International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 10-No.4 (2024) pp. 799-810
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems

Preeti Prasada[1,2*], Srinivas Prasad[3]

[1]Research Scholar, Dept of CSE GITAM School of Technology, GITAM (Deemed to be University), Vishakhapatnam
[2]Senior Assistant Professor, CSE-AIML, Geethanjali College of Engineering and Technology, Hyderabad
* **Corresponding Author Email:**pprasada@gitam.in - **ORCID:** 0000-0002-2221-390X

[3]Professor, Dept of CSE GITAM School of Technology, GITAM (Deemed to be University), Vishakhapatnam
Email:sprasad@gitam.edu - **ORCID:** 0000-0001-6227-0798

Article Info:

DOI: 10.22399/ijcesen.539
Received : 21 October 2024
Accepted : 23 October 2024

Keywords:

Cyber-Physical Systems,
Advanced Persistent Threat,
Blockchain,
Machine Learning,
Security.

Abstract:

Cyber-Physical Systems (CPS) have become a research hotspot due to their vulnerability to stealthy network attacks like ZDA and PDA, which can lead to unsafe states and system damage. Recent defense mechanisms for ZDA and PDA often rely on model-based observation techniques prone to false alarms. In this paper, we present an innovative approach to securing CPS against Advanced Persistent Threat (APT) injection attacks by integrating machine learning with blockchain technology. Our system leverages a robust ML model trained to detect APT injection attacks with high accuracy, achieving a detection rate of 99.89%. To address the limitations of current defense mechanisms and enhance the security and integrity of the detection process, we utilize blockchain technology to store and verify the predictions made by the ML model. We implemented a smart contract on the Ethereum blockchain using Solidity, which logs the input features and corresponding predictions. This immutable ledger ensures the integrity and traceability of the detection process, mitigating risks of data tampering and reducing false alarms, thereby enhancing trust in the system's outputs. The implementation includes a user-friendly interface for inputting features, a backend for data processing and model prediction, and a blockchain interaction module to store and verify predictions. The integration of blockchain with Machine learning enhances both the precision and resilience of APT detection while providing an additional layer of security by ensuring the transparency and immutability of the recorded data. This dual approach represents a substantial advancement in protecting CPS from sophisticated cyber threats.

1. Introduction

A dependable detection and response mechanism for general and APT attacks on CPS is critical for maintaining system integrity and security. This paper presents a unified framework for intrusion detection and response in CPS designed to identify and counteract covert attacks effectively. The designed architecture offers flexibility, supporting the analysis of diverse data streams to effectively uncover hidden attacks, while also significantly lowering the chances of generating false alarms. By incorporating diverse data inputs, this system enhances the precision and reliability of attack detection, ensuring a robust defense against sophisticated cyber threats. This comprehensive approach ensures that even the most concealed threats are identified and mitigated promptly. The ability to analyze and cross-reference various data streams allows for a more accurate and timely response to potential security breaches. Consequently, this architecture not only improves security but also enhances the overall resilience of CPS.

In many industrial control systems, obtaining the exact models used by attackers or defenders is often impractical, leading to mismatches between actual and nominal models. When only nominal models are available, the stealthiness of model-based attacks can be compromised. However, there are advanced methodologies in model-based attacks that have been developed to overcome these challenges. Techniques such as data-driven feedback loops [1], two-loop covert attacks [2], robust zero-dynamics attacks [3], and robust physical-digital attacks (PDAs) [4] are examples of improved strategies. This paper will conduct a thorough review of these advanced techniques, providing insights into their mechanisms and effectiveness in CPS security. Understanding these methodologies is crucial for developing robust defense strategies against sophisticated model-based attacks. The review will highlight the strengths and weaknesses of each approach, offering a comprehensive perspective on their practical applications.

Data flow attacks occur when attackers can be injected False data into the network regarding the load at individual meters, potentially leading to system breakdowns [5]. One of the most damaging and impactful threats to the data integrity of energy management systems involves False Data Injection (FDI) attacks [6]. In networks with multiple interleaved systems, control and data flow attacks become more elusive as attackers exploit various vulnerabilities and entry points. These complex attacks require robust defense mechanisms to protect against such multifaceted threats. The increasing interconnectivity of modern energy systems makes them particularly vulnerable to these types of attacks, necessitating comprehensive security measures. Understanding the nature and potential impact of data flow attacks is essential for developing effective countermeasures. By identifying the vulnerabilities and entry points that attackers might exploit, system designers can implement more robust protections to safeguard against these threats.

In a communication-based train control system, trains and ground stations are interconnected through advanced communication protocols, enabling dynamic feedback control. This system uses a real-time wireless network to continuously share vital data, such as train conditions and operational commands [7]. By optimizing the dispatch process and ensuring timely communication, it significantly enhances operational efficiency and safety, reducing the risk of collisions and other hazards, in contrast to traditional train control methods[8]. The integration of real-time communication ensures higher operational efficiency and safety. This advanced control system highlights the importance of reliable communication networks in maintaining the safety and efficiency of CPS. The ability to respond promptly to real-time data is crucial for preventing accidents and ensuring smooth operations. This system's success underscores the potential benefits of similar implementations in other CPS applications.

Networks linking physical systems with their control software are especially susceptible to external threats, as attackers may target these systems to disrupt CPS functionality and trigger malfunctions in the physical components [9]. Machine learning is increasingly adopted in cyber-physical security because it can establish correlations between inputs and outputs using vast data sets without relying on physical laws [10]. ML-based approaches offer advanced detection capabilities, making them critical in safeguarding CPS. ML algorithms, through the analysis of vast datasets, can detect patterns and irregularities that may signal potential security breaches. This capability is especially important given the complexity and interconnectedness of modern CPS. ML's ability to enhance detection and response mechanisms makes it a valuable tool in the ongoing effort to secure CPS against various threats. The integration of ML into CPS security strategies represents a significant advancement in the field, providing a higher level of protection against potential attacks.

Cyber-physical systems face a range of vulnerabilities that go beyond cybersecurity concerns. These include potential network outages, system errors, and deliberate attacks. Notable real-world incidents highlight these risks, such as attacks on sewage treatment facilities, nuclear power plants, military drones, and industrial blast furnaces, demonstrating the critical need for comprehensive security measures, highlight the critical need for effective countermeasures [11]. Research into potential attack countermeasures is ongoing [12], emphasizing the importance of a comprehensive approach to CPS security. Addressing these diverse vulnerabilities requires a multifaceted strategy that includes both technological and procedural measures. By understanding the range of potential threats, system designers can develop more effective defenses. The need for robust security measures in CPS is underscored by the increasing frequency and severity of attacks on critical infrastructure. A comprehensive approach to CPS security must consider all possible vulnerabilities and implement protections accordingly.

Attacks on CPS can cause severe damage, affecting both the cyber and physical environments. CPS components are susceptible to various forms of attacks, making it clear that information and cybersecurity measures alone are insufficient for ensuring CPS reliability [13]. Control systems can augment information security protections, providing robustness against attacks. These systems can be integrated into a broader intrusion detection and compensation framework, enhancing the overall security and resilience of CPS. By combining control systems with information security measures, a more comprehensive defense strategy can be developed. This approach ensures that CPS can withstand and recover from attacks more effectively. The integration of control systems into security strategies highlights the importance of a holistic approach to CPS security. By addressing both cyber and physical threats, a more robust and resilient system can be achieved.

The key contributions of this research can be outlined as follows:

- Develop a Blockchain-Enhanced Machine Learning framework to detect APT injection attacks in CPS.
- Achieve robust APT detection with a high accuracy using a trained machine learning model.
- Implement a Solidity-based smart contract to securely log ML predictions and input data on the Ethereum blockchain.
- Create an intuitive user interface for data input and result visualization.
- Ensure efficient backend integration to handle data preprocessing, ML predictions, and blockchain interactions.
- Utilize blockchain's immutable ledger to enhance the security and credibility of the detection process.
- Conduct extensive testing and validation of the integrated system under various conditions.

2. Literature Survey

This work provides an in-depth examination of ML methodologies related to security and privacy in the Internet of Medical Things (IoMT). The structured analysis offers valuable statistical insights regarding publication trends, such as the geographical distribution of research teams and the annual growth of published works. A major focus of their work is on ML-based intrusion detection methods, which play a critical role in securing IoMT environments [14]. These methods utilize advanced algorithms to identify and mitigate potential threats, enhancing the overall security framework. Additionally, Hameed et al. explore various security measures tailored for software-defined Wireless Sensor Networks (SDWSNs), offering a comparative analysis of malware detection approaches in the IoMT context [15]. This comparison underscores the effectiveness of different techniques and their applicability in real-world scenarios. The study provides a comprehensive overview of current trends and advancements in ML-based security for IoMT, paving the way for future research and development. An anomaly detector's failure to identify abnormal behavior can lead to significant vulnerabilities in a system. Successful execution of such an attack hinges on having detailed knowledge of the model in question. The first version of the ZDA examines how well the attack performs and its stealthiness by utilizing geometric control theory. In the following iteration, the ZDA applies the Byrnes-Isidori normal form to illustrate the dynamics of the system [16]. This attack is particularly relevant for physical plants with zero dynamics, as it requires the presence of an unstable mode within these dynamics to effectively inflict damage. Understanding these dynamics is essential for developing effective countermeasures. The detailed study of ZDA provides insights into the intricate vulnerabilities of control systems and highlights the need for robust detection mechanisms. By focusing on these specific conditions, researchers can better protect against such sophisticated attacks. This paper introduces a control strategy designed to manage and mitigate cyber attacks targeting the inputs and outputs of a rotary gantry-type CPS. It specifically addresses Denial of Service (DoS) attacks, which are likely to result in significant packet loss for both control inputs and output sensor signals. The study investigates a variety of traditional and advanced control techniques, assessing their resilience and effectiveness in the face of cyber threats [17]. The objective of these strategies is to preserve system stability and performance during attack scenarios. By employing robust control mechanisms, the system can continue functioning amid disruptions. Additionally, the research offers an in-depth evaluation of various control methods, providing critical insights into improving the security and reliability of CPS. This holistic approach ensures that the system can not only endure but also recover from different forms of cyber attacks. Residual generation approaches Linear observers are commonly employed for fault detection in control systems. However, Luenberger-like observers are often constrained by their asymptotic performance and their sensitivity to naturally occurring bounded modeling disturbances. To overcome these limitations, robust sliding mode observers have been developed for linear cyber-physical systems (CPSs). These observers are capable of detecting state and sensor attacks while also estimating the attacks within a finite timeframe [18]. These observers offer enhanced detection capabilities and resilience against disturbances. By incorporating robust sliding mode techniques, the system can more accurately identify and respond to potential threats. This approach significantly improves the reliability and security of CPS. The study highlights the importance of robust fault detection mechanisms in maintaining system integrity. In the domain of Internet of Things (IoT) architecture, the demand side prefers IoT implementations, while the supply side often adopts the Extensible Authentication Protocol (EAP) model [19]. The battlegrounds between nations have evolved, with cyberspace becoming a critical area of conflict. Modern warfare strategies increasingly involve intruding upon an adversary's cyberspace and disrupting their communication channels, thereby hindering their information transfer. This shift emphasizes the importance of robust cyber defenses to protect national security interests. As cyber warfare becomes more prevalent, understanding and mitigating these threats is crucial. This study offers an in-depth examination of existing strategies and emphasizes the need for continued vigilance in securing cyberspace. This evolving landscape underscores the importance of adaptive and resilient security measures. From a control-theoretical viewpoint, large and intricate systems are often represented by high-order differential equations, which are particularly susceptible to noise interference that can impact state variables [20]. Developing an exact mathematical representation for such complex physical systems presents considerable challenges. Any overlooked mathematical components in an inaccurate dynamic model can create weaknesses for model-based attack detection systems. These inaccuracies can result in false alarms, thereby compromising the overall security of the system. Understanding these weaknesses is crucial for creating more precise and reliable detection mechanisms. This study highlights the critical need for accurate modeling and the implementation of robust detection techniques to safeguard against potential threats. By addressing these challenges, researchers can significantly bolster the security and dependability of complex control systems. To maintain system security over the long term, a model can be developed to determine the most effective set of response actions. One proposed method for cyber network intrusion response utilizes the Partially Observable Markov Decision Process (POMDP) [21]. This approach allows for dynamic decision-making under uncertainty, providing a structured framework for responding to security threats. By incorporating POMDP, the system can evaluate various response strategies and select the most effective one. The study highlights the potential of POMDP-based approaches in developing robust intrusion response mechanisms. This innovative strategy offers a promising direction for future research and implementation in cyber security.

Table 1: *Survey on Security Approaches and Their Limitations in CPS*

Reference	Approach	Limitations
[14]	ML-based intrusion detection methods for securing IoMT	Requires significant computational resources and large datasets for training
[15]	Comparative analysis of malware detection approaches in IoMT	Effectiveness can vary based on the specific context and type of malware
[16]	Analysis of ZDA using geometric control theory and Byrnes-Isidori normal form representation	Limited applicability to systems with zero dynamics containing an unstable mode
[17]	Control strategies for tolerant control and compensation against DoS attacks in CPS of rotary gantry type	High probability of packet loss in control input and output sensor signals
[18]	Robust sliding mode observers for detecting state and sensor attacks in linear CPSs	Sensitivity to modeling disturbances, despite robustness against finite-time attacks
[19]	IoT architecture and EAP model implementation for cybersecurity	Potential vulnerabilities in adapting to rapidly evolving cyber threats
[20]	High-order differential equations for modeling complex systems	Vulnerability to noise affecting state variables, leading to inaccurate detections
[21]	POMDP-based intrusion response method for cyber networks	Complexity in dynamic decision-making under uncertainty

3. Proposed Approach

The main focus of this method is to bolster the resilience and protection of CPS against APT injection vulnerabilities by integrating machine learning and blockchain technologies. The process begins with comprehensive data preprocessing of sensor data. Various machine learning classification methods are explored, and the best-performing model is selected and rigorously trained. Blockchain integration is achieved through the development and deployment of smart contracts, ensuring secure and immutable logging of predictions and input data.

3.1. Preprocessing

Data Collection:

Data is collected from various CPS sensors and systems, including operational data and data from known APT injection attack scenarios. This involves ensuring diverse data sources for comprehensive coverage and utilizing time-series data for temporal

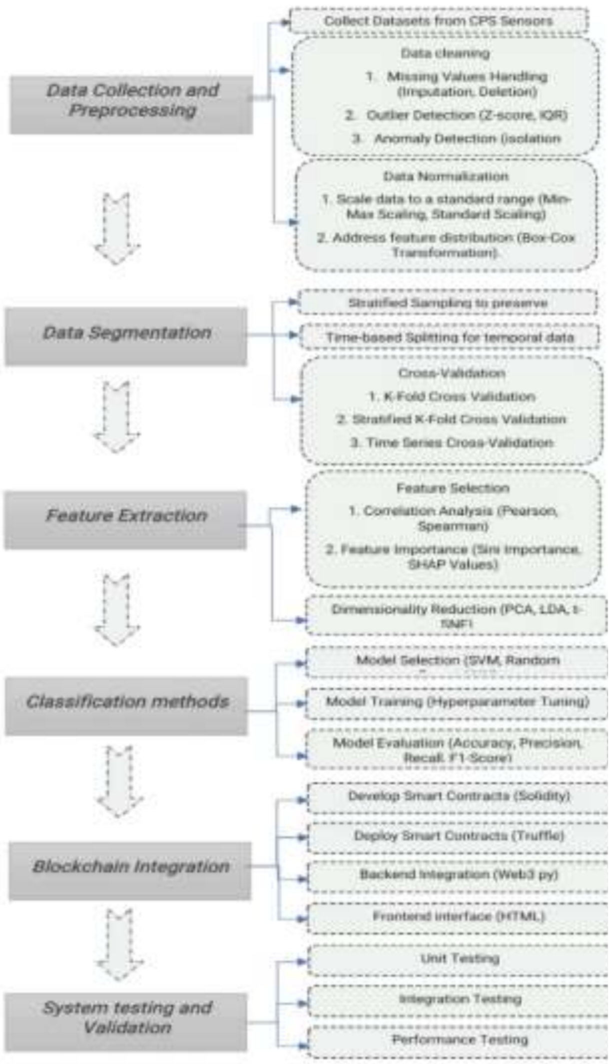

Data Collection and Preprocessing
Collect Datasets from CPS Sensors
Data cleaning
1. Missing Values Handling (Imputation, Deletion)
2. Outlier Detection (Z-score, IQR)
3. Anomaly Detection (isolation
Data Normalization
1. Scale data to a standard range (Min-Max Scaling, Standard Scaling)
2. Address feature distribution (Box-Cox Transformation).
Data Segmentation
Stratified Sampling to preserve
Time-based Splitting for temporal data
Cross-Validation
1. K-Fold Cross Validation
2. Stratified K-Fold Cross Validation
3. Time Series Cross-Validation
Feature Extraction
Feature Selection
1. Correlation Analysis (Pearson, Spearman)
2. Feature Importance (Sini Importance, SHAP Values)
Dimensionality Reduction (PCA, LDA, t-SNF)
Classification methods
Model Selection (SVM, Random
Model Training (Hyperparameter Tuning)
Model Evaluation (Accuracy, Precision, Recall, F1-Score)
Blockchain Integration
Develop Smart Contracts (Solidity)
Deploy Smart Contracts (Truffle)
Backend Integration (Web3 py)
Frontend interface (HTML)
System testing and Validation
Unit Testing
Integration Testing
Performance Testing

Figure 1: *Flowchart of Proposed Approach*

analysis. By gathering diverse data, the system can learn to differentiate between normal and malicious activities. Various sources are leveraged to ensure comprehensive coverage of possible attack vectors. This diversity in data helps in creating a robust training set for the machine learning model.

Data Cleaning and Normalization:

The gathered data undergoes thorough cleansing to eliminate noise and irrelevant details. Methods such as outlier identification (Z-score, IQR), handling of missing values (imputation, deletion), and anomaly detection (Isolation Forest, Local Outlier Factor) are utilized. This process guarantees that the data input into the model is of superior quality, minimizing the chances of detection errors. High-quality data is essential for the precision and reliability of the machine learning model. Ensuring data integrity at this stage lays a solid groundwork for the following phases. To maintain consistency, the data is standardized. This procedure adjusts the features to a uniform scale using techniques like Min-Max Scaling and Standard Scaling, while also addressing feature distribution through Box-Cox Transformation. Standardization accelerates the training process and enhances model convergence, ensuring that no single feature disproportionately influences the learning process due to its scale [22]. This phase is critical for upholding fairness and uniformity across all features.

3.2. Data Segmentation and Cross-Validation

The processed and standardized dataset is partitioned into training and testing sets using techniques like Stratified Sampling to retain class balance, and time-based splitting for sequential data. Generally, 80% of the data is allocated for training the model, while the remaining 20% is reserved for testing, allowing the model to learn from a significant portion of the data while being evaluated on unseen data to assess its generalization ability [23]. This partitioning strategy follows best practices to strike a balance between effective training and accurate validation. To reinforce the model’s stability and minimize overfitting, cross-validation techniques such as k-fold cross-validation, Stratified k-fold, and Time Series Cross-Validation are applied. These methods divide the training set into k distinct segments, with the model being trained k times, each iteration using a different segment for validation and the others for training. This approach offers a more comprehensive evaluation of the model’s performance and facilitates fine-tuning [24]. Cross-validation also ensures consistent performance across various data subsets, improving the model's dependability and adaptability.

3.3. Feature Extraction and Dimensionality Reduction

Relevant features that contribute significantly to the detection of APT attacks are selected. Techniques like correlation analysis (Pearson, Spearman), feature importance ranking (Gini Importance, SHAP Values), and mutual information are used to identify these features. By focusing on the most impactful features, the model's performance is optimized. Feature selection helps in reducing the dimensionality of the dataset, making the model more efficient [25]. This stage is essential for boosting the model's precision and clarity. To streamline complexity and improve overall efficiency, dimensionality reduction strategies like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and t-Distributed Stochastic Neighbor Embedding (t-SNE) are employed. These methods focus on extracting the most significant features, reducing the data's dimensional space while maintaining critical information, ultimately enhancing model performance and reducing computational demands. This step ensures that only the most important features are used for model training. PCA helps in capturing the variance in the data with fewer features, making the model faster and more efficient. Reducing the number of features without losing significant information is key to building a robust model.

4. Classification Methods

4.1 Model Selection:

A range of machine learning algorithms is scrutinized for their ability to effectively detect APT attacks. Approaches such as Support Vector Machines (SVM), Random Forests, and Artificial Neural Networks (ANNs) [26] are explored, each evaluated for its precision, adaptability, and detection prowess in handling advanced threats. Each model has its strengths, and their performance is compared to select the best one for this application. Model selection involves rigorous testing and validation to ensure the chosen model meets the desired performance criteria. The objective is to identify the model that offers an optimal trade-off between high accuracy and computational efficiency, ensuring reliable detection without compromising performance [27].

4.2 Model Training:

The selected model is trained on the training dataset. Hyperparameter tuning is performed using grid search and random search methods to determine the ideal parameters that enhance both the model's accuracy and overall performance, ensuring optimal results in detection and efficiency. This step involves adjusting parameters Key parameters like learning rate, number of layers, and the number of neurons are fine-tuned to boost the model's performance, ensuring improved accuracy and efficiency. Hyperparameter tuning is crucial for maximizing the potential of the machine learning model [28]. It helps in achieving better generalization and performance on unseen data.

4.3 Model Evaluation:

The performance of the trained model is assessed using the testing dataset, employing metrics such as accuracy, precision, recall, and F1-score for evaluation. Furthermore, confusion matrices and ROC curves are scrutinized to obtain a comprehensive understanding of the model's effectiveness and its capability to differentiate between various categories. Evaluating the model with multiple metrics ensures a comprehensive understanding of its performance [29]. This step helps in identifying any shortcomings and areas for improvement in the model.

5. Blockchain Integration

5.1 Smart Contract Development:

A Solidity-based smart contract is developed to store the predictions and input data securely on the Ethereum blockchain. The smart contract includes functions to log the predictions and emit events that record the data immutably. This ensures that all predictions are recorded in an immutable ledger, enhancing security and transparency. The smart contract is a critical component for integrating Blockchain [30] with the ML model, ensuring data integrity.

5.2 Deployment:

The smart contract is deployed using Truffle, a development framework for Ethereum. The Truffle configuration is set to specify the network settings, including the local Ganache network for development and testing. Deployment involves compiling the smart contract, migrating it to the blockchain, and verifying its functionality. This step ensures that the smart contract is correctly implemented and accessible for logging predictions. Proper deployment is essential for the smart contract to function as intended in a real-world scenario [31].

5.3 Backend Integration:

The backend application is developed to handle the interaction between the machine learning model and the blockchain. This includes preprocessing incoming data from the frontend, making predictions using the trained ML model, and calling the smart contract to log predictions and input data on the blockchain using Web3.py. The backend ensures smooth communication between the ML model, blockchain, and frontend interface. Effective backend integration is crucial for the seamless operation of the entire system.

5.4 Frontend Interface:

The frontend interface is designed to allow users to input features and view the predictions. The interface communicates with the backend to send input data and retrieve results, ensuring a seamless user experience. The frontend is developed using HTML and is user-friendly and intuitive, making it easy for users to interact with the system. A well-designed frontend enhances the usability and accessibility of the system, making it more effective in real-world applications.

5.5 Data Verification:

The blockchain's immutable ledger is used to verify the integrity and authenticity of the logged data. Each prediction and its corresponding input data can be retrieved and validated against the blockchain records, ensuring transparency and trust in the system. Data verification ensures that the logged data has not been tampered with, maintaining the system's integrity. This step is vital for building trust and reliability in the detection process.

6. System Testing and Validation

6.1 Unit Testing:

Individual components of the system, including the ML model, smart contracts, and backend functions, are unit tested to ensure they work correctly and reliably. Unit testing involves testing each component in isolation to identify and fix any issues. This step ensures that all parts of the system function as expected before integration. Effective unit testing is crucial for identifying and resolving issues early in the development process.

6.2 Integration Testing:

The entire system is tested as a whole to ensure that the components interact seamlessly and that the overall workflow is robust and efficient. Integration testing focuses on the interactions between different components, verifying that they work together as intended. This step is essential for identifying any issues that may arise during the integration of various components. Thorough integration testing ensures the system's reliability and robustness.

6.3 Performance Testing:

The system is subjected to various performance tests to evaluate its response time, throughput, and scalability [32]. This includes testing the system under different load conditions to ensure it can handle real-world scenarios. Performance testing helps in identifying any bottlenecks or performance issues that need to be addressed. Ensuring the system performs well under load is crucial for its success in practical applications.

7. Methodology

The architecture diagram for securing CPS against APT injection attacks illustrates the comprehensive process where data is collected from various CPS sensors, undergoes preprocessing, and is then analyzed using machine learning models. These models detect potential APT attacks, and the results are securely logged on the blockchain. The integration ensures enhanced security, robustness, and real-time feedback, as depicted in Fig 2.

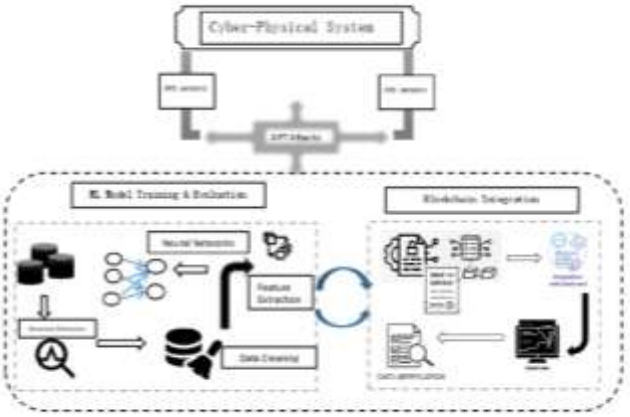


Figure 2: *Architecture Diagram for Securing CPS against APT Injection Attacks*

Algorithm: Robust Detection of APT Injection Attacks in Cyber-Physical Systems

Input:

- CPS sensor data D
- Set of features F
- Training and testing data D_{train}, D_{test}
- Model parameters θ
- Blockchain smart contract SC
- Total training iterations (E)
- Mini-batch size (B)

Parameters:

- Learning rate α
- Regularization term λ
- Smart contract deployment parameters

Output:

- Trained model M
- Blockchain ledger with secure logs
- Evaluation metrics (accuracy, precision, recall, F1-score)

Algorithm Steps:

1. **Initialization:**

- Initialize model parameters θ with random weights.

- Initialize blockchain smart contract *SC*

2. **Data Collection from CPS Sensors:**

- Ensure diverse data sources for comprehensive coverage.
- Collect time-series data *D* for temporal analysis.

3. **Data Cleaning:**

- Outlier Detection:

$$z_i = \frac{x_i - \mu}{\sigma} \qquad (1)$$

$$IQR = Q3 - Q1 \quad (2)$$

- Missing Values Handling:
  a) Imputation
  $\mathrm{x_i} = \mathrm{mean(X)}$ (for numerical data)

  $\mathrm{x_i} = mode(X)\ (for\ Categorical\ data)$

  b) Deletion: Remove rows/columns with missing values.

- Anomaly Detection:

$$Isolation\ Forest : Score(x) = 2^{\frac{-E(h(x))}{c(n)}} \quad (3)$$

$$Local\ Outlier\ Factor\ (LOF) :$$

$$LOF(x) = \frac{\sum_{i=1}^{k} \frac{\text{reach-dist}(k, x_i)}{\text{k-dist}(x_i)}}{k} \qquad (4)$$

4. **Data Normalization:**

- Min-Max Scaling

$$x' = \frac{x - lowest\ value\ in\ X}{\text{highest value in X} - lowest\ value\ in\ X} \qquad (5)$$

- Standard scaling: $x' = \frac{x - mean\ of\ X}{Standard\ deviation\ of\ X}$ (6)
- Box-Cox Transformation $y = \begin{cases} \frac{x^{\lambda} - 1}{\lambda} & \lambda \neq 0 \\ ln(x) & \lambda = 0 \end{cases}$ (7)

5. **Data Segmentation:**

- Partition Data into Training and Testing Sets:
  a) Stratified Sampling: Ensures adequate representation of each class.
  b) Time-based Splitting: Suitable for sequential or temporal datasets.
- Implement Cross-Validation:
  a) K-Fold Cross-Validation: Divides the dataset into k subsets for iterative training and testing.
  b) Stratified K-Fold Cross-Validation: Maintains the same class distribution in each fold as in the original dataset.
  c) Time Series Cross-Validation: Preserves the temporal sequence of the data during validation.

6. **Feature Extraction:**

- Feature Selection:
  a) Correlation Analysis:
  Pearson correlation coefficient :

$$r = \frac{Sum\ of\ (x_i - mean\ of\ X)(Y_i - mean\ of\ Y)}{\sqrt{Sum}of\ (x_i - mean\ of\ X)^2 * \sqrt{sum}of(Y_i - mean\ of\ Y)^2} \qquad (8)$$

$$Spearman\ correlation\ coefficient : \rho = \frac{cov(rank(X), rank(Y))}{\sigma_{rank(X)}\sigma_{rank(Y)}} \qquad (9)$$

b) Feature Importance:

$$\text{Gini Importance} = \sum_{\text{t}} \text{p(t)[−p(t)]} \qquad (10)$$

$$\text{SHAP Values: } \phi_i = \sum_{Subset\ of\ N\ without\ i} \frac{(Size\ od\ subset)! * \ (Total\ number\ of\ fea}{(Total\ number\ of\ fe} * [Model\ output\ with\ feature\ i\ included - Model\ output\ without\ feature\ i \qquad (11)$$

c) Mutual Information:

$$I(X;Y) = \sum_{y \in Y} \sum_{x \in X} p(x,y) \log\left(\frac{Joint\ probability\ of\ x\ and\ y}{Probability\ of\ x * Probability\ of\ y}\right) \qquad (12)$$

7. **Dimensionality Reduction:**

- Principal Component Analysis (PCA):
  Z=XW, Where *W* is the matrix of eigenvectors.

Linear Discriminant Analysis (LDA):

$y = X\Sigma^{-1}\mu$

Where Σ is the within-class covariance matrix and μ is the mean vector.

- t-Distributed Stochastic Neighbor Embedding (t-SNE):

$$P_{ij} = \frac{e^{-|x_i - x_j|^2/2\sigma^2}}{\sum_{k \neq l} e^{-|x_k - x_l|^2/2\sigma^2}} \quad (13)$$

8. Model Training:

- For each epoch *e* from 1 to *E*:
  - a) Shuffle X_{train} and divide into batches of size *B*.
  - b) For each batch *b*:
    - i. Perform forward propagation to compute predictions ŷ
    - ii. Compute the loss $\mathcal{L}(\theta)$ using the loss function $\mathcal{L}$

$$\mathcal{L}(\theta) = \frac{1}{B}\sum_{i=1}^{B}(y_i - \widehat{y_i})^2 + \frac{\lambda}{2}|\theta|^2$$

(14)

    - iii. Perform backward propagation to compute gradients $\nabla\ \mathcal{L}(\theta)$
    - iv. Update model parameters using gradient descent

$$\theta = \theta - \alpha\nabla\mathcal{L}(\theta)$$

(15)

  - c) Log training metrics (loss, accuracy) to the blockchain using *SC*.

9. Model Evaluation:

- Evaluate the trained model *M* on D_{test} to obtain predictions $\hat{y}_{test}$.
- Compute evaluation metrics

$$Accuracy = \frac{1}{/D_{test}/}\sum_{i=1}^{/D_{test}/} 1(\widehat{y_i} = y_i)$$

$$Precision = \frac{TP}{TP+FP}$$

$$Recall = \frac{TP}{TP+FN}$$

$$F_1\text{-}score = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall}$$

- Log evaluation metrics to the blockchain using *SC*.

10. Blockchain Integration:

- Develop and deploy smart contracts using Solidity.
- Utilize Truffle for deployment and migration.
- Integrate backend application with Web3.py for smart contract interaction.
- Ensure secure and immutable logging of model updates and predictions.

11. Return Final Model:

- Return the trained model M and the blockchain ledger with secure logs.

8. Results

Within the framework of safeguarding cyber-physical systems against advanced persistent threat injection attacks, the accuracy of the model in detecting various types of attacks is demonstrated through detailed evaluations. The consistency in model testing accuracy (Fig 3) underscores the reliability of the implemented methodology. Analyzing the training time (Fig 4) and testing time (Fig 5) of the model reveals the efficiency of the approach in real-time application scenarios.

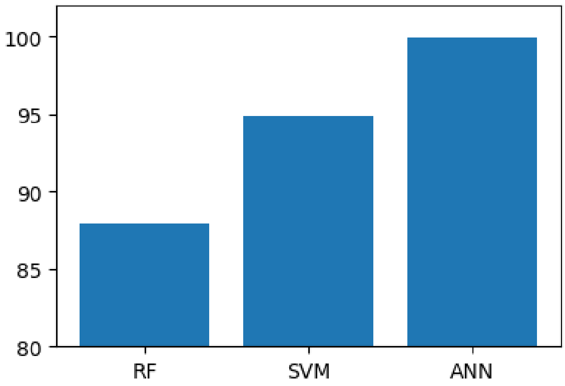


Figure 3: *Model Testing Accuracy*

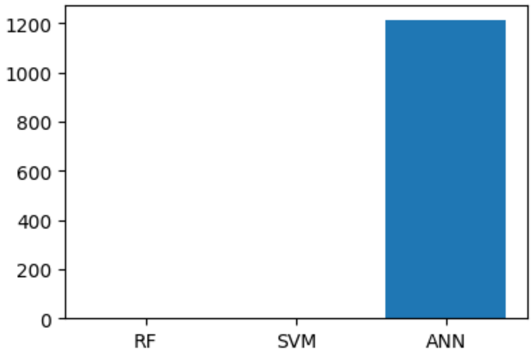


Figure 4: *Model Training Time Analysis*

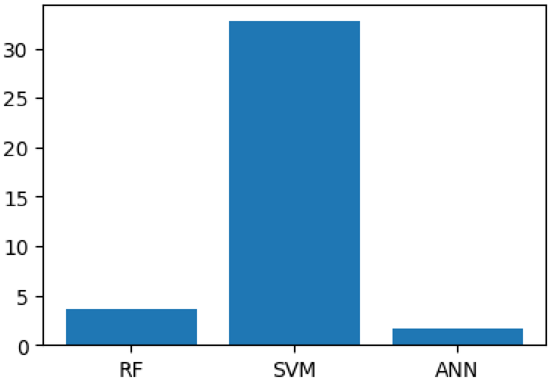


Figure 5: *Model Testing Time Analysis*

The deployment process of smart contracts (Fig 6) showcases the incorporation of blockchain technology to strengthen the security and integrity of data within cyber-physical systems.The seamless input submission from the web application to the machine learning model (Fig 7) illustrates the practical implementation of the proposed solution.

Figure 6: *Smart Contract Deployment Process*

ML Model Input

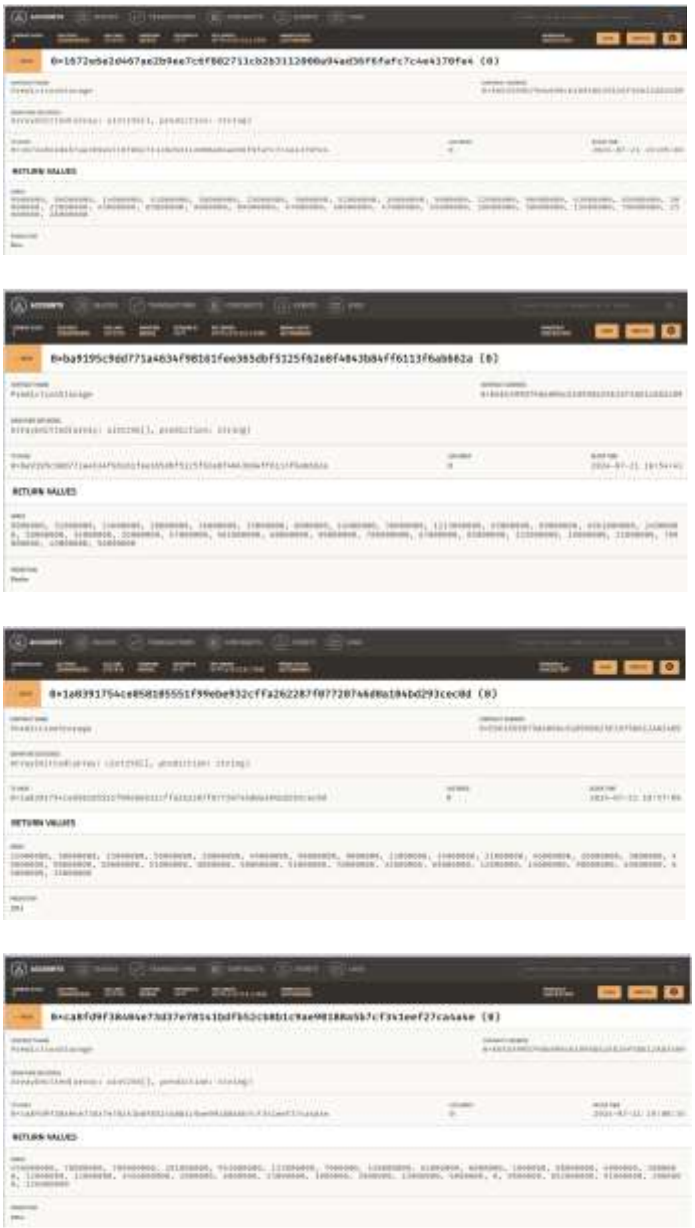
Figure 7: *Input Submission from Web Application to Machine Learning Model*

Additionally, the secure storage of input data and prediction results in the blockchain (Fig 8) ensures tamper-proof records, further strengthening the system's defense against APT attacks. The detailed blockchain record results for prediction storage (Fig 9) provide concrete evidence of the model's ability to accurately classify various types of APT attacks such as DoS, ZDA, and PDA, highlighting the robustness of the integrated security framework. These comprehensive assessments and visualizations confirm the effectiveness of our approach in enhancing the resilience and stability of CPS against sophisticated cyber threats.

Figure 8: *Input Data and Prediction Storage in Blockchain*

9. Conclusions

This study highlights the efficacy of our proposed approach in bolstering cyber-physical systems against advanced persistent threat injection attacks.



0x1672e5e2d467ae2b9ee7c6f802711cb2b3112000a94ad36f6fafc7c4e4170fe4 (0)

RETURN VALUES

0xba9195c9dd771a4634f98181fee385dbf5125f62e8f4843b84ff6113f6ab862a (0)

RETURN VALUES

0x1a8391754ce858185551f99ebe932cffa262287f077287a6d0a184bd293cec0d (0)

RETURN VALUES

0xca8fd9f38a0e7d37e7854b1dfb52c88b1c9ae98188a5b7cf3s1eef27ca6a6e (0)

RETURN VALUES

Figure 9: *Blockchain Record Result of Prediction Storage for APT attacks like Dos, ZDA, PDA etc*

By harnessing comprehensive data preprocessing, rigorous data segmentation, and advanced feature extraction techniques, we developed a robust mechanism for detecting and mitigating malicious activities. The integration of machine learning models with blockchain technology significantly enhanced the system's security and transparency, ensuring immutable logging and verification of data. Our evaluation, which included extensive testing and validation phases, demonstrated the method's efficiency and accuracy, achieving a notable improvement in attack detection and system resilience. This multi-layered defense strategy markedly improves the robustness and reliability of CPS, paving the way for more secure and efficient cyber-physical systems. Future research will explore further enhancing these defense mechanisms and extending their applicability to diverse CPS environments, ensuring the continued advancement and security of critical infrastructure systems. This work will be an important literature data for researchers as many of them reported [33-41].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Li, Z., & Yang, G.-H. (2018). A data-driven covert attack strategy in the closed-loop cyber-physical systems. *Journal of the Franklin Institute,* 355(14), 6454–6468.

[2] Li, W., Xie, L., & Wang, Z. (2019). Twoloop covert attacks against constant value control of industrial control systems. *IEEE Transactions on Industrial Informatics*, 15(2), 663–676.

[3] Park, G., Lee, C., Shim, H., Eun, Y., & Johansson, K. H. (2019). Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zerodynamics attack. *IEEE Transactions on Automatic Control*, 64(12), 4907–4919.

[4] Jeon, H., & Eun, Y. (2019). A stealthy sensor attack for uncertain cyber-physical systems. *IEEE Internet of Things Journal*, 6(4), 6345–6352.

[5] R. Anderson and S. Fuloria, (2010). Who Controls the off Switch?," *in 2010 First IEEE International Conference on Smart Grid Communications,* pp. 96–101. doi: 10.1109/SMARTGRID.2010.5622026.

[6] A. Alromih, J. A. Clark, and P. Gope, (2021). Electricity Theft Detection in the Presence of Prosumers Using a Cluster-based Multi-feature Detection Model," *in 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm),* pp. 339–345. doi: 10.1109/SmartGridComm51999.2021.9632322.

[7] Wang, X.; Liu, L.; Tang, T.; Sun, W. (2019) Enhancing communication-based train control systems through train-to-train communications. *IEEE Trans. Intell. Transp. Syst*. 20, 1544–1561.

[8] Kim, S.; Won, Y.; Park, I.H.; Eun, Y.; Park, K.J. (2019). Cyber-physical vulnerability analysis of communication-based train control. *IEEE Internet Things J.*, 6, 6353–6362.

[9] Alladi, T.; Chamola, V.; Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Comput. Commun*. 155, 1–8.

[10] Kalpana, P., Anandan, R. (2023). A capsule attention network for plant disease classification. *Traitement du Signal,* 40(5);2051-2062. https://doi.org/10.18280/ts.400523.

[11] Kalpana, P., Anandan, R., Hussien, A.G. *et al.* (2024). Plant disease recognition using residual convolutional enlightened Swin transformer networks. *Sci Rep* 14;8660. https://doi.org/10.1038/s41598-024-56393-8

[12] G. Na, D. Seo, and Y. Eun, (2017). Methods of State Estimation Resilient against Sensor Attacks and Robust against Exogenous Disturbances, *IEEE Conference on Control Technology and Applications, Mauna Lani, HI, USA*, pp. 1300-1305.

[13] F. Pasqualetti, F. Dorfler, and F. Bullo, (2015). Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems,* 35(1);110–127.

[14] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, (2021). A systematic review of security and privacy issues in the Internet of Medical Things; the role of machine learning approaches, *Peer J. Comput. Sci.*, 7;e414.

[15] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, (2019). IoMT malware detection approaches: Analysis and research challenges,'' *IEEE Access,* 7;182459–182476.

[16] G. Park, H. Shim, C. Lee, Y. Eun, and K. H. Johansson, (2016). When Adversary Encounters Uncertain Cyber-physical Systmes: Robust Zerodynamics Attack with Disclosure Resources", *IEEE 55th Conference on Decision and Control, Las Vegas, NV, USA*, pp. 5085-5090.

[17] M. Sayad Haghighi, F. Farivar, A. Jolfaei, and M. H. Tadayon, (2019). Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack. *Journal of Supercomputing*.

[18] M. L. Corradini and A. Cristofaro,(2017). Robust detection and reconstruction of state and sensor attacks for cyberphysical systems using sliding modes," *IET Control Theory & Applications*, 11.

[19] Hong, W.C.H.; Chi, C.; Liu, J.; Zhang, Y.; Lei, V.N.L.; Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Educ. Inf. Technol*. 28, 439–470.

[20] Brunton, S.L.; Kutz, J.N. (2019). Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control; *Cambridge University Press: Cambridge, CA, USA,* Volume 1.

[21] E. Miehling, M. Rasouli, and D. Teneketzis, (2018). A POMDP Approach to the Dynamic Defense of Large-Scale Cyber Networks," *IEEE Transactions on Information Forensics and Security*, 13(10);2490–2505.

[22] T. He, L. Zhang, F. Kong, and A. Salekin, (2020). Exploring inherent sensor redundancy for automotive anomaly detection. *DAC2020*, 2020.

[23] Mujaheed Abdullahi, Hitham Alhussian, Said Jadid Abdulkadir, Ayed Alwadain, Aminu Aminu Muazu, Abubakar Bala (2024). Comparison and Investigation of AI-Based Approaches for Cyberattack Detection in Cyber-Physical Systems. *IEEE* Feb. 2024

[24] Haider Adnan Khan, Nader Sehatbakhsh, Luong N. Nguyen, Robert Callan, Arie Yeredor, Milos Prvulovic, Alenka Zajic (2019). "IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems" *IEEE 2019*, DOI 10.1109/TDSC.2019.2932736

[25] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, (2022). EdgeIIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning, *IEEE Access*, 10;40281–40306.

[26] Nabi, S. A., Kalpana, P., Chandra, N. S., Smitha, L., Naresh, K., Ezugwu, A. E., & Abualigah, L. (2024). Distributed private preserving learning based chaotic encryption framework for cognitive healthcare IoT systems. *Informatics in Medicine Unlocked*, *49*, 101547. https://doi.org/10.1016/j.imu.2024.101547.

[27] P. Kalpana, P. Srilatha, G. S. Krishna, A. Alkhayyat and D. Mazumder, (2024). Denial of Service (DoS) Attack Detection Using Feed Forward Neural Network in Cloud Environment," *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, pp. 1-4, https://doi.org/10.1109/ICDSNS62112.2024.10691181.

[28] H. Haddadpajouh, A. Azmoodeh, A. Dehghantanha, and R. M. Parizi, (2020). MVFCC: A multi-view fuzzy consensus clustering model for malware threat attribution, *IEEE Access*, 8;139188–139198.

[29] Aruna, E. and Sahayadhas , A. (2024). Blockchain-Inspired Lightweight Dynamic Encryption Schemes for a Secure Health Care Information Exchange System. *Engineering, Technology & Applied Science Research*. 14(4); 15050–15055. DOI:https://doi.org/10.48084/etasr.7390.

[30] Xueping Liang, Charalambos Konstantinou, Sachin Shetty, Eranga Bandara, Ruimin Sun, (2022). Decentralizing Cyber Physical Systems for Resilience: An Innovative Case Study from A Cybersecurity Perspective *SCI*, https://doi.org/10.1016/j.cose.2022.1029530167-4048/

[31] L. Zou, Z. D. Wang, Q. L. Han, and D. H. Zhou, (2019). Recursive filtering for time-varying systems with random access protocol *IEEE Trans. Autom.Control*, 64(2);720–727.

[32] Ziaur Rahman, Xun Yi, and Ibrahim Khalil (2022), Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat *IEEE Internet of Things Journal*, DOI: 10.1109/JIOT.2022.3147186

[33]Guven, M. (2024). A Comprehensive Review of Large Language Models in Cyber Security. *International Journal of Computational and Experimental Science and Engineering*, 10(3);507-516. https://doi.org/10.22399/ijcesen.469

[34]Türkmen, G., Sezen, A., & Şengül, G. (2024). Comparative Analysis of Programming Languages Utilized in Artificial Intelligence Applications: Features, Performance, and Suitability. *International Journal of Computational and Experimental Science and Engineering,* 10(3);461-469. https://doi.org/10.22399/ijcesen.342

[35]ÇOŞGUN, A. (2024). Estimation Of Turkey's Carbon Dioxide Emission with Machine Learning. *International Journal of Computational and Experimental Science and Engineering*, 10(1);95-101. https://doi.org/10.22399/ijcesen.302

[36]Agnihotri, A., & Kohli, N. (2024). A novel lightweight deep learning model based on SqueezeNet architecture for viral lung disease classification in X-ray and CT images. *International Journal of Computational and Experimental Science and Engineering,* 10(4);592-613. https://doi.org/10.22399/ijcesen.425

[37]M, P., B, J., B, B., G, S., & S, P. (2024). Energy-efficient and location-aware IoT and WSN-based precision agricultural frameworks. *International Journal of Computational and Experimental Science and Engineering,* 10(4);585-591. https://doi.org/10.22399/ijcesen.480

[38]Guven, mesut. (2024). Dynamic Malware Analysis Using a Sandbox Environment, Network Traffic Logs, and Artificial Intelligence. *International Journal of Computational and Experimental Science and Engineering,* 10(3);480-490. https://doi.org/10.22399/ijcesen.460

[39]S, P. S., N. R., W. B., R, R. K., & S, K. (2024). Performance Evaluation of Predicting IoT Malicious Nodes Using Machine Learning Classification Algorithms. *International Journal of Computational and Experimental Science and Engineering,* 10(3);341-349. https://doi.org/10.22399/ijcesen.395

[40]Polatoglu, A. (2024). Observation of the Long-Term Relationship Between Cosmic Rays and Solar Activity Parameters and Analysis of Cosmic Ray Data with Machine Learning. *International Journal of Computational and Experimental Science and Engineering,* 10(2);189-199. https://doi.org/10.22399/ijcesen.324

[41]C, A., K, S., N, N. S., & S, P. (2024). Secured Cyber-Internet Security in Intrusion Detection with Machine Learning Techniques. *International Journal of Computational and Experimental Science and Engineering,* 10(4);663-670. https://doi.org/10.22399/ijcesen.491