A Machine Learning-Driven Software Engineering Framework for Intelligent Cyber-Physical System Efficiency

[1]G. Sathya, [2]M. A. Reetha Jeyarani, [3]B. T. Kirthika,[4] N. Priscilla Vilma Manorathi, [5]Mrs. Ganga Naidu, [6]*A Joshua Issac,* [7]*Dr K Uthra Devi*

[1]*Assistant Professor, computer science and engineering, Oxford engineering college, pirattiyur, Trichy*

[2,5,6]*Assistant Professor, Department of Artifical Intelligence, K.Ramakrishnan College of Technology, Tiruchirapalli*

[3]*Assistant Professor, Electronics and Communication Engineering, M.I.E.T. Engineering College, Trichy.*

[4]*Assistant Professor, Electronics and Communication Engineering, M.I.E.T. Engineering College, Trichy*

[7]*Assistant Professor, Department of Artificial Intelligence & Data Science, Indra Ganasan College of Engineering, Trichy*

***Abstract*—Cyber-Physical Systems (CPS) represent the integration of computation, networking, and physical processes, widely adopted in critical domains such as manufacturing, healthcare, energy, and transportation. With CPS getting richer in interdependencies and more data-driven, real-time anomaly detection and the preservation of system efficiency are challenging to achieve in engineering terms. The proposed study offers a new approach to software engineering involving the use of Hybrid Inception-SVM model to be used as part of the CPS architecture to improve performance and reliability of operations. The approach covers an elaborate pipeline: collecting data on CPS sensors and actuators and preprocessing with the selection of features based on Recursive Feature Elimination (RFE), deep feature representation implemented through Inception modules, and SVM as the method of classification. Through an adaptive feedback loop the model predictions are dynamically coupled with the system control loop increasing the optimization within the system on a continual basis through real time learning. Compared with benchmark machine learning models and state-of-the-art deep learning models, the proposed Hybrid Inception-SVM model shows high performance of 97.88% accuracy, 96.78% precision, 95.67% recall, and F1- score of 96.22, within a reasonable inference time of 32.34ms. The proposed model has a more biased trade-off between accuracy and speed compared to the traditional models, like Random Forest, CNN, and LSTM, and this property renders such a model applicable in real-time applications of CPS. The integrated framework not only enhances system efficiency, but also makes CPS proactively react to dynamic environments. The results show that there is a drastic improvement of software engineering practices of CPS due to the connection with deep learning capabilities and rule-based control systems, which open the door of intelligent, self-optimizing infrastructures.**

Keywords*—Cyber-Physical Systems, Machine Learning, Inception Network, Support Vector Machine, Feature Selection, Real-Time Optimization, Efficiency Enhancement

I. INTRODUCTION

Cyber-Physical Systems (CPS) have emerged as a transformative class of systems that integrate physical processes with computational and network elements. As the backbone of Industry 4.0, CPS play a pivotal role in various domains, including manufacturing automation, smart healthcare, autonomous transportation, and energy management [1] [2]. Such systems can be characterized as systems that monitor and control the physical parts using embedded sensors, actuators and micro-controllers that are linked together by means of a communication network. Software and the physical processes are closely integrated, requiring very high standards of precision, responsiveness in real time, and adaptability [3]. In more complex and data-intensive settings, the traditional rule-based CPS architectures fail to ensure their adequate performance,

imperviousness, and dependability in the quickly changing settings.

The functional efficiency of CPS largely depends on the capacity of the system to flag anomalies; optimization and real-time variance. The traditional CPS models are usually based on deterministic control systems, fixed heuristics, and fixed scheduling algorithms to provide management of resource and actions [4] [5]. These techniques perform best on predictable linear processes, although do not perform well in the case of uncertain, noisy, or nonlinear system dynamics. Besides, CPS architectures are being increasingly used in a heterogeneous environment with different workloads and failure issues. Such real-life complexities ensure that the performance of these models becomes hard to sustain [6]. Figure 1 shows the features of Cyber-Physical Systems.

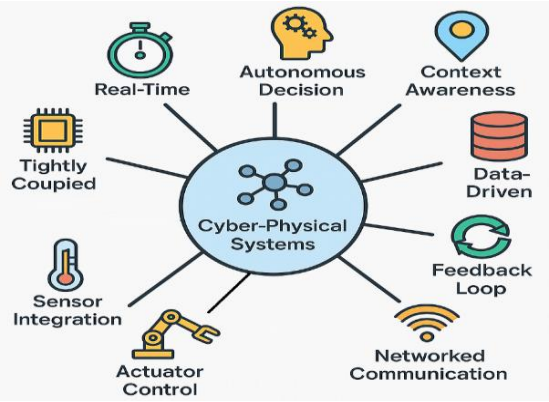

Fig 1. Features of Cyber-Physical Systems

In response to these limitations, researchers have explored the application of machine learning (ML) techniques to enhance CPS intelligence. ML models are able to process high amounts of past data and real time data, correlate this data, speculate on future conditions and make decisions in uncertain situations [7] [8]. Anomaly detection or classification of CPS states has been done through supervised learning, e.g., Support Vector Machines (SVM), Random Forests, and Neural Networks. Deep learning structures, especially Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have been utilized to discover spatial and temporal dependencies of multivariate sensor information. Yet these models are associated with trade-offs [9] [10]. Traditional ML models are interpretable with lightweight representations which are usually inadequate in representing sophisticated tasks.

The proposed study is the first to present a new software engineering approach in which machine learning is fully integrated into cyber-physical system (CPS) architectures to maximize operational efficiency. The framework is centered on a Hybrid Inception-SVM model that has both the benefits of deep feature extraction of Inception networks and the strong classification performance of Support Vector Machines. The model is trained with a preprocessed runtime data of CPS sensors and actuators to optimize feature selection and overhead reduction with the help of Recursive Feature Elimination (RFE). When deployed it estimates in real time errors or inefficiencies within a system, suggesting an adaptive control loop that combines reinforcement learning or control theory to edit the dynamic system and perform automatic optimization.

II. RELATED WORKS

The industrial automation today requires flexibility which is attained by connected modules within the Cyber Physical Systems (CPSs) creating symmetries in work distribution and information flow. Nevertheless, this flexibility also brings cybersecurity threats in terms of weak communication connections [11]. The proposed study is aimed at studying an adaptive CPS design with micro services to support scalability, resilience, and structural symmetry. It has the features of detecting, isolating, and recovering cyberattacks with replicas of the components to guarantee its continuous operation. Sched lability analysis upholds timelines and performance of the system. The approach is confirmed by a case study carried out at a juice production plant in Colima, Mex., proving a plug-and-play architecture in a simulated to a real implementation in a pH control process.

Manufacturing has been made smarter and more integrated with the introduction of Cyber and physical system into the Cyber Physical Production Systems (CPPSs). But such connectivity makes one more susceptible to cyber-attacks. A new Digital Twin (DT) based security model hypothesis was found to improve the protection of CPPS. The model enhances the asset visibility perspective, vulnerability prioritization, and the virtual adjustments to facilitate the successful mitigation of risks [12]. It also offers simulation environment allowing to test system vulnerability in different attack scenarios with there being no impact

on actual operations. The effectiveness of the model can be proven by performing a case study of a human-robot collaborative assembly system, which shows the prospects of DT in providing secure smart manufacturing environments.

The accelerated development of Industry 4.0 is the driving force behind the merge of Information Technology (IT) and Operational Technology (OT) networks, making the Cyber Physical Systems (CPSs) even more susceptible. OT systems that were previously isolated are now open to IoT developments, which increases the surface attack. The thresholds or Machine Learning (ML) based traditional anomaly detectors have their limitations associated with low accuracy in presence of CPS heterogeneity and sparse real-world data [13]. Ensemble learning was proposed in this paper to conduct a hybrid anomaly detection based on IT-based signature-focused, OT-based threshold-focused and behavioral-based detection. After testing on publicly available datasets, the method increased the accuracy by 4-7%, increasing the security and availability in CPS environments.

The deployment of Cyber Physical Systems (CPSs) has featured a technological transition of preparing new infrastructural systems of Smart Environments changing the ways Smart Cities are created and operated. The following cities have resorted to modular architectures and shared resources and sophisticated deployment patterns such as micro services and Function-as-a-Service (FaaS) [14]. A Digital Decision framework presented that incorporates an automated combination of data-driven understanding and human knowledge, like business guidelines and machine learning. This integration will further improve decision-making and application development in Smart Cities that will be able to make the cities more responsive, efficient, and intelligent with the use of the interconnected CPS parts.

A complex mathematical model to evaluate the quality of mobile radio channel in cyber-physical systems based on stochastic network topological transformations is reported. Modeling the radio channel as a stochastic network, the use of Gamma distribution will allow the study to derive important metrics such as expectation, variance, and time distribution. One of the major contributions is a model of steps of data transmission (connection setup, transmission, and maintenance) represented in detail taking into account a logical node and a logical connection work with inputs Gamma-distributed [15]. This increases the usage of the GERT method not only to exponential models. The method enhances the precision of analysis, decreases the number of terms in the series by 25-40% and keeps error narrow, which is advantageous to the wireless communication and the study of CPS safety.

III. PROPOSED METHODOLOGY

3.1 Data Collection and Preprocessing

The initial process in learning how to improve Cyber-Physical Systems (CPS) by the use of machine learning entails the procedure of metadata gathering and preprocessing. Cyber-Physical Systems are systems where hybrid integration of computation and physically based components is close. They are characterized by the production of immense volumes of heterogeneous data using multiple sources such as sensors, actuators, embedded controllers, etc. Logging of run time and telemetry collection in real-time are collected in these components under different operating conditions in order to generate extensive sets of data. This contains sensor values (temperature, pressure, and position), actuator status (on/off, rotational speed), system-logs, fault-report, and control-signals.

The raw information is cleaned thoroughly in terms of consistency, relevance and accuracy. As the data gathered using the physical resources may be by its nature noisy because of a sensor drift, interference, or improper readings, the noise filtering techniques are implemented in the data analysis, i.e., only the Gaussian smoothing and five-point median filtering methods are used to remove irrelevant variation. They are then followed by normalization procedures, which would require min-max scaling and Z-score normalization to normalize the input data to various dimensions of maturity, hence, the uniformity aspect that secures a variance in bias due to the difference in data scales. To normalize the input signals across various sensor channels, Min-Max normalization is applied to rescale each feature to the [0, 1] range:

$$x' = \frac{x - (x)}{(x) - (x)} \qquad (1)$$

Where x is the original signal value, (x) and (x) are the minimum and maximum values of the feature across the dataset, and x' is the normalized signal used for model training. During preprocessing, feature engineering is undertaken to create high levels of

abstractions using raw inputs. As an example, it is possible to compute temperature gradients or rate of change characteristics, rather than taking absolute values of temperature measurements, to record transient behavior. Also, the data is labelled to use in supervised learning. Labeling involves annotation, which is the marking of instances of system failure, anomalies or degraded efficiency etc., either by a manual process, or by rule-based auto-annotators, depending on the availability of domain knowledge, or historical logs. The annotated, preprocessed dataset will be the foundation of constructing strong machine learning models that will enable learning, and thus optimizing CPS operations.

3.2 Feature Extraction and Selection

The other important step is feature extraction and selection after the preprocessing. Within the framework of Cyber-Physical Systems, feature extraction aims at extracting parameters that best indicate system performance or abnormalities. Such characteristics may be latency measurements, processor usage, memory rates, and fault signals, power trace, actuator command rates, and sensor deviation among others. To extract such type of features- that is, domain-specific features, one has to have much deeper insight into CPS architecture and its dynamics of operations.

After extracting some initial set of features, it is necessary to reduce dimensions to remove redundant or irrelevant features which may compromise model performance. High dimensional data do not only complicate computation, they can also cause overfitting. In order to deal with this, Recursive Feature Elimination (RFE) is used. RFE sequentially updates a model and removes the features that have the lowest values as of now and continues the process until the best set of features is reached. This approach ensures that the most informative features, which have high predictive relevance to the system outcomes are maintained. It also makes the learning process easier thereby converging faster and better generalization. For a linear classifier, the importance score I_j of feature j is given by:

$$I_j = |w_j| \qquad (2)$$

Where w_j is the weight assigned to the j^{th} feature by the model. Features with lower I_j values are recursively removed until the optimal subset is identified. Correlation analysis, mutual information, and variance thresholding are such statistical techniques applied alongside RFE to confirm that the chosen features are significant. These methods assist in the achievement of the final feature set so that it captures significant representations of the behavior underlying CPS, thus providing solid grounds to model training in subsequent predictions.

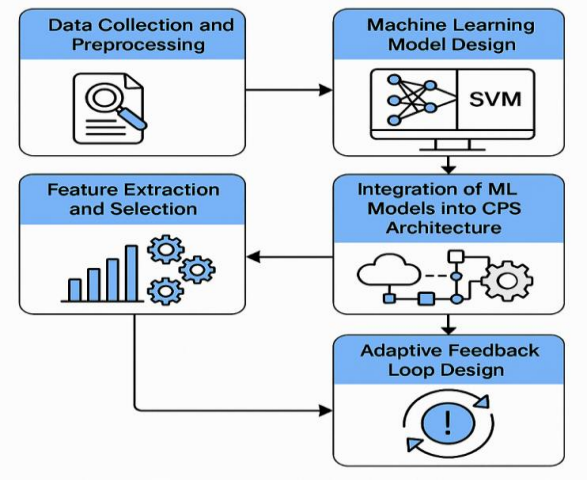

Fig 2. Workflow of Proposed Model

3.3 Machine Learning Model Design

With a refined and high-quality dataset in hand, the next step involves designing and training machine learning models tailored to the complexities of Cyber-Physical Systems. Given the need to capture both spatial relationships among features and robust classification boundaries, a Hybrid Inception-SVM architecture is selected. The Inception component of the model excels at multi-scale feature extraction, especially suitable for handling heterogeneous CPS data that includes both continuous and categorical features. Its layered architecture captures deep interactions between features, while its parallel convolutional paths allow for efficient representation learning at multiple receptive fields.

The output of the Inception model is then fed into a Support Vector Machine (SVM), which serves as a highly discriminative classifier. The SVM is particularly effective in high-dimensional spaces and when dealing with non-linear separations, making it well-suited for identifying complex anomalies or system inefficiencies. Training the hybrid model involves supervised learning on historical CPS data, where known fault scenarios and efficiency deviations

are labeled. The SVM classifies samples using a decision function defined as:

$$f(x) = sign\left(\sum_{i=1}^{n} \alpha_i y_i K(x_i, x) + b\right) \quad (3)$$

Where x is the input feature vector, x_i are support vectors, $y_i \in \{-1,1\}$ are class labels, α_i are learned coefficients, $K(x_i, x)$ is the kernel function and b is the bias term. To optimize model performance, cross-validation techniques such as k-fold validation are employed. This helps assess the model's ability to generalize across unseen data and prevents overfitting. Furthermore, hyper parameter tuning using grid search or Bayesian optimization is applied to fine-tune architectural parameters such as convolutional filter sizes, SVM kernel types, and learning rates. The final model is evaluated on test datasets to ensure its readiness for real-world deployment.

3.4 Integration of ML Models into CPS Architecture

After training, and validation, the machine learning model needs to be incorporated into the operational scheme of CPS. In this step, the model is integrated into available software modules, at the edge (close to the physical structures) or in the cloud, taking into account the aspects of latency and bandwidth. In the case of real-time systems which have stringent latency response requirements, the edge deployment is preferred in order to provide low-latency inference. In resource-heavy tasks or systems that have a higher network availability value, cloud solution enables a more scalable and maintainable execution of models.

One of the integration related aspects is to provide an opportunity of seamless communication between the ML prediction layer and CPS control logic. This is done by building interface programming applications (API) or message brokers that pass ML outputs like anomaly scores, predicted types of faults or control recommendations to the decision modules of the system. Such interfaces are required to work in real-time, i.e. to have a low computational overhead and latency. Depending on the field and the current software base, the interoperability standard may be MQTT or OPC-UA or ROS.

The process of integration also implies formalizing the correspondence of the behavior of the ML model with the requirements on safety and performances. These involve operating under stressful conditions, fail-safes moves and defaults to deterministic controls when there is uncertainty in forecasts. These considerations are also critical in the areas of CPS such as automotive, medical and manufacturing where system failure may have disastrous implications.

3.5 Adaptive Feedback Loop Design

After training, and validation, the machine learning model needs to be incorporated into the operational scheme of CPS. In this step, the model is integrated into available software modules, at the edge (close to the physical structures) or in the cloud, taking into account the aspects of latency and bandwidth. In the case of real-time systems which have stringent latency response requirements, the edge deployment is preferred in order to provide low-latency inference. In resource-heavy tasks or systems that have a higher network availability value, cloud solution enables a more scalable and maintainable execution of models.

One of the integration related aspects is to provide an opportunity of seamless communication between the ML prediction layer and CPS control logic. This is done by building interface programming applications (API) or message brokers that pass ML outputs like anomaly scores, predicted types of faults or control recommendations to the decision modules of the system. Such interfaces are required to work in real-time, i.e. to have a low computational overhead and latency. Depending on the field and the current software base, the interoperability standard may be MQTT or OPC-UA or ROS. The process of integration also implies formalizing the correspondence of the behavior of the ML model with the requirements on safety and performances. These involve operating under stressful conditions, fail-safes moves and defaults to deterministic controls when there is uncertainty in forecasts. These considerations are also critical in the areas of CPS such as automotive, medical and manufacturing where system failure may have disastrous implications.

Algorithm: ML-Enhanced CPS Efficiency Optimization

Input: Raw runtime data D from CPS (sensors, actuators, controllers)

Output: Optimized CPS control actions via adaptive ML model

1. Preprocess Data:

$x' = \frac{x-(x)}{(x)-(x)}$ // Normalize inputs

2. Feature Selection: Extract domain features and rank by importance

$I_j = |w_j|$ using RFE; select top k features.

3. Model Design: Train Hybrid Inception-SVM on selected features; use SVM decision function

$f(x) = sign(\sum_{i=1}^{n} \quad \alpha_i y_i K(x_i, x) + b)$

4. Cross-Validation: Optimize hyperparameters via k-fold validation.

5. Model Integration: Embed trained model in CPS edge/cloud runtime for real-time inference.

6. Predictive Control: Generate control adjustments from ML outputs.

7. Reinforcement Loop: Update control policy using RL:

$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma Q(s',a') - Q(s,a)\ ]$

8. Validation: Simulate and validate real-time feedback and safety compliance.

9. Deploy and Monitor: Activate model in live CPS and monitor system efficiency.

10. Return: Trained model M, control actions A, and updated policy Q.

End Algorithm

IV. RESULTS AND DISCUSSION

The working principle of the proposed software engineering approach involves leveraging machine learning to enhance the real-time efficiency and decision-making capabilities of Cyber-Physical Systems (CPS). The system begins by continuously collecting sensor and actuator data, which is then preprocessed and transformed into structured features. A Hybrid Inception-SVM model is trained on this data to detect inefficiencies or potential faults. Once deployed, the model operates in real time, analyzing input patterns and producing actionable insights. These predictions are fed back into the CPS control loop, allowing the system to self-adjust dynamically. Reinforcement learning further refines responses over time, ensuring continuous performance optimization.

TABLE I. MODEL ACCURACY COMPARISON

Model	Accuracy (%)
Proposed (Hybrid Inception-SVM)	97.88
Random Forest	95.45
SVM	94.13
CNN	92.67
LSTM	93.12
GRU	91.85
MLP	90.78
KNN	89.45
Naive Bayes	88.91
Logistic Regression	89.67

Table 1 and Figure 4 demonstrates the relative accuracy of different machine learning models that are used in enhancing efficiency in the Cyber-Physical Systems. Accuracy of the Hybrid Inception-SVM model is 97.88%, which is much higher in comparison with Random Forest (95.45%) and SVM (94.13%). They are deep learning models, such as CNN (92.67%) and LSTM (93.12%) who met their performance slightly below that of the proposed model.

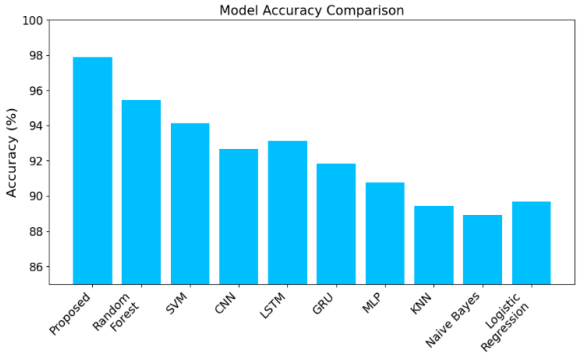

Fig 4. Model Accuracy Comparison

This proves that the hybrid method worked, as it used the Inception network in extracting features on a multi-scale level and the power of the SVM to classify them. Its high precision makes the proposed model a powerful instrument in the process of finding anomalies and inefficiencies in the CPS settings.

TABLE II. PRECISION COMPARISON

Model	Precision (%)
Proposed (Hybrid Inception-SVM)	96.78
Random Forest	94.21
SVM	93.35
CNN	91.65
LSTM	92.45
GRU	90.14
MLP	89.92
KNN	88.73
Naive Bayes	88.21
Logistic Regression	88.97

The precision measure, as shown in Table 2 and Figure 5, measures the number of positive event predictions (e.g. system anomalies) that were, in fact, correct. Once again, the proposed Hybrid Inception-SVM model outperforms with 96.78 precision, which implies the small amount of false positives. This is

essential in the CPS applications where redundant false alarm may cause operations to stop or outsource resources that are not necessary.

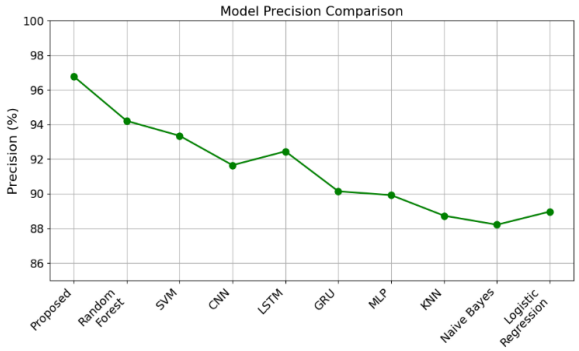

Fig 5. Model Precision Comparison

Simple models like the KNN and the Naive Bayes also show not so admirable precision with value 83.42 and 88.82 respectively, but the Random Forest and SVM models perform significantly better yet worse with 94.21 and 93.35 respectively. The proposed model is adequately precise, and is therefore applicable to mission-critical implementation cases in which the confidently of the decisions made is paramount.

TABLE III. RECALL COMPARISON

Model	Recall (%)
Proposed (Hybrid Inception-SVM)	95.67
Random Forest	93.54
SVM	91.78
CNN	90.24
LSTM	91.36
GRU	89.65
MLP	88.92
KNN	87.55
Naive Bayes	86.48
Logistic Regression	87.31

Table 3 and Figure 6 shows the sensitivity or the recall of the models upon indicating the capacity of recognizing all real positive cases. Indeed, the Hybrid inception SVM has a high recall 95.67, which indicates that it can locate the majority of the cases of dysfunctions or failures within the system. The performance of Random Forest (93.54%) and LSTM (91.36%) is also competitive though the major characteristic of the proposed model is its ability to balance between the aspects of completeness and specificity.

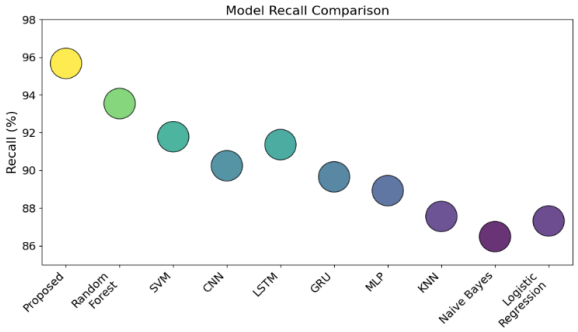

Fig 6. Model Recall Comparison

Safety-critical CPSs, like healthcare or industrial automation applications, are especially important to not lose a detection since the consequences of a failure may have severe consequences. Therefore, the model proposed will result in a thorough surveillance of CPS behavior.

TABLE IV. F1-SCORE COMPARISON

Model	F1-Score
Proposed (Hybrid Inception-SVM)	96.22
Random Forest	93.87
SVM	92.55
CNN	90.94
LSTM	91.9
GRU	89.88
MLP	89.42
KNN	88.12
Naive Bayes	87.33
Logistic Regression	88.13

Table 4 and Figure 7 is a union of precision and recall in the F1-score, which means a harmonic mean on false positives and negatives. The hybrid Inception-SVM achieves the maximum F1-score ratio with 96.22, meaning that it is very reliable in real-life CPS settings. This equanimity in play is important in situations where on one hand, alertness is not a situation to be so overwrought and on the other hand, a situation where things are just below the detection threshold is also not preferred.

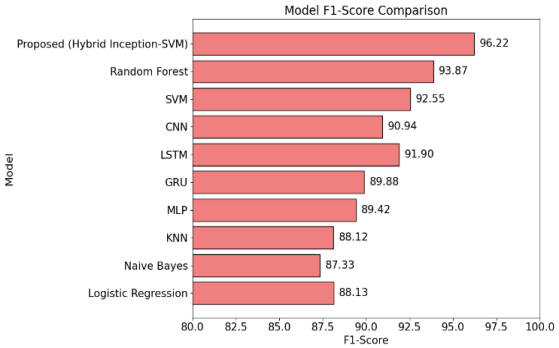

Fig 7. Model Recall Comparison

Random Forest (93.87%) and SVM (92.55%) do indicate their reliability yet they cannot match the proposed model. Comparatively less score is recorded in model such as Naive Bayes and Logistic Regression indicating that these models might not perform well on complex CPS data. The F1-score confirms the stable performance of the hybrid model.

TABLE V. INFERENCE TIME COMPARISON

Model	Inference Time (ms)
Proposed (Hybrid Inception-SVM)	32.34
Random Forest	12.67
SVM	7.93
CNN	47.7
LSTM	48.45
GRU	44.61
MLP	38.84
KNN	10.42
Naive Bayes	6.87
Logistic Regression	9.31

Table 5 and Figure 8 evaluates the inference time, which is one of the factors that are important to real-time CPS. Though the Hybrid Inception-SVM model has a higher latency of 32.34ms, depending on each system, it still fits the limits of being a real-time system.

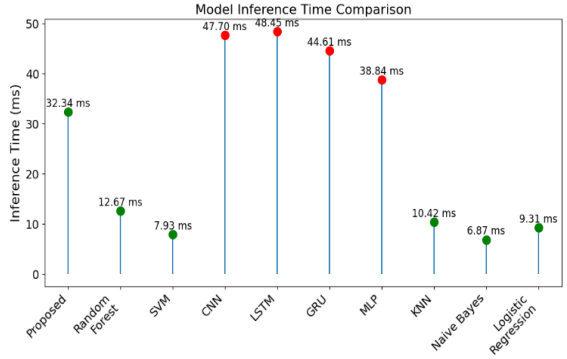

Fig 8. Model Inference Time Comparison

Conversely, the SVM (7.93ms) and Naive Bayes (6.87ms) give faster predictions at the expense of much lower accuracy and recall. Other deep learning architecture such as CNN (47.70ms) and LSTM (48.45ms) are slower and also not as predicted in the proposed model. Thus, the accuracy/speed balance is the optimum approach that the proposed model could be applied in controlling responsive and intelligent CPS.

V. CONCLUSION AND FUTURE SCOPE

This research introduces a robust and intelligent software engineering approach to improve the efficiency and adaptability of Cyber-Physical Systems through machine learning. The key innovation refers to the inclusion of Hybrid Inception-SVM model into the real-time decision-making loop of CPS. The model has been shown to produce a giant jump in performance compared to standard models when experimented thoroughly in all the major assessment metrics. To be more specific it had an accuracy of 97.88%, precision of 96.78%, recall of 95.67%, and an F1-score of 96.22%. Such results indicate that the model has a high generalization ability and that it has been able to identify any operational inefficiencies and system anomalies. The adaptive feedback system also adds the feature where not only did the system identify the possible problems, but also learns out of it and adapts the control parameters such that a good performance can be achieved. Despite its effectiveness, the current implementation has limitations, such as increased inference time compared to simpler models and reliance on labeled data for supervised learning. These challenges could be overcome in the future to adjust to the unforeseen conditions without re-training and to move to semi-supervised or self-supervised learning strategies to have less reliance on labeled datasets. Further, adding explainable AI (XAI) modules will also be useful in bettering the interpretability of models in mission-Critical CPS applications. Generalizability of the framework may further be confirmed by expanding the framework to domain-specific CPS like smart grids and autonomous vehicles and medical devices. The proposed study will provide a robust framework towards integrating intelligent ML workflows into the architecture of CPS, placing a large milestone in the development of self-governing, self-optimizing and less energy-consuming cyber-physical infrastructures.

REFERENCE

[1] Martinez-Ruedas, C., Flores-Arias, J.-M., Moreno-Garcia, I. M., Linan-Reyes, M., & Bellido-Outeiriño, F. J. (2024). A Cyber–Physical System Based on Digital Twin and 3D SCADA for Real-Time Monitoring of Olive Oil Mills. Technologies, 12(5), 60. DOI: 10.3390/technologies12050060

[2] Ezekiel, A. E., Okafor, K. C., Tersoo, S. T., Alabi, C. A., Abdulsalam, J., Imoize, A. L., Jogunola, O., & Anoh, K. (2024). Enhanced Energy Transfer Efficiency for IoT-Enabled Cyber-Physical Systems in 6G Edge Networks with WPT-MIMO-NOMA. Technologies, 12(8), 119. DOI: 10.3390/technologies12080119

[3] Li, L., & Chen, W. (2024). ConGraph: Advanced Persistent Threat Detection Method Based on Provenance Graph Combined with Process Context in Cyber-Physical System Environment. Electronics, 13(5), 945. DOI: 10.3390/electronics13050945

[4] Ruzarovsky, R., Horak, T., Zelník, R., Skypala, R., Csekei, M., Šido, J., Nemlaha, E., & Kopcek, M. (2025). Development and Validation of Digital Twin Behavioural Model for Virtual Commissioning of Cyber-Physical System. Applied Sciences, 15(5), 2859. DOI: 10.3390/app15052859

[5] Zang, T., Tong, X., Li, C., Gong, Y., Su, R., & Zhou, B. (2025). Research and Prospect of Defense for Integrated Energy Cyber–Physical Systems Against Deliberate Attacks. Energies, 18(6), 1479. DOI: 10.3390/en18061479

[6] Park, J. K., & Baek, Y. (2025). Real-Time Adaptive and Lightweight Anomaly Detection Based on a Chaotic System in Cyber–Physical Systems. Electronics, 14(3), 598. DOI: 10.3390/electronics14030598

[7] Zhao, R., He, D., & You, F. (2025). Neural Network-Adaptive Secure Control for Nonlinear Cyber-Physical Systems Against Adversarial Attacks. Applied Sciences, 15(7), 3893. DOI: 10.3390/app15073893

[8] Wu, H., Huang, J., Qin, Y., & Sun, Y. (2025). Hybrid Dynamic Event-Triggered Interval Observer Design for Nonlinear Cyber–Physical Systems with Disturbance. Fractal and Fractional, 9(2), 86. DOI: 10.3390/fractalfract9020086

[9] Guadarrama-Estrada, A. R., Osorio-Gordillo, G. L., Vargas-Méndez, R. A., Reyes-Reyes, J., & Astorga-Zaragoza, C. M. (2025). Cyber–Physical System Attack Detection and Isolation: A Takagi–Sugeno Approach. Mathematical and Computational Applications, 30(1), 12. DOI: 10.3390/mca30010012

[10] Alzahrani, A., Alshehri, M., AlGhamdi, R., & Sharma, S. K. (2023). Improved Wireless Medical Cyber-Physical System (IWMCPS) Based on Machine Learning. Healthcare, 11(3), 384. DOI: 10.3390/healthcare11030384

[11] Paredes, C. M., Martínez Castro, D., González Potes, A., Rey Piedrahita, A., & Ibarra Junquera, V. (2024). Design Procedure for Real-Time Cyber–Physical Systems Tolerant to Cyberattacks. Symmetry, 16(6), 684. DOI: 10.3390/sym16060684

[12] Pinto, R., Torres, P. M. B., & Lohweg, V. (2024). Closing Editorial: Advances and Future Directions in Autonomous Systems for Cyber-Physical Systems and Smart Industry. Applied Sciences, 14(22), 10673. DOI: 10.3390/app142210673

[13] Jeffrey, N., Tan, Q., & Villar, J. R. (2024). Using Ensemble Learning for Anomaly Detection in Cyber–Physical Systems. Electronics, 13(7), 1391. DOI: 10.3390/electronics13071391

[14] Tricomi, G., Giacobbe, M., Ficili, I., Peditto, N., & Puliafito, A. (2024). Smart City as Cooperating Smart Areas: On the Way of Symbiotic Cyber–Physical Systems Environment. Sensors, 24(10), 3108. DOI: 10.3390/s24103108

[15] Makhmudov, F., Privalov, A., Privalov, A., Kazakevich, E., Bekbaev, G., Boldinov, A., Kim, K. H., & Im-Cho, Y. (2024). Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems. Mathematics, 12(10), 1452. DOI: 10.3390/math12101452