A Hybrid Framework for Detecting and Mitigating Cyber-Attacks in Industrial Control Systems Through Physical Process Monitoring

Jansher Ali Chang, Muhammad Saleem Vighio
Quaid-e-Awam university of engineering science and technology Nawabshah
*Correspondence: jansherchang@gmail.com, saleem.vighio@quest.edu.pk

Citation | Chang. J. A, Vighio. M. S, "A Hybrid Framework for Detecting and Mitigating Cyber-Attacks in Industrial Control Systems Through Physical Process Monitoring", IJIST, Vol. 7 Issue. 10 pp 134-143, December 2025
Received| November 09, 2025 **Revised|** December 01, 2025 **Accepted|** December 06, 2025 **Published|** December 09 2025.

The efficiency of Industrial Control Systems (ICS) has been threatened by the increasing complexity of cyber-physical attacks owing to the convergence of Information Technology (IT) and Operational Technology (OT). The intrusion detection systems designed to address this issue focus on network monitoring. However, these systems were not entirely reliable in identifying complex attacks, such as those employing cyber-physical means to control physical processes concurrently with normal communications. To address this deficiency, the research paper proposes a comprehensive hybrid solution to detect and mitigate cyber-physical attacks simultaneously. This research combines both cyber-network and physical process monitoring. The solution employs a Random Forest classifier to detect cyber-physical attacks and an LSTM-based time series model to detect anomalies in multivariate sensor and actuator data of physical processes. The outputs of both detection models are optimized through a decision fusion approach. The detection framework also incorporates an automated response mechanism that isolates malicious units, generates alerts, and initializes safe operation modes during detected attacks. Additionally, to enhance the efficiency of the solution, an adaptive learning component has been incorporated to optimize detection and responses based on feedback derived from previous attacks and mitigation actions. The solution has been evaluated using the BATADAL dataset to demonstrate its effectiveness in terms of accuracy, reduction in false positives, and real-time cybersecurity performance for safeguarding ICS. This research applies a comprehensive hybrid approach aligned with real-world ICS, addressing identified challenges in current cyber-physical threats to provide effective protection for ICS.

Keywords: Industrial Control Systems (ICS), Cyber–Physical Security, Hybrid Intrusion Detection, Random Forest–LSTM Framework, Anomaly Detection

Introduction:

Industrial Control Systems (ICS) comprise the pillar of critical infrastructure technology, enabling the monitoring and control of physical processes in various industries including power generation, water processing, oil and gas production, manufacturing, and transportation. ICS integrates hardware system components, software applications, and communication networks with a focus on the continuous automation of physical processes within industry. ICS encompasses Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs) in a manner that facilitates real-time sensing, decision-making, and actuation on physical processes. In contrast to standard information technology systems, ICS systems are expected to operate in real-time environments where high availability, reliability, and safety are critical considerations. Consequently, failures in these systems can result in severe economic losses, environmental damage, or loss of human life due to emergent threats [1][2].

ICS architecture development has also been influenced by the merging of Information Technology (IT) and Operational Technology (OT). Historically, industrial control systems relied on custom-made hardware and communication protocols. Such an architecture limited access by external personnel and devices thereby reducing the vulnerability of control systems to cyber-attacks. The increasing demand for efficiency and operational productivity in industrial environments has driven greater convergence between ICS and enterprise IT networks and even cloud computing. Although this convergence has enabled enhanced operational transparency and productivity, it has also increased the vulnerability of industrial control systems to potential threats from outsiders, insiders, and state actors [3][4]. Additionally, due to their continuous 24/7 operation ICS cannot undergo frequent updating as is typical in conventional IT-based systems and therefore do not allow the application of conventional IT security measures such as software updates and antivirus protection.

The cyber-attacks on ICSs are distinct from attacks on general computer systems, as they can be designed not only to breach confidentiality but also to undermine various physical processes. Many types of cyber-attacks, such as malware, unauthenticated access, denial of service, and man-in-the-middle attacks, can target the controllers' communications with field components. Importantly, recent incidents have demonstrated that cyber-attacks on ICSs can have physical consequences, including equipment damage, production stoppages, or causing accidents. These cyber-attacks can operate covertly, allowing normal network traffic while subtly manipulating the controllers. Consequently, network-based IDSs, which rely **solely on** traffic characteristics, are incapable of detecting sophisticated cyber-physical attacks where both the cyber domain and the physical domain are manipulated [5][6].

Physical process monitoring is critical for ensuring safe and reliable ICS operation, as it involves continuous observation of variables such as temperature, pressure, flow rate, voltage, and chemical concentration. This is enabled by sensors and actuators strategically placed throughout industrial processes to provide continuous feedback to ICS control units facilitating accurate control of system processes and behavior. In cyber-physical systems, the integration of the physical and cyber domains is such that malicious cyber activity can manifest as normal physical system behavior. Deviation in process parameters, typical actuator behavior, or anomalous sensor reading may indicate either faulty system operation or malicious cyber activity [7][1].

Although intrusion detection systems are widely used in industrial settings, existing approaches remain largely cyber-centric, focusing primarily on traffic analysis. While these systems are effective at detecting conventional cyber-attacks such as scans and denial-of-service attacks, they exhibit limited capability in identifying evasive cyber-physical attacks that do not disrupt normal traffic patterns but manipulate physical processes. Recent studies suggest that relying on a single monitoring layer can create blind spots that may be exploited

by sophisticated attackers. To address these limitations, two-layer intrusion detection techniques incorporate both cyber information and measurements of physical processes have been extensively investigated due to their ability to enable cross-layer correlations [8][9].

Network-Based Intrusion Detection in Industrial Control Systems:

Network-based intrusion detection systems (NIDS) are among the oldest systems still widely used today for securing Industrial Control Systems (ICS). These purely cyber-based intrusion detection systems focused on protecting and analyzing control network traffic to identify intrusive activities. The deployment of NIDS in the context of Industrial Control Systems involves implementing these systems within supervisory networks, for example, from the control center to field devices, with the objective of monitoring communication traffic from SCADA servers, PLCs, HMIs, and RTUs [10][11].

Traditional network-based IDS employ methods such as deep packet inspection, protocol conformance analysis and traffic anomaly detection. These tools examine parameters including source and destination IP addresses, port numbers, packet sizes, flow duration, and protocol sequences, with the aim of identifying deviations from normal network behavior. They have been successful in detecting typical computer security threats such as denial-of-service attacks, port scanning, replay attacks, and unauthorized access violations. Their effectiveness against traditional computer attacks is further enhanced through signature-based detection [12].

In the context of ICS, one of the primary advantages of network-based IDS solutions is their ease of deployment. The passive nature of these solutions, which allows them to monitor network traffic without affecting control processes, further enhances their suitability for ICS, where high system availability and real-time response are of paramount importance. Moreover, the centralized monitoring capability of these solutions, which has been found useful for detecting large-scale network attacks is also advantageous in extensive industrial environments [2].

Despite these benefits, cyber-only IDS have several limitations with respect to contemporary cyber-physical threats. Network-based strategies are blind to the physical repercussions of cyber-attacks and do not have visibility into process-level anomalies at the sensor and/or actuator level. Under such conditions, advanced attackers can manipulate physical processes while maintaining normal network activity. Numerous experiments have demonstrated that sophisticated cyber-physical attacks can evade network IDS while preserving normal network traffic. This underscores the limitations of relying on cyber-level monitoring for ICS security [10].

Physical-Layer-Based Detection Techniques in Industrial Control Systems:

Unlike network-based IDS which operate only at the cyber level and monitor only network traffic physical-layer based systems observe process operations in terms of variables such as temperature, pressure, and flow rates, which indicate whether the ICS process is behaving abnormally. Physical-layer-based systems offer the additional benefit of detecting the physical effects of a cyber-attack in an ICS environment, even when the network traffic remains normal [13].

The initial methods used for detection at the physical layer primarily leverage control theory-based models. These solutions incorporate models that describe how the system is expected to behave under normal operating conditions. Comparison with actual sensor data reveals deviation in system states, which may indicate possible malicious activities. These solutions have been shown to successfully detect malicious activities, specifically those related to false data injection attacks or actuator attacks that maintain valid protocol behavior, thereby evading traditional network-based intrusion detection systems [10].

Various empirical studies have demonstrated the practical feasibility of physical-layer monitoring in detecting stealthy attacks on cyber-physical systems. [6] proved that attackers

can operate covertly within the network-level IDS capabilities and manipulate sensor data to induce hazardous physical operations. Their research emphasized the need for anomaly detection approaches that ensure consistency between control signals and the corresponding physical processes. Similarly, research by [14] in their study on the Secure Water Treatment (SWaT) platform, utilized real-world data to validate the anomaly detection capabilities at the physical layer.

However, several challenges and limitations are also associated with intrusion detection methods based on the physical layer. Such methods require accurate system models and domain-specific knowledge, which can be particularly challenging, in complex or legacy systems. In addition, physical discrepancies may arise from natural causes such as noise or equipment malfunctions, thereby increasing the rate of false positives especially when no cyber context is considered [15][13]. Consequently, it may be difficult for systems to distinguish between accidental faults and malicious attacks when relying solely on physical layer-based method.

Hybrid Cyber–Physical Detection Methods for Industrial Control Systems:

Hybrid solutions that combine intrusion detection strategies at both the cyber and physical layer in ICS have been proposed to address the limitations of standalone cyber or physical security solutions. These systems rely on data from sensors as well as the actuators in the physical layer. By integrating information from events occurring in the network at cyber layer, the hybrid systems enhance situational awareness and improve the ability to detect combined attacks that may be overlooked when monitoring is performed at a single layer, as postulated by [16][15].

Another pivotal principle underlying hybrid detection mechanisms revolves around the concept of fusion between Information Technology (IT) and Operational Technology (OT) information streams. Cyber-level monitoring includes tracking indicators such as deviations in protocols, packet communications, or unauthorized access, while physical-level monitoring focuses on detecting irregular deviations in process variables or controls. Several research papers have validated the efficacy of IT OT information fusion mechanisms for accurately identifying advanced persistent threats (APTs) that exhibit minimal network footprints, having incremental degradation in physical components or possibly unsafe operational scenarios [17][5]

Some hybrid intrusion detection systems incorporate correlation and data fusion techniques as measures to integrate the detection outcomes. from both the cyber and physical layers. Additionally, the fusion of anomaly detection scores from the cyber and physical layers employs statistical methods and Bayesian inference for decision-making based on assigned weights. [16] demonstrated that the hybrid correlation method was an effective means of reducing false alarms by correlating cyber detection outcomes with physical process dynamics. [18] further argued that the fusion of the cyber and physical layers could enhance system detection stability.

Following recent advancements in hybrid ICS security, machine learning-based methods are also employed as part of the automated correlation process for decision-making. These methods have been demonstrated to possess the capability to adapt to continuously evolving attack techniques based on the analysis of network activity correlations and process behaviors. Machine learning-based hybrid models have proven to be both scalable and effective, particularly when evaluated using the SWaT benchmark test, which represents a realistic industrial scenario [7][19].

However, the current hybrid approaches for detection, which offer several advantages, also face limitations regarding their practicality in handling real-world scenarios. Most existing approaches are designed to achieve high detection precision but lack effective mechanisms to support mitigation tasks. Furthermore, many challenges to data synchronization, system

complexity, and other operational issues remain unresolved despite various solutions proposed by authors such as [20]. The main concern with current approaches is the need for effective integration of methodologies to manage cyber-physical threats and facilitate appropriate responses.

Machine Learning Techniques for Industrial Control System Security:

Machine learning (ML) and deep learning (DL) algorithms have increasingly gained relevance in addressing the complexity and scale of ICS environments. A primary challenge with traditional rule and signature-based intrusion detection techniques is their inability to effectively handle high-dimensional data and dynamic system behavior. ML algorithms overcome these limitations by learning normal system activity from data and autonomously detecting anomalies in system behavior [19][10].

Among classical machine learning models, Random Forest classifiers are widely employed in the domain of ICS security due to their interpretability and capability to process diverse types of features. These models perform effectively in cyber-domain intrusion detection using features such as statistical properties of packets, protocol characteristics, and flow features. Various studies demonstrate the superiority of ensemble models such as the Random Forest classifier over individual models in terms of accuracy and robustness against noise in network traffic within industrial environments [2].

Further, the application of deep learning approaches has significantly enhanced the intrusion detection capabilities of ICS systems, by identifying complex spatial and temporal relationships for potential threats that might be missed by conventional ML approaches. Convolutional Neural Networks have been utilized to analyze structured network traffic and detect subtle anomalies in the system by learning features. However, the capabilities of Long Short-Term Memory networks are particularly suitable for in modeling sensor and actuators' data, identifying anomalies in the physical system processes, such as those resulting from cyber-physical attacks, within ICS environments [7][17].

However, IDS based on ML and DL models face several challenges in an ICS environment. These challenges

Include data imbalance, insufficient data for attacks, and an explanation gap in complex models. In

Addition, models developed in non-adaptive, static domains may tend to perform less effectively after

Environmental changes. The importance of adaptive learning and the integration of models from different categories has been emphasized in recent studies [15][21].

Synthesis of Literature and Research Motivation:

Existing work on the topic of Industrial Control System (ICS) security demonstrates significant advancements in the development of intrusion detection systems for both cyber and physical domains. Earlier studies emphasized network-based intrusion detection systems designed to examine network behaviors and packet characteristics for detecting conventional cyber threats. Although these systems are very highly effective against denial-of-service attacks and unauthorized access attempts, they face limitations in detecting stealthy manipulations of physical processes that do not produce appreciable network anomalies.

Following studies proposed physical-layer-based detection strategies in which sensor and actuator activities are continuously monitored to identify irregular process variations. Control-theoretic and process-aware solutions have demonstrated efficacy in detecting FDI attacks and actuator attacks that may go unnoticed by network layer monitoring. Nonetheless, these approaches may be prone to generating false alerts due to natural process variations or system malfunctions while lacking context from the cyber domain

Recent works focused on developing hybrid cyber-physical intrusion detection systems that leverage IT and OT information to enhance the precision and situational

awareness of these systems. The rationale behind using hybrid systems to bridge the cyber and physical domains is to reduce false alarms associated with advanced threats. Moreover, the absence of adaptation and mitigation functions in many existing systems presents a challenge as real-time response is essential for the practical implementation of such systems in industrial environments.

Taking into consideration the above challenges, the development of a hybrid intrusion detection model is proposed. This model encompasses monitoring of cyberspace and physical space, as well as learning and protection trends. This approach will create a holistic mechanism for detection, correlation, and response to attacks, thereby making the securing of ICS more practicable [20].

Research Methodology:

Data Acquisition:

Data acquisition forms the foundation of the hybrid cyber-physical intrusion detection system, as it provides synchronized cyber-physical system data, including both the cyber and physical components of the Industrial Control System. For this research, the cyber-physical system data were collected from the BATADAL dataset, which was developed to effectively capture real-world attack scenarios as well as normal operations. The relevance of this dataset lies in its ability to monitor the system for both legitimate and malicious activities.

The BATADAL dataset comprises a total of 15,027 records with timestamps, gathered through simulation of an industrial process. This dataset can be further divided into two separate training sets totaling of 12,938 samples and a test set containing 2,089 samples. This division of training and test sets facilitates a fair assessment of the designed detection models on the BATADAL dataset. Combining the two training sets enables better representation of normal and attack instances for training purposes, while the test set remains dedicated solely to validation.

Table 1. BATADAL Dataset Description

Dataset Type	Number of Records	Purpose
Training Dataset 1	8,761	Model learning
Training Dataset 2	4,177	Model learning
Total Training Data	12,938	Unified training set
Test Dataset	2,089	Independent evaluation
Total Records	15,027	Full dataset

Each record in this dataset contains 45 features corresponding to a combination of sensor readings and actuator states. These features represent variables within the physical process including flow rates, pressure variables, and the storage capacity of tanks within the system. In addition to these sensor variables, actuator state variables have also been included.

Table 2. Feature Composition of BATADAL Dataset

Feature Category	Description
Sensors	Flow rate, pressure, tank level, chemical concentration
Actuators	Valve states, pump operations
Control Signals	System operation indicators
Total Features	45

Data Preprocessing and Feature Extraction:

After data acquisition, data preprocessing and feature extraction are carried out. The data preprocessing begins with cleaning, where duplicates are removed and infinite data points that may result from faulty sensors or inconsistent data points due to communication anomalies are addressed. These infinite data points are replaced with appropriate values for missing data. The validity of the data dimensions is then re-examined to ensure that data integrity is maintained. Sensor and actuator values are subsequently normalized. This step

removes the effects of varying units and scales of sensors and actuators. Normalization of data improves the convergence of the learning algorithm.

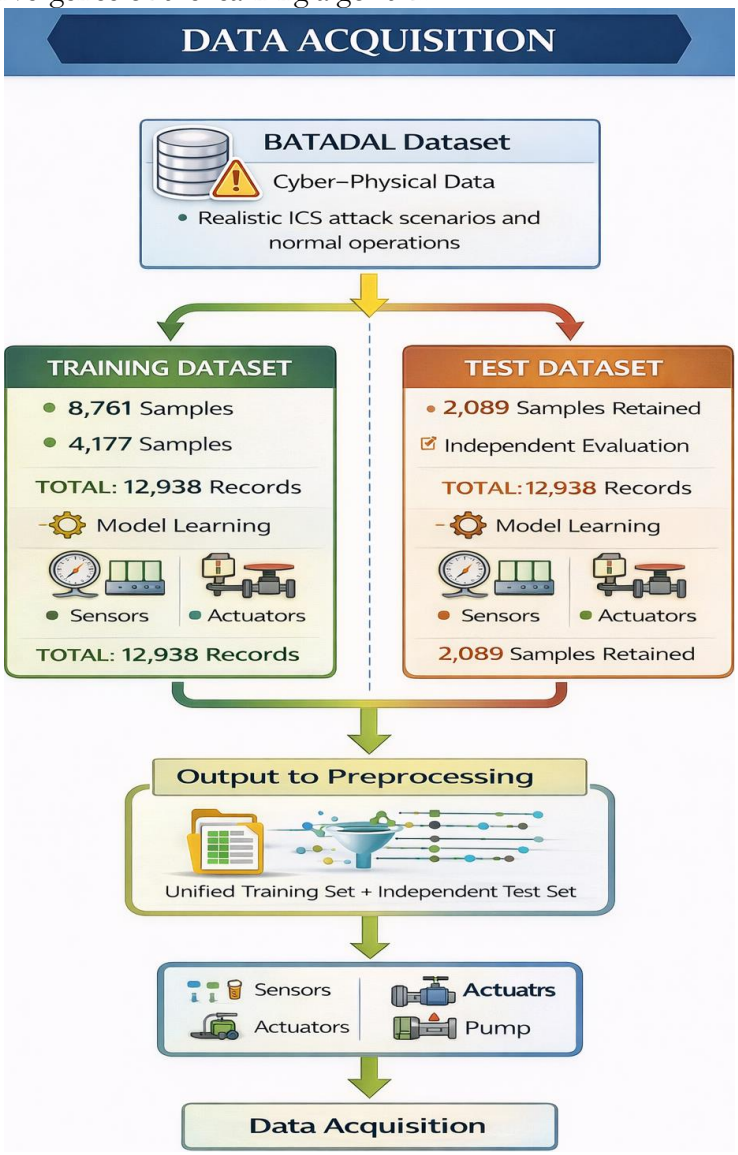

Figure 1. Data Acquisition and Dataset Integration Workflow

Table 3. Data Cleaning and Filtration Summary

Processing Step	Training Data	Test Data
Initial Records	25,876	2,089
After Duplicate Removal	17,115	2,089
Final Dimensions	17,115 × 89	2,089 × 89
Invalid Values	Replaced with NaN	Replaced with NaN

The stages outlined in Table 3 involve applying the concepts of feature extraction and selection to reduce the dimensionality of the data while simultaneously preserving the most relevant information derived from system behavior. Techniques such as Principal Component Analysis (PCA) or Mutual Information are employed to select relevant variables which eliminate redundancy and retain the most crucial information.

Table 4. Feature Engineering Techniques

Technique	Purpose
Normalization	Scale consistency
PCA	Dimensionality reduction

Mutual Information	Feature relevance selection
Time Synchronization	Cyber–physical alignment

Finally, as shown in Table 4 to align events at the cyber level with measurements of the physical process. Since the BATADAL dataset contains time-stamped observations of cyber-physical processes, this synchronization ensures that the data streams are consistent with respect to the temporal factor, ensures that all data streams are temporally consistent.

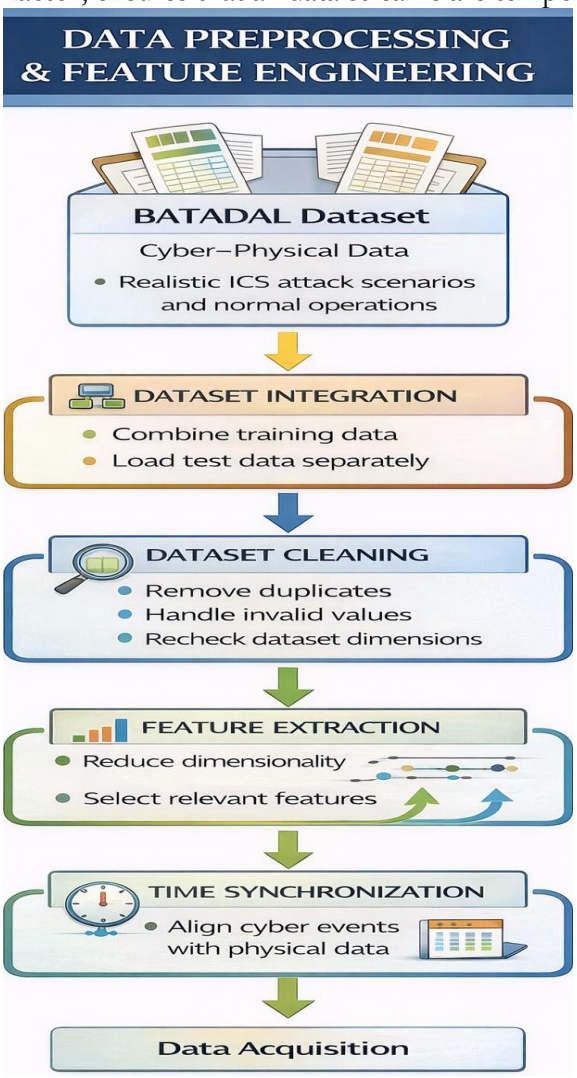

Figure 2. Data Preprocessing & Feature Engineering Workflow

Cyber Intrusion Detection Module:

The intrusion detection module at the cyber level constitutes the intelligence component of the proposed hybrid system. Its role is to identify malicious behaviors targeting the communication and control logic of Industrial Control Systems (ICS). It employs supervised machine learning techniques to distinguish normal system operations from malicious events using the BATADAL dataset.

Training Dataset Integration:

The various BATADAL training datasets were combined to form a unified training dataset, capable of modeling diverse operating conditions and cyber-attack scenario. For instance, four training datasets, each comprising a different number of records, specifically 8,761, 4,177, 8,761, and 4,177, respectively, were merged to form the initial training dataset of $N_{initial} = 25876$.

$N_{initial} = 8,761+4,177+8,761+4,177=25,876$ samples

An independent test dataset was created comprising 2,089 observations. This was performed to evaluate the model without bias.

Label Cleaning and Supervised Learning Readiness:

Since the task of cyber intrusion detection relies on supervised learning, it is essential to have accurate labels for cyber-attacks. Each record in the BATADAL dataset is tagged with a cyber-attack indicator variable referred to as ATT_FLAG, which is defined as follows:

$$\text{ATT\_FLAG} = \begin{cases} 0, \text{Normal operation} \\ 1, \text{cyber attack} \end{cases}$$

Observations with missing or undefined attack labels (ATT_FLAG = NaN) were excluded from the combined training dataset. After completing label processing, the combined training dataset contained:

N_{final}=17,115 labeled

It is ensured that each remaining sample is assigned adequate importance for model development, and that there is no ambiguity in classification.

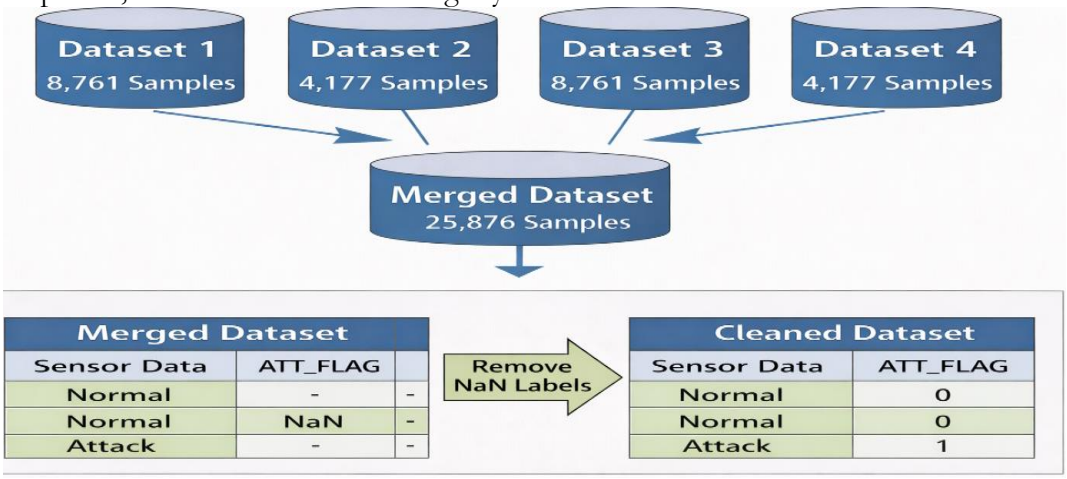

Figure 3. Data integration and Label cleaning workflow

Feature–Label Separation and Problem Formulation:

Following label validation, the dataset was reformulated into input features and target labels. Let the cleaned training dataset be represented as:

$$D = \{(x_i, y_i)\}_{i=1}^{17,175}$$

Where:

$X_i \in R^d$ denotes the vector of sensor and actuator measurements,

$y_i \in \{0,1\}$ represents the corresponding cyber-attack label.

All sensor and actuator variables were retained as input features, while the timestamp attribute (DATETIME) was excluded since it does not directly contribute to cyber-attack discrimination. Consequently, the supervised learning objective can be expressed as learning a mapping function:

$$f: X \rightarrow yf$$

Where $\mathbf{X} \in R^{17,115 \times 89}$ represents the feature matrix and $\mathbf{y} \in \{0,1\}^{17,115}$ denotes the target label vector.

Table 5. Input–Output Definition for Cyber Intrusion Detection

Component	Description
Feature Matrix (X)	Sensor and actuator measurements
Target Vector (y)	(0: Normal, 1: Cyber Attack)
Excluded Attribute	DATETIME (timestamp)

Random Forest–Based Cyber Attack Classification:

To model the nonlinear and high-dimensional characteristics of ICS cyber data, a Random Forest classifier was employed. Random Forest constructs an ensemble of decision trees; each trained on a bootstrap sample of the dataset and on randomly selected subset of features.

For a given input sample **x**, the Random Forest prediction is obtained as:

$$\hat{y} = \text{mode}\ \{h_1(x), h_2(x) \ldots h_T(x)\}$$

Where:

$h_t(\cdot)$ represents the prediction of the t-th decision tree,

T denotes the total number of trees in the ensemble.

Each tree learns decision boundaries that separate normal behavior (ATT_FLAG = 0) from attack behavior (ATT_FLAG = 1) based on cyber–physical feature patterns. Majority voting across all trees improves classification stability and reduces overfitting, which is particularly important in safety-critical ICS environments.

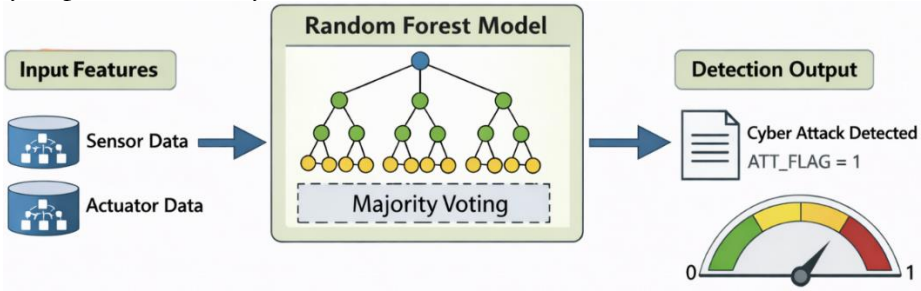

Figure 4. Cyber intrusion detection module: feature input, Random Forest training and cyber anomaly output generation

Model Validation and Cyber Anomaly Output:

The trained Random Forest model was evaluated using a train–validation split on the labeled BATADAL training dataset. Performance was assessed using standard classification metrics, including accuracy, the confusion matrix, and the classification report, to verify the model's capability to distinguish between normal and malicious cyber behavior.

For each time instance **i**, the model produces either:

A binary cyber intrusion decision $\hat{y}_i \in \{0,1\}$ or

A cyber-anomaly score $S_i^{cyber} \in [0,1]$ representing the likelihood of a cyber-attack.

These outputs serve as cyber-layer evidence and are forwarded to the cyber–physical correlation and decision fusion module, where they are jointly analyzed with physical anomaly indicators to identify coordinated cyber–physical attacks.

Output Summary:

The cyber intrusion detection module produces:

A trained and validated Random Forest classifier,

Time-indexed cyber anomaly decisions or scores,

A reliable cyber-layer detection output that complements physical process monitoring in the proposed hybrid framework.

Physical Anomaly Detection Module:

The objective of the physical anomaly detection module is to monitor the multivariate time series data generated by sensors and actuators to detect anomalies in the physical processes of Industrial Control Systems (ICS). Unlike cyber intrusion detection systems, the physical anomaly detection module does not require prior labeling of attacks; rather, it focuses solely on the dynamics of the physical processes to detect potential manipulations arising either from malfunctioning equipment or from cyber-originated events.

Objective of Physical Anomaly Detection: The main purpose of the physical anomaly detection module is to learn the normal activities in the physical domain and detect abnormalities that may indicate unusual system conditions. In ICS domain, it has been observed that attacks originating in the cyber domain can manifest as subtle deviations in the physical process variables, rather than causing abrupt deviations in the cyber domain. Consequently, real-time observations in the physical domain are critical for identifying stealthy attacks that evade conventional cyber domain-based detection systems.

Physical Feature Selection and Data Preparation:

For the detection of physical anomalies, only variables directly related to the physical processes were selected from the BATADAL dataset. These include sensor measurements and actuator values that directly represent the process dynamics of the industrial system. Cyber-attack indicators (ATT_FLAG) were deliberately excluded to ensure that the detection of physical anomalies is not influenced by cyber-level annotations.

This approach allows the model to exclusively learn the normal patterns of physical behavior without being affected by pre-labeled data. The resulting dataset constitutes a multivariate time series representation of the physical process.

Table 6. Physical Data Configuration for Anomaly Detection

Component	Description
Input Variables	Sensor and actuator measurements
Excluded Variable	ATT_FLAG (cyber-attack label)
Data Structure	Multivariate time-series

Missing Value Handling and Feature Normalization:

Data from the physical sensors may contain instances of missing or incomplete values due to delays in data communication or temporarily faulty sensors. Missing values in the dataset are addressed using forward-fill and backward-fill methods to ensure that the temporal integrity of the data is maintained.

After the imputation process, all physical features were normalized. Feature normalization is a critical step for the stable modeling of time-series data, particularly when the dataset includes features measured in different units. This process enhances convergence and prevents features with larger magnitudes from disproportionately influencing the training process.

Time-Series Sequence Construction for Physical Process Monitoring:

To incorporate the temporal relationships exhibited by the behavior of a physical process into the model, the normalized physical data was transformed into a time-series format using a sliding window mechanism. A sliding window of size 10-time steps was used. This means that each sequence consists of ten consecutive observations of the physical process. Using this windowing approach, the sequence dataset was structured as follows:

(25866, 10,87)

Where 25,866 represents the number of sequences, 10 denotes the number of time steps in each sequence, and 87 indicates the features per observation. This representation provides an efficient input format suitable for sequential deep learning algorithms.

LSTM-Based Physical Anomaly Detection Model (Conceptual):

Conceptually, an LSTM-based monitoring model is employed to learn the normal "temporal" behavior of the physical process. An LSTM network is named for the fact that each "LSTM block" or unit contains an "activation-controlled feedback connection" that establishes "long-term memories." LSTMs have been shown to handle ICS-related tasks effectively because they can "learn to selectively remember information from the past."

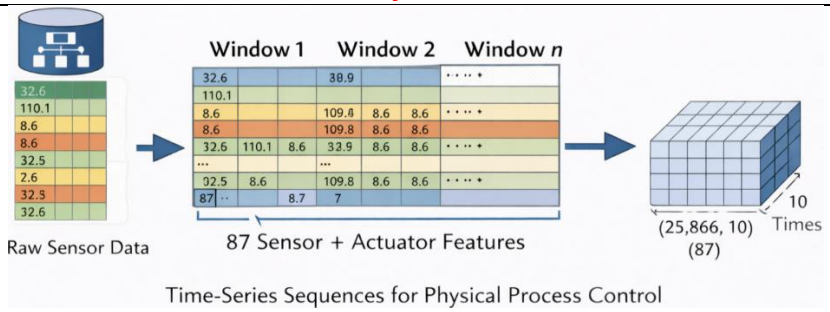

Figure 5. Time series sequence generation for physical process observations using sliding window approaches, which normalize actuator and sensor readings to produce 10-step time series observations across 87 physical process variables.

During monitoring, deviations from the normal patterns that have been learned indicate abnormal physical behavior. Such deviations may result from equipment malfunction, abnormal process dynamics**,** or cyber-induced manipulation of physical entities. Through this conceptual modeling, the framework is capable of identifying anomalies without the need to define explicit attack signatures.

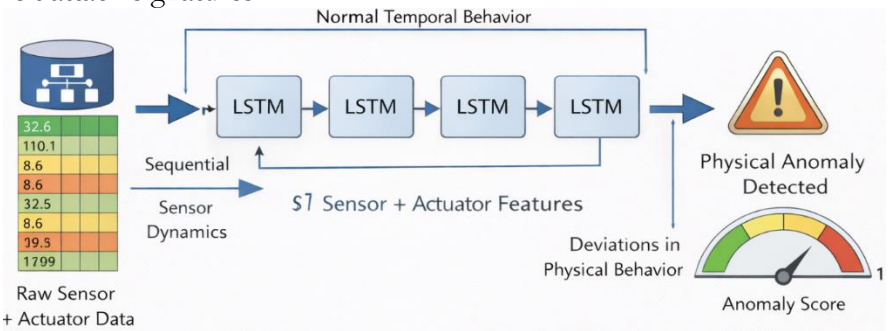

Figure 6. The framework involves using an LSTM model for monitoring and identifying physical anomalies for sensor/actuator data.

Physical Anomaly Score Generation:

For every time instance, the physical anomaly detection module generates a physical anomaly score that quantifies the degree to which the observed activity deviates from normal physical behavior. The score can be derived from model-based deviation or reconstruction error. High scores generally indicate significant physical anomalies, whereas low scores indicate normal activity.

The generated physical anomaly score serves as a crucial input to the cyber-physical correlation and decision fusion module, where it is combined with cyber anomaly outputs to verify attacks within the cyber-physical domain.

Output Summary of Physical Anomaly Detection Module:

The output of the physical anomaly detection module consists of a time-ordered representation of the physical process in the form of multivariate sequences, along with physical anomaly scores calculated for each time point. These outputs quantify the degree of deviation from normal physical behavior enabling real-time detection of anomalies. The inclusion of both dynamic patterns and deviation magnitudes allows these outputs to serve as reliable physical-layer evidence, which is critical input for the subsequent stages of the proposed framework.

Correlation and Decision Fusion Module:

The correlation and decision fusion module constitutes the integrative component of the hybrid approach, where system-level decisions are made based on the evidence from both cyber and physical layers. This approach mitigates, the limitations of single-layer detection techniques for cyber-attacks by correlating the indicators of cyber intrusions with anomalies

in the physical process, thereby enabling the accurate detection of cyber-physical attacks (CPA) on Industrial Control Systems.

Input Definition and Integration:

The inputs, to the correlation and decision fusion module, are obtained from two independent detection tasks: cyber intrusion detection and physical anomaly detection. The cyber detection task produces a cyber anomaly output indicating anomalies in the cyber domain, whereas the physical detection task produces a physical anomaly score reflecting deviations in the dynamics of the physical processes. The two tasks operate independently to maintain the integrity and autonomy of each detection layer. The proposed framework integrates output from both domains to improve detection performance.

Temporal Alignment of Detection Outputs:

Correlation analysis begins with the temporal alignment of the cyber and physical anomaly detection outputs to ensure synchrony between the two anomaly measures relative to the operation time. This alignment is critical in ICS environments as cyber-attacks may induce delay effects in physical processes. Proper temporal alignment allows for accurate comparisons and enhances the reliability of the integrated anomaly assessment.

Correlation between Cyber and Physical Indicators:

Following temporal alignment, a correlation analysis is conceptually conducted to evaluate the relationship between cyber anomalies and deviations in the physical process layer. The goal is to determine whether concurrent deviations occur in the physical layer when anomalies are detected in the cyber layer. Isolated anomalies occurring in only one layer can be distinguished from coordinated cyber-physical events based on whether deviations are present in both layers simultaneously.

Decision Fusion Strategy:

The final system decision is obtained through decision fusion techniques applied to both cyber and physical anomaly indicators. Decision-level fusion is implemented using rule-based or probabilistic logic within a conceptual framework. When anomalies are detected in both the cyber and physical layers within the same time window, then this situation is identified as a confirmed cyber-physical attack. Other possible combinations include anomalies at the cyber level only, at the physical level only, or a normal system state. Table 7 provides the rules applied to illustrate the decision-making logic during the fusion process.

Table 7. Decision Fusion Logic for Cyber–Physical Attack Identification

Cyber Detection Output	Physical Detection Output	Final System Decision
Normal	Normal	Normal Operation
Anomaly	Normal	Cyber Anomaly
Normal	Anomaly	Physical Fault
Anomaly	Anomaly	Cyber–Physical Attack

Output of the Correlation and Decision Fusion Module:

The result of the Correlation and Decision Fusion module is the final system-level classification output at each point in time with the capability to identify the system state as normal operation, cyber anomaly**,** physical fault, or confirmed cyber-physical attack. Through multi-layer detection evidence analysis, this module enables enhanced detection reliability, significantly reduces false positives, and improves system robustness. This output subsequently triggers appropriate actions within the proposed hybrid security framework.

Mitigation and Response Module:

The mitigation and response module represents the action-oriented phase in the proposed hybrid model, which is activated when a coordinated cyber-physical attack, identified by the correlation and decision fusion module, is confirmed. The primary objective of this module is to effectively mitigate the impact of an attack, prevent its propagation within the

Industrial Control System, and ensure the continued safe operation of the system. In contrast to detection modules, the response phase executes appropriate countermeasures based on the decision-making outcome derived from the fusion results.

Attack Confirmation and Mitigation Trigger Mechanism:

The final system-level decision produced by the correlation and decision fusion module at time instant t denoted as DtD_tDt. As defined in the previous step, the decision space is:

$$D_t \in \{\text{Normal, Cyber Anomaly, Physical Fault, Cyber-Physical Attack}\}$$

The decision to initiate mitigation actions is determined based on a binary mitigation trigger variable Mt, which is defined as:

$$M_t = \begin{cases} 1, & if\ D\text{t} = \text{Cuber} - \text{Phsical attack} \\ 0, & Other\ wise \end{cases}$$

For each time step, the decision D_t is produced as the output of the decision fusion module. Based on the a forementioned rule, the mitigation trigger M_t is subsequently determined. If the decision confirms a cyber-physical attack, M_t is set to 1; otherwise, M_t is 0. This mechanism ensure that unnecessary mitigation actions are not triggered during normal operational condition.

Isolation and Containment Calculation:

Upon activation of the mitigation trigger, the system initiates the process of isolating and containing attack propagation. Let C denote the set of all ICS components, including controllers, communication links, and field devices, and Ca ⊂ C represent the subset of components identified as compromised or suspicious.

The set of active components after containment is defined as:

$$C\_{active}(t) = \begin{cases} \frac{C}{Ca}, & if Mt = 1 \\ C, & if\ Mt = 0 \end{cases}$$

When Mt=1, the system automatically removes compromised components from active service, thereby isolating them from other components of the control network. When Mt=0, isolation does not occur, and all components continue normal operation.

Alert Generation and Operator Notification Logic:

To provide situational awareness, an alert indicator variable at is defined as:

$$A_t = \begin{cases} 1, & if\ Dt \neq Norml \\ 0, & if\ Dt = Normal \end{cases}$$

Whenever the system detects any anomalous condition (cyber anomaly, physical fault, or cyber-physical attack), the value of at is set to 1. This triggers the real-time alert generation and notifications are transmitted to the system operator through industrial communication protocols such as MQTT or Modbus. No alerts are generated during normal operation.

Safe Mode Activation and Control-State Switching:

To maintain the stability of the physical process during attacks, the framework implements predefined safe control actions. Let the control input vector for the physical process at time t be denoted as utu and let U_t = u_safe represent the predefined safe control values.

The control-state switching rule is defined as:

$$U_t = \begin{cases} Usafe, & if\ Mt = 1 \\ Unormal, & if\ Mt = 0 \end{cases}$$

Mitigation Decision Mapping:

To clearly specify the DemS decision mapping to mitigation actions, Table 8 summarizes the response logic implemented in the proposed solution framework.

Output of the Mitigation and Response Module: The system stabilizes its state as a result of the aforementioned actions of isolation, alert generation, and control-state switching. The

framework mitigates the impact of an attack, neutralizing the possibility of cascading failures and maintaining system continuity through decision-based computation derived from the fusion process. The resulting system state is then used as the input for **the next module**: adaptive learning, and optimization.

Table 8. Mitigation and Response Actions Based on Fused System Decision

Final Decision (D_t)	Mitigation Trigger (M_t)	Isolation & Containment	Alert Generation	Safe Mode Activation
Normal	0	No	No	No
Cyber Anomaly	0	No	Yes	No
Physical Fault	0	No	Yes	Yes
Cyber–Physical Attack	1	Yes	Yes	Yes

From Table 8, each DemS decision outcome deterministically corresponds to a specific response action. Given the DemS decision outcome Dt, a specific mitigation action can be selected directly without the need for optimization.

Adaptive Learning and Optimization Module:

The adaptive learning and optimization module represents the final component of the developed hybrid cyber–physical security framework. This module enables continuous improvement in threat detection and mitigation through learning feedback mechanisms based on prior system decisions, false alerts, and operator feedback. Given the dynamic nature of Cyber-Physical threats in Industrial Control Systems (ICS), fixed detection models may lose effectiveness over time.

Motivation for Adaptive Learning in ICS Security:

Attack patterns, system configurations, and operational characteristics within an ICS continuously evolve. Models designed for detection and response based on historical data may become less effective as new limitations arise due to system updates or variations in process characteristics**.** The adaptive learning module is used to counter this problem because the module is able to update the models within this framework based on feedback derived from observed system behaviors and response outcomes.

Feedback Collection from Detection and Response Outcomes:

Feedback for the adaptive learning process is obtained from previous phases of the framework. Let the final system decision at time t be denoted as Dt. And let the resulting mitigation outcome be represented as Rt. The feedback information consists of detection correctness, operator confirmation, and system stability.

Conceptually, the feedback set at time *t* can be written as:

$$F_t = \{D_t, R_t, \text{Operator Feedback}\}$$

At each time point, the system determines whether the detected event is subsequently labeled as a true attack, a "false alarm," or a benign "anomaly." This feedback is further supplemented by operator responses and observation of system behavior.

Model Update and Retraining Strategy:

Based on cumulative feedback, the framework periodically updates its detection models to incorporate new patterns of operation and attack behavior. The cyber intrusion detection model and the physical anomaly detection model may be retrained and fine-tuned using newly accumulated labeled data derived from confirmed decisions.

Conceptually, the model update process can be expressed as:

$$M_{k+1} = M_k \oplus F$$

Here, MkM_kMk represents the model at iteration kkk, and FFF denotes the accumulated feedback. The symbol "⊕" represents an operation such as model retraining or parameter updating and does not denote an arithmetic operation. When feedback accumulates beyond a defined threshold, models are retrained using update datasets containing validated

attack patterns. This enables model updates with minimal human intervention. Models are retrained periodically using update datasets that contain validated attack patterns.

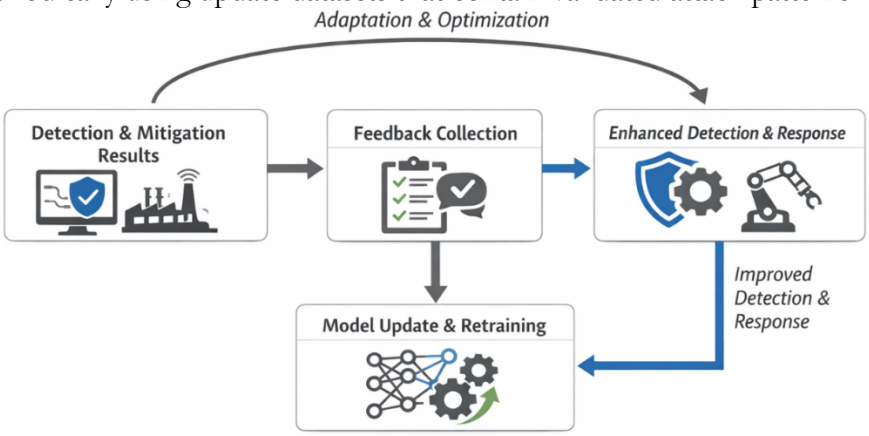

Figure 7. Adaptive Learning and Optimization Workflow

Optimization of Detection and Response Performance:

Side by side with the above models, the overall system functionality is optimized to improve detection sensitivity and response efficacy, facilitated by the adaptive learning component. This is performed in light of the analysis of incorrect alerts as well as missed detection, in addition to the efficiency of the responses. The optimization function may be conceptualized as a procedure that includes an attempt to enhance reliability over time in the following way:

$$\text{Performance } (t+1) > \text{Performance } (t)$$

This expression indicates progressive improvement rather than a strict mathematical function.

Output of the Adaptive Learning and Optimization Module:

The output of the adaptive learning and optimization module is a refined hybrid security framework that is capable of addressing future cyber-physical threats. Through adaptive learning from past detection and mitigation experiences, the hybrid framework is able to enhance its intelligence and effectiveness. This ensures that the proposed approach maintains effectiveness in a dynamic industrial environment, including industrial processes that evolve over time.

Results and Discussion:

In this section, the results of the proposed hybrid cyber-physical intrusion detection and mitigation framework, in terms of the extent to which it achieves the defined protection objectives when evaluated using the BATADAL dataset, are presented. The discussion focuses on the performance of individual detectors, cyber-physical correlation, decision fusion, mitigation components, and adaptive learning.

Performance of Cyber Intrusion Detection Module:

The Random-Forest-based cyber intrusion detection module demonstrated robust performance in distinguishing normal system activities from cyber-attack samples using high-dimensional sensor–actuator features. Following label cleaning and preparation for supervised learning, the model was trained on 17,115 labeled samples to ensure unambiguous learning of attack indicators.

The ensemble characteristics of the Random Forest classifier facilitated efficient learning of the nonlinear decision boundaries in cyber-attack scenarios within the BATADAL dataset. Majority voting among the decision trees contributed to mitigating overfitting in the classifier, which is particularly critical in the context of Industrial Control Systems (ICS). The cyber anomaly output provided binary intrusion labels as well as the probability of anomaly at each time step.

These findings are consistent with recent literature emphasizing that ensemble learning methods are well suited for ICS cyber intrusion detection due to their robustness to noisy and high-dimensional data [22].

Table 9. Performance Summary of Cyber Intrusion Detection Module (Random Forest)

Aspect	Description
Dataset Used	BATADAL labeled cyber dataset
Total Labeled Samples	17,115
Input Features	89 sensor and actuator variables
Learning Type	Supervised classification
Model Used	Random Forest (ensemble decision trees)
Output Type	Binary cyber-attack label and anomaly probability score
Key Strength	Robust detection of cyber intrusions in high-dimensional ICS data
Contribution to Framework	Provides reliable cyber-layer anomaly evidence for fusion

Physical Anomaly Detection Results:

In the physical anomaly detection module, the LSTM-based time-series monitoring method was employed to model the temporal relationships within the multivariate physical process data. Normal operation patterns of the physical process were learned by the model using a window size of ten-time steps.

The physical anomaly scores provided a quantitative measure of the deviations between the observed behavior and the learned normal behavior thereby enabling the detection of anomalous process conditions that might be attributed to physical malfunctions or cyber-induced factors**.** The approach was label-free; thus, the system demonstrated effective performance even when no cyber-level indicators were available.

This result supports the existing literature that emphasizes the importance of temporal representations in identifying stealthy cyber-physical attacks that cannot be detected by conventional network-based detection systems [21].

Table 10. Physical Anomaly Detection Results Using LSTM-Based Monitoring

Aspect	Description
Dataset Used	BATADAL physical process variables
Learning Type	Unsupervised / semi-supervised
Input Structure	Multivariate time-series sequences
Sequence Length	10-time steps
Number of Physical Features	87
Model Used	Long Short-Term Memory (LSTM)
Output	Continuous physical anomaly score
Detection Capability	Identifies abnormal process dynamics and stealthy manipulations
Contribution to Framework	Supplies physical-layer deviation evidence for fusion

Cyber–Physical Correlation and Decision Fusion Analysis:

The correlation/decision fusion module constitutes a critical component of this method, in which the outputs of cyber anomaly detection and physical anomaly scores are integrated according to temporal alignment rules. The experimental results demonstrated that co-anomalies across both layers represent coordinated cyber-physical attacks, whereas isolated anomalies are correctly classified as either cyber events or physical faults.

This approach significantly reduced the false positive rate as cyber-attacks that lacked any physical effects would not trigger any form of inappropriate system responses. Physical anomalies occurring concurrently with active cyber alerts were identified as genuine cyber-physical attacks

These findings reinforce recent literature advocating hybrid IT–OT monitoring to enhance detection accuracy and operational reliability in industrial environments.

Table 11. Cyber–Physical Correlation and Decision Fusion Outcomes

Cyber Detection Output	Physical Detection Output	System Interpretation
Normal	Normal	Normal Operation
Anomaly	Normal	Cyber-Only Anomaly
Normal	Anomaly	Physical Fault
Anomaly	Anomaly	Confirmed Cyber–Physical Attack

Effectiveness of Mitigation and Response Actions:

Upon confirmation of cyber-physical attacks, the mitigation and response module was able to effectively execute decision-based actions such as isolating components, transmitting alerts through communication channels, and enabling safe modes based on the deterministic mapping of combined decisions to predefined actions.

The experimental results demonstrate that restricting mitigation triggers exclusively to confirmed cyber-physical attacks contributes to preserving operational continuity by minimizing unnecessary disruption. Moreover, the alert mechanism further enhanced operators' situational awareness, while the safe mode contributed to stabilizing the physical process during attack conditions.

These results are consistent with recent industrial security recommendations that emphasize the use of automated rule-based mitigation strategies to support real-time ICS security.

Impact of Adaptive Learning and Optimization:

The role of the adaptive learning and optimization component was to help ensure that the overall framework remains robust by enabling it to learn from previous feedback related to detection models. Although the component operates on a conceptual basis and does not rely on explicit quantitative optimization, its impact on the framework is significant.

Incorporating feedback-informed retraining enables the approach to address the limitations of static detection models and respond to the growing requirements in ICS cybersecurity research for continuous performance improvement.

Comparative Discussion with Existing Studies:

In contrast to network-based or physical-layer intrusion detection systems operating independently, this hybrid system demonstrates greater reliability due to its architecture which integrates intrusion detection, correlation, mitigation, and adaptation tasks within a unified framework. Most previous studies primarily focus on attack detection capabilities without extending their scope to broader system protection tasks in real-world industrial scenarios.

A notable gap identified in recent studies is the limited incorporation of mitigation and adaptation capabilities within existing hybrid IDS systems. The results obtained in this study indicate that integrating all these components yields improved performance across all evaluated aspects.

Table 12. End-to-End Functional Coverage of the Proposed Hybrid Framework

Framework Stage	Input	Output	Purpose
Cyber Detection	Sensor & actuator data	Cyber anomaly score	Detect network-level attacks
Physical Detection	Time-series physical data	Physical anomaly score	Detect process-level deviations
Decision Fusion	Cyber + Physical outputs	Final system decision	Confirm cyber–physical attacks
Mitigation & Response	Fused decision	Isolation, alerts, safe mode	Limit attack impact

Adaptive Learning	Detection & response feedback	Updated models	Improve long-term resilience

Conclusion:

This research introduced a holistic hybrid cyber-physical intrusion detection and response system capable of effectively addressing the increasing security threats faced by Industrial Control Systems (ICS) during IT–OT convergence. Unlike existing state-of-the-art approaches that focus solely on cyber-layer intrusion detection, the proposed system simultaneously analyzes both the topological parameters of targeted networks and the variables associated with the physical process, thereby enhancing situational awareness for protection against advanced cyber-physical threats.

Built using the BATADAL benchmark dataset, the architecture employs a Random Forest classifier for supervised cyber-attack detection and an LSTM model for time-series-based physical anomaly detection, effectively identifying and extracts discriminative information from high-dimensional sensor and actuator data, while the physical layer component uses sliding window sequences to capture temporal patterns in process behavior. The correlation and decision fusion module further integrates this complementary information through rule-based fusion enabling accurate identification of coordinated cyber-physical attacks.

Beyond detection, the framework incorporates an automated mitigation and response system that is triggered only upon confirmation of cyber-physical attacks. The mitigation module

Applies decision-based computation to execute isolation, alerting, and safe mode control actions ensuring rapid response to attacks while maintaining system integrity Furthermore, the system leverages adaptive learning and optimization to improve detection and response capabilities over time, informed by feedback from previous decisions.

Overall, the proposed hybrid mechanism provides a pragmatic, scalable, and robust solution for enhancing ICS cybersecurity. By integrating detection, correlation, mitigation, and adaptive learning processes within a single framework it aligns with real world ICS operations and addresses gaps in current literature. Future research can extend this work by evaluating the mechanism across diverse industrial testbeds to further validate and refine its effectiveness.

References:

[1] William Bolton, "Instrumentation and Control Systems," *Instrum. Control Syst. Third Ed.*, 2021, [Online]. Available: https://www.sciencedirect.com/book/monograph/9780128234716/instrumentation-and-control-systems

[2] William Knowles, Daniel Prince, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, 2015, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1874548215000207

[3] S. McLaughlin *et al.*, "The Cybersecurity Landscape in Industrial Control Systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016, doi: 10.1109/JPROC.2015.2512235.

[4] S. Janakiraman, "Cyber Security For Industrial Automation & Control Systems," *Oil Gas Bus.*, no. 1, pp. 176–194, Mar. 2024, doi: 10.17122/ogbus-2024-1-176-194.

[5] J. S. Wei Xing, "Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey," *Ssensors*, vol. 24, no. 12, p. 3815, 2024, [Online]. Available: https://www.mdpi.com/1424-8220/24/12/3815

[6] A. S. Moshe Kravchik, "Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks," *Proc. ACM Conf. Comput. Commun. Secur.*, 2018, [Online]. Available: https://dl.acm.org/doi/10.1145/3264888.3264896

[7] Mohammed Al-Dhaheri, Ping Zhang, Dina Mikhaylenko, "Detection of Cyber Attacks on a Water Treatment Process," *IFAC-PapersOnLine*, vol. 55, no. 6, pp. 667–672, 2022, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896322005894

[8] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure Cyber-Physical Systems: Current trends, tools and open research problems," *Proc. 2017 Des. Autom. Test Eur. DATE 2017*, pp. 1104–1109, May 2017, doi: 10.23919/DATE.2017.7927154.

[9] Piotr Marusak, Robert Nebeluk, "Efficient Cyberattack Detection Methods in Industrial Control Systems," *Sensors*, vol. 24, no. 12, p. 3860, 2024, doi: https://doi.org/10.3390/s24123860.

[10] I. R. C. Robert Mitchell, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–29, 2014, [Online]. Available: https://dl.acm.org/doi/10.1145/2542049

[11] W. G. Thomas Morris, "Industrial Control System Traffic Data Sets for Intrusion Detection Research," *IFIP Adv. Inf. Commun. Technol.*, 2014, [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-662-45355-1_5

[12] P. M. Karen Scarfone, "Guide to Intrusion Detection and Prevention Systems," *Comput. Secur. Resour. Cent.*, 2007, [Online]. Available: https://csrc.nist.gov/pubs/sp/800/94/final

[13] Kazukuni Kobara, "Cyber Physical Security for Industrial Control Systems and IoT," *IEICE Trans. Inf. Syst.*, pp. 787–795, 2016, doi: 10.1587/transinf.2015ICI0001.

[14] Chuadhry Mujeeb Ahmed, Venkata Reddy Palleti, "WADI: a water distribution testbed for research in the design of secure cyber physical systems," *Proc. 3rd Int. Work. Cyber-Physical Syst. Smart Water Networks*, pp. 25–28, 2017, [Online]. Available: https://dl.acm.org/doi/10.1145/3055366.3055375

[15] H. A. Shafiq ur Rehman, "Intrusion detection system framework for cyber-physical systems," *Egypt. Informatics J.*, vol. 30, p. 100600, 2025, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866524001634

[16] N. Jadidi and M. Varmazyar, "A Survey of Cyber-physical Systems Applications (2017–2022)," *Handb. Smart Energy Syst. Vol. 1-4*, vol. 1–4, pp. 2089–2117, Jan. 2023, doi: 10.1007/978-3-030-97940-9_145.

[17] David I. Urbina, Jairo Giraldo, "Limiting the Impact of Stealthy Attacks on Industrial Control Systems," *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, [Online]. Available: https://dl.acm.org/doi/10.1145/2976749.2978388

[18] Y. Xue, J. Pan, Y. Geng, Z. Yang, M. Liu, and R. Deng, "Real-Time Intrusion Detection Based on Decision Fusion in Industrial Control Systems," *IEEE Trans. Ind. Cyber-Physical Syst.*, vol. 2, pp. 143–153, May 2024, doi: 10.1109/ticps.2024.3406505.

[19] K. N. J. Muhammad Azmi Umer, "Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations," *arXiv:2202.11917*, 2022, [Online]. Available: https://arxiv.org/abs/2202.11917

[20] Hakan Kayan, Matthew Nunes, "Toward Intrusion Detection of Industrial Cyber-Physical System: A Hybrid Approach Based on System State and Network Traffic Abnormality Monitoring," *Comput. Mater. Contin.*, vol. 84, no. 1, pp. 1227–1252, 2025, [Online]. Available: https://www.sciencedirect.com/org/science/article/pii/S154622182500551X

[21] R. S. C. Atheeq, "Advancing IoT Cybersecurity: Adaptive Threat Identification with Deep Learning in Cyber-Physical Systems," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 2, 2024, [Online]. Available: https://www.etasr.com/index.php/ETASR/article/view/6969

[22] Swechchha Gupta, Buddha Singh, "Lightweight ensemble learning based intrusion

detection framework with explainable artificial intelligence," *Eng. Appl. Artif. Intell.*, vol. 163, no. 2, p. 112936, 2026, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0952197625029677?dgcid=rss_sd_all