlinear and ensemble models significantly outperformed Logistic Regression, thus proving that the combined fluid, mechanical, electrical, and cyber behaviors cannot be captured by a linear decision boundary. The final results of the proposed soft voting ensemble method reached an impressive accuracy of 91.43% and a remarkable weighted F1-score of 91.37%.

8.2 Class-Wise Ensemble Performance

Table 5. Class-wise performance of the soft-voting ensemble

Class	Precision	Recall	F1-Score	Support
Normal	82.70%	93.07%	87.58%	750
Fluid fault	91.39%	88.50%	89.92%	600
Mechanical fault	100.00%	99.50%	99.75%	600
Electrical fault	99.50%	99.17%	99.33%	600
Cyber-attack	86.60%	76.50%	81.24%	600

Mechanical and electrical failures achieved the best discrimination since vibration, torque, voltage, current, frequency, and power-factor patterns were relatively distinct. Cyber-attacks, in contrast, were more challenging to differentiate due to intentional similarity of spoofing cases to normal process excursions. Nevertheless, an overall F1-score of 81.24% was achieved for the cyber-attack class.

8.3 Effect of Cross-Domain Feature Engineering

An ablation experiment was carried out by stripping out the flow residual, current residual and power-balance features while keeping the other raw measurements. Without cross-domain consistency information, the ensemble accuracy was 89.08%. Restore residual features improved the ensemble accuracy by 2.35 percentage points to 91.43%, with cyber-attack recall increased from 69.50% to 76.50%, and F1-score from 75.20% to 81.24%. The experimental results verified the initial hypothesis, that is, physical relationships could provide an additional cybersecurity signal.

8.4 Feature Importance

Table 6. Leading Random Forest feature importances

Feature	Relative Importance
Vibration RMS	0.224
Flow residual	0.172
Current residual	0.121
Power factor	0.107
Voltage	0.057
Torque	0.053
Pressure	0.047
Fluid temperature	0.047
Flow rate	0.036
Frequency	0.034

Vibration RMS turned out to be the most prominent single feature, while the flow and current residuals were also significant. This is explained by the fact that the residuals characterize the interaction of different domains, and not individual characteristics, which confirms the importance of the cross-domain feature engineering.

9. Discussion

The results showed that the combined condition monitoring was more informative than the analyses of each subsystem. Mechanical vibrations were the most informative for identifying mechanical failures, while the electrical disturbances were best differentiated using voltage, current, frequency, and power factor. Pressure, flow, valve position, and shaft speed were critical in diagnosing fluid problems.

The obtained results support the general approach to machine learning described by the provided literature. Thus, Rath et al. [2] emphasize the importance of finding informative variables and selecting effective models that are capable of capturing all details of the process under study. Similarly, Swain et al. [3] discuss the possibility of simultaneous use of sensor data and machine learning algorithms. In turn, HeartFog study [1] demonstrates that real-time AI application with the Fog concept can be implemented and provides an opportunity to evaluate such algorithms from the perspective of multiple performance indicators, including accuracy, time, energy consumption, and so on.

A particularly desirable effect is the ability to distinguish cyber-attacks from legitimate operation after the introduction of physical residuals. Typically, a cybersecurity system would evaluate traffic characteristics, credentials, or particular events. However, the proposed solution provides an additional question: whether the information follows the physics of the equipment. This provides an additional level of security, even if the attacker was able to use a legitimate channel.

The use of fog computing is beneficial for this context due to the possibility of executing critical inferences close to the process. The work of Pati et al. [4] provides fog nodes, gateway devices, cloud components, and artificial intelligence inference, with latency, congestion, energy consumption, and cost considered in simulation. Such an architecture can be used to implement industrial systems in which it is necessary to perform fault recognition and safety actions without waiting for the processing of information received from the cloud.

10. Practical Implementation Scenario

A practical deployment may have the following structure: Sensors -> Secure Industrial Gateway -> Fog AI Node -> Physical-Consistency Engine -> Fault/Security Classifier -> PLC/Safety Controller -> Cloud Digital Twin. The fog device would perform the continuous inference while the cloud would be used for analytics, fleet-wide optimization, archival and periodic retraining of the AI models.

For instance, upon detecting a drop in pressure, the framework does not conclude that there is a fluid failure. It will also look at the shaft speed, valve command, motor torque, electrical current, vibration, flow rate, authentication, and the most recent control commands. If there is a decrease in pressure and flow rate but normal shaft speed and electrical loading, it may indicate a leakage-related fluid issue. On the other hand, if there is a decrease in the flow rate accompanied by increases in torque, current, and vibration, it may indicate a mechanical obstruction. At the same time, a discrepancy in the reported flow rate, pressure, and speed together with authentication or command irregularities suggests a cyber-physical attack.

11. Limitations

The current evaluation is a proof-of-concept study and cannot be used as an industrial field trial. The primary limitations are the use of synthetic data instead of real-world plant data, simplified hydraulic and electromechanical relationships, a limited number of cyber-attack classes considered, absence of hardware-in-the-loop testing, no direct comparison of different industrial communication standards including, for example, Modbus, OPC UA, PROFINET, or EtherNet/IP, and lack of a dataset for the degradation process over an extended period of time. Therefore, the numerical results should be considered as a proof of concept for the viability of the described framework and not as an indication of the performance level that can be expected in a particular industrial case.

12. Future Scope

Future research should be dedicated to the implementation of the proposed framework in a physical testbed comprising a motor-driven pump, pressure and flow rate sensors, vibration sensors, current and voltage sensors, a variable frequency drive, an industrial PLC, and an edge/fog computing node. In addition, the future works could investigate the possibility of using the transformer-based approach for multivariate time series modeling, LSTM/GRU-based prognosis for faults, interpretation of the models, federated learning from multiple plants, the digital-twin-enabled synchronized control and monitoring, adversarial AI robustness, zero-trust industrial network infrastructure, blockchain-based event certification, model-driven root cause analysis for the remaining useful life prognosis, and hardware-in-the-loop test for cyber attack simulation.

13. Conclusion

This research proposed a secure AI-based cyber-physical system that fuses fluid, mechanical, electrical, communication, and cybersecurity information rather than separately monitors them. The IoT sensors provide continuous system measurements, and the fog nodes execute local data preprocessing, AI models, and rapid anomaly detection. Cross-domain physical residuals present another approach for examining whether sensor measurements are consistent with the energy and process relationships.

The reproducible synthetic digital-twin experiment composed of 10,500 measurements demonstrated that the developed soft-voting ensemble attained 91.43% accuracy and 91.37% weighted F1-score on normal operations, fluid faults, mechanical faults, electrical faults, and cyber-attacks. The utilization of cross-domain residual features enhanced the overall accuracy by 2.35% and the recall of detecting cyber-attacks from 69.50% to 76.50%.

The findings reveal that next-generation industrial monitoring systems should treat the artificial intelligence, cybersecurity, fluid mechanics, mechanical behavior, and electrical state as a unified entity rather than separate areas of technology. It is the only way to enable fault diagnosis, attack detection, predictive maintenance, operational resilience, and safe intelligent control.

References

1. Pati, A., Parhi, M., & Pattanayak, B. K. (2022). HeartFog: Fog Computing Enabled Ensemble Deep Learning Framework for Automatic Heart Disease Diagnosis. In *Intelligent and Cloud Computing, Smart Innovation, Systems and Technologies*, Vol. 286. Springer Nature Singapore. https://doi.org/10.1007/978-981-16-9873-6_4
2. Rath, S., Das, N. R., & Pattanayak, B. K. (2024). An Analytic Review on Stock Market Price Prediction using Machine Learning and Deep Learning Techniques. *Recent Patents on Engineering*, 18, e030323214351. <https://doi.org/10.2174/1872212118666230303154251>
3. Swain, S., Pattnayak, B. K., Mohanty, M. N., Jayasingh, S. K., Patra, K. J., & Panda, C. (2024). Smart livestock management: integrating IoT for cattle health diagnosis and disease prediction through machine learning. *Indonesian Journal of Electrical Engineering and Computer Science*, 34(2), 1192-1203. <https://doi.org/10.11591/ijeecs.v34.i2.pp1192-1203>
4. Pati, A., Parhi, M., Pattanayak, B. K., Singh, D., Singh, V., Kadry, S., Nam, Y., & Kang, B.-G. (2023). Breast Cancer Diagnosis Based on IoT and Deep Transfer Learning Enabled by Fog Computing. *Diagnostics*, 13, 2191. <https://doi.org/10.3390/diagnostics13132191>