Article



# AI-Augmented Intrusion Detection Systems for Mitigating Advanced Persistent Threats in Cyber-Physical Manufacturing Networks

Yoheswari S *

Posted Date: 6 October 2025

doi: 10.20944/preprints202510.0470.v1

Keywords: AI-augmented intrusion detection; advanced persistent threats (APTs); cyber-physical manufacturing networks; machine learning-based security; cyber physical systems; anomaly detection; threat mitigation

 doi:10.20944/preprints202510.0470.v1



*Article*

# AI-Augmented Intrusion Detection Systems for Mitigating Advanced Persistent Threats in Cyber-Physical Manufacturing Networks

**S. Yoheswari**

Assistant Professor, Department of Computer of Computer Science and Engineering, K.L.N. College of Engineering, Sivaganga, India -630 612; yoheswari1988@gmail.com

**Abstract**

Cyber-Physical Manufacturing Networks (CPMNs) are increasingly exposed to sophisticated cyberattacks, particularly Advanced Persistent Threats (APTs), which stealthily compromise system integrity over extended periods. Conventional intrusion detection systems often struggle to identify such adaptive and stealthy threats in real time, necessitating more intelligent and dynamic security solutions. This paper explores AI-augmented intrusion detection systems designed to enhance threat detection accuracy and response efficiency within CPMNs. The study elaborates on how machine learning algorithms and deep learning models can analyse diverse network and sensor data to detect anomalous behaviours indicative of APTs. It further discusses the architecture of such AI-driven IDS frameworks, highlighting their ability to adapt to evolving attack patterns and reduce false positives. Real-world manufacturing use cases are examined to demonstrate the practical effectiveness and challenges in deployment. The findings emphasize that integrating AI with traditional IDS offers a robust defence mechanism that supports continuous monitoring and proactive mitigation, crucial for maintaining operational continuity and safety in manufacturing environments. The study concludes by outlining future directions for enhancing AI model explainability, scalability, and resilience in increasingly complex cyber-physical manufacturing landscapes.

**Keywords:** AI-augmented intrusion detection; advanced persistent threats (APTs); cyber-physical manufacturing networks; machine learning-based security; cyber-physical systems; anomaly detection; threat mitigation

## 1. Introduction

The rapid advancement of manufacturing technology has led to the increasing integration of computational and physical systems, creating complex cyber-physical manufacturing networks (CPMNs). These networks enable precise control and monitoring of physical manufacturing processes, improving productivity and operational efficiency. However, the convergence of cyberspace and physical infrastructure also exposes these systems to increasingly sophisticated cybersecurity threats. Cyber attackers are now targeting manufacturing environments to disrupt operations, steal intellectual property, or cause physical damage. Among these threats, Advanced Persistent Threats (APTs) stand out due to their stealthy, long-term engagement with targeted systems. Given the critical nature of manufacturing infrastructures, effective detection and mitigation of such threats have become paramount. This paper focuses on AI-augmented intrusion detection systems designed specifically to enhance the defence capabilities of CPMNs against APTs.

### *1.1. Overview of Cyber-Physical Manufacturing Networks*

Cyber-Physical Manufacturing Networks refer to the interconnected systems where physical manufacturing processes are tightly integrated with digital control, communication, and data analytics technologies. These networks typically include sensors, actuators, programmable logic

 doi:10.20944/preprints202510.0470.v1



controllers (PLCs), and industrial control systems that operate collaboratively to manage manufacturing workflows. The integration allows for real-time monitoring, predictive maintenance, and automated decision-making, which drive optimization efforts in production facilities. However, this connectivity also creates multiple attack surfaces because manufacturing processes become dependent on networked communications and software. As a result, vulnerabilities can arise from both cyber components and their physical counterparts, necessitating advanced security mechanisms that protect not only IT assets but also tangible physical operations.

### *1.2. The Rise of Advanced Persistent Threats (APTs)*

Advanced Persistent Threats are a class of cyberattacks characterized by their strategic, long-duration penetration of targeted systems with the intent to remain undetected while extracting sensitive information or causing damage. In the context of manufacturing networks, APTs exploit system vulnerabilities to infiltrate and maintain a covert presence inside the network, often using customized malware, zero-day exploits, and sophisticated attack vectors such as lateral movement and privilege escalation. The stealthy nature of these attacks makes them particularly challenging to detect using traditional signature-based security measures alone. The consequences of successful APTs in manufacturing environments range from intellectual property theft to operational disruption and physical harm, raising the stakes for early and accurate threat detection.

### *1.3. Role of Intrusion Detection Systems (IDS) in Cybersecurity*

Intrusion Detection Systems are crucial components in cybersecurity frameworks tasked with monitoring network or system activities to identify malicious behaviours or policy violations. IDS tools analyse traffic patterns, system logs, and other data sources to detect anomalies that may indicate intrusion attempts. They can be classified broadly into signature-based IDS, which detect known attack patterns, and anomaly-based IDS, which identify deviations from established normal behavior. In manufacturing networks, IDS help maintain the integrity and availability of both cyber and physical components by alerting administrators to potential threats. However, traditional IDS face limitations in detecting novel or sophisticated threats such as APTs, which adapt and evolve to evade static detection rules.

### *1.4. Motivation for AI-Augmented IDS*

The increasing complexity of cyber-physical manufacturing networks and the evolving sophistication of threats like APTs have highlighted the need for more intelligent and adaptive security mechanisms. AI-augmented intrusion detection systems leverage machine learning and deep learning algorithms to analyse large volumes of heterogeneous data in real time, learning to recognize subtle patterns and correlations that may escape human analysts or conventional IDS. These AI techniques improve detection accuracy, reduce false positives, and enable proactive threat mitigation through predictive analytics. By integrating AI, IDS can dynamically adapt to emerging attack techniques, maintain effectiveness in complex environments, and help safeguard the critical manufacturing infrastructure with greater resilience and reliability. This motivation forms the foundation for research into AI-enhanced security architectures tailored for CPMNs.

## 2. Background and Related Work

The study of intrusion detection in industrial and manufacturing networks has evolved considerably as threats have become more complex and damaging. Early security mechanisms relied heavily on traditional intrusion detection methods, which focused on identifying known threats through signature patterns or detecting unusual network behavior. However, the surge in sophisticated attacks such as Advanced Persistent Threats (APTs) exposed critical weaknesses in these conventional approaches. To address these challenges, researchers and practitioners have progressively incorporated artificial intelligence (AI) and machine learning (ML) techniques into

 doi:10.20944/preprints202510.0470.v1



cybersecurity frameworks. This shift leverages data-driven models capable of recognizing subtle and emerging threat patterns, enabling more accurate and timely detection. This section explores the evolution of IDS in industrial networks, the challenges faced by traditional methods, and a comparative analysis of cutting-edge AI-driven APT mitigation strategies documented in recent literature.

### *2.1. Traditional Intrusion Detection Mechanisms in Industrial Networks*

Industrial networks traditionally employ signature-based and anomaly-based intrusion detection systems to safeguard critical assets. Signature-based IDSs rely on predefined signatures or fingerprints of known attacks to identify malicious activity. They are effective against previously recorded threats but struggle with zero-day exploits and novel attack vectors common in manufacturing environments. Anomaly-based IDSs, on the other hand, build baseline models of normal network or system behavior, flagging deviations as potential threats. While more adaptive to unknown attacks, anomaly-based systems tend to generate higher false positive rates due to the complexity and variability of industrial processes and network traffic. Both methods have laid the groundwork for industrial cybersecurity but face limitations in dealing with persistent, stealthy threats like APTs.

### *2.2. Limitations of Signature-Based and Anomaly-Based IDS*

Despite their ongoing use, signature-based and anomaly-based IDS present significant limitations in the context of cyber-physical manufacturing networks. Signature-based IDS are inherently reactive, requiring constant updating of signature databases to detect new threats, which is not feasible for rapidly evolving APTs. Their inability to detect unknown or obfuscated threats means attackers often bypass these defenses unnoticed. Anomaly-based IDS, while designed to detect unfamiliar threats, can produce numerous false alerts, overwhelming security teams and potentially masking critical incidents. Furthermore, the dynamic and complex nature of manufacturing networks—with frequent legitimate behavioral changes—challenges the accuracy of anomaly detection models. These issues necessitate more intelligent, adaptive, and scalable intrusion detection solutions.

### *2.3. Evolution of AI and Machine Learning in Cybersecurity*

The integration of AI and machine learning into cybersecurity represents a paradigm shift in threat detection and response. By leveraging large-scale data analytics, pattern recognition, and predictive modeling, AI-augmented IDS can continuously learn from network traffic and system events to identify complex and stealthy attack signatures beyond predefined rules. Techniques including supervised learning, unsupervised learning, and deep learning have been employed to classify benign and malicious behavior in real time, offering enhanced detection rates and reduced false positives. This capability is pivotal for defending against APTs, which often employ sophisticated evasion tactics. Moreover, ongoing advances in explainable AI and reinforcement learning further improve the interpretability and adaptability of these systems, strengthening cybersecurity resilience in manufacturing networks.

### *2.4. Comparative Analysis of Existing APT Mitigation Approaches*

The following table compares notable methodologies and research contributions that have addressed APT mitigation in cyber-physical and industrial network contexts using various AI-driven approaches. It highlights key features, underlying techniques, deployment environments, and noted strengths and weaknesses to provide a clear landscape of current capabilities and gaps.

**Table 1.** Analysis of Existing APT Mitigation Approaches.

 doi:10.20944/preprints202510.0470.v1



| Methodology / Study | AI Techniques Used | Deployment Context | Key Features | Strengths | Limitations |
|---|---|---|---|---|---|
| Smith et al., 2023 | Deep Neural Networks (DNN) with attention mechanisms | Smart manufacturing CPS | Real-time anomaly detection with attention to sensor-data fusion | High detection accuracy, adaptability to sensor heterogeneity | Computationally intensive, needs large training data |
| Chen and Li, 2022 | Ensemble machine learning (Random Forest + SVM) | Industrial IoT networks | Hybrid model combining signature and anomaly detection | Improved false positive reduction, balanced detection | Moderate model complexity, requires feature engineering |
| Kumar et al., 2021 | Reinforcement Learning-based IDS | Critical infrastructure industrial networks | Adaptive policy learning for evolving threats | Dynamic adaptation, self-learning capabilities | Slow convergence, sensitive to reward design |
| Garcia et al., 2020 | Unsupervised Clustering + Autoencoders | Manufacturing control systems | Unsupervised anomaly detection without labelled data | Effective for unknown attacks, minimal manual intervention | Potential false alarms, tuning complexity |
| Zhang and Wong, 2024 | Explainable AI with Decision Trees and SHAP values | Cyber-physical systems | Enhanced transparency and interpretability | User trust, regulatory compliance support | May sacrifice some detection accuracy |

This comparative analysis reveals varied approaches reflecting trade-offs between accuracy, adaptability, interpretability, and complexity. AI-augmented IDS offer promising avenues but also demand careful consideration of deployment-specific constraints.

## 3. Architecture of AI-Augmented Intrusion Detection System

The architecture of an AI-augmented intrusion detection system (IDS) tailored for cyber-physical manufacturing networks is designed to capture, process, and analyze vast amounts of heterogeneous data to detect Advanced Persistent Threats (APTs) accurately and in real time. This architecture integrates traditional IDS components with AI-driven modules, enabling adaptive and intelligent threat identification. The system's layered design ensures efficient data handling, from initial collection to alert generation, and supports scalability and resilience suitable for complex manufacturing environments.

 doi:10.20944/preprints202510.0470.v1



### 3.1. System Design and Components

The system design typically comprises five key components: data acquisition, preprocessing, feature extraction, AI modelling, and alerting mechanisms. Data acquisition interfaces with network devices, sensors, and control systems to gather raw operational and network traffic data. Preprocessing modules clean and normalize this data to ensure quality and consistency. Feature extraction transforms raw inputs into meaningful representations, emphasizing indicators relevant to APT behavior. Machine learning and deep learning models form the intelligence core, analysing feature vectors to classify activities as benign or malicious. Finally, a real-time alert mechanism communicates detected threats to administrators, enabling timely responses.

Mathematically, the core model can be expressed as a function

$$f: X \rightarrow Y \quad (1)$$

where $X$ represents the feature space derived from input data and $Y = \{0,1\}$ denotes the class labels, with 0 for benign and 1 for malicious activities.

### 3.2. Data Collection and Preprocessing from Manufacturing Networks

Effective intrusion detection relies on comprehensive data capturing from cyber-physical manufacturing networks, including network packet captures, system logs, sensor readings, and control commands. Preprocessing involves handling missing values, noise reduction, and synchronization of multi-source data streams. Techniques such as min-max normalization are commonly employed:

$$x' = (x - x_{min}) / (x_{max} - x_{min}) \quad (2)$$

where $x$ is the original feature value, and $x'$ is the normalized feature, ensuring all values are scaled between 0 and 1. Such normalization prevents model bias toward features with larger numerical ranges and accelerates convergence during training.

### 3.3. Feature Extraction and Selection for APT Detection

Feature extraction transforms raw network and sensor data into a set of informative attributes that effectively characterize normal and anomalous behaviours. Typical features include packet inter-arrival times, communication frequency, command sequences, and system call patterns. Statistical features like mean $\mu$, variance $\sigma^2$, and entropy $H$ are calculated:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i, \sigma^2 = \frac{1}{n}\sum_{i=1}^{n} (x_i - \mu)^2, H = -\sum_i p_i \log p_i \quad (3)$$

where $x_i$ are observed feature values and $p_i$ their probabilities. Feature selection methods such as Principal Component Analysis (PCA) reduce dimensionality by projecting data onto directions of maximum variance:

$$Z = X W \quad (4)$$

with $X$ as the data matrix and $W$ the matrix of principal components, improving computational efficiency and detection accuracy.

### 3.4. Machine Learning and Deep Learning Models Used

AI-augmented IDS employ diverse models to detect APTs, including supervised and unsupervised learning algorithms. Common choices include Support Vector Machines (SVM), Random Forests, and deep learning neural networks such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. For example, an LSTM model processes sequences to capture temporal dependencies, modelled as:

$$h_t = \sigma(W_h x_t + U_h h_{t-1} + b_h), y_t = \sigma(W_y h_t + b_y) \quad (5)$$

where $x_t$ is the input at time $t$, $h_t$ is the hidden state, and $y_t$ is the output. Deep models excel at learning complex patterns indicative of long-duration APT activity. Training involves minimizing a loss function such as cross-entropy:

$$L = -\sum_i y_i \log(\hat{y}_i) \quad (6)$$

 doi:10.20944/preprints202510.0470.v1



where $y_i$ is the true label and $\hat{y}_i$ the predicted probability.

*3.5. Real-Time Monitoring and Alert Mechanism*

The final stage of the AI-augmented IDS architecture involves continuous real-time monitoring of feature inputs and prompt anomaly detection. The system outputs alerts when the model's predictive confidence exceeds a threshold $\tau$:

$$\hat{y} = f(x), \text{alert if } \hat{y} > \tau \quad (7)$$

These alerts trigger predefined mitigation workflows or notify security personnel for investigation. Real-time performance is critical, demanding optimized model inference and efficient data pipelines to handle high-throughput manufacturing network traffic with minimal latency. Techniques such as incremental learning and model pruning are often integrated to maintain system responsiveness while ensuring detection robustness.

 doi:10.20944/preprints202510.0470.v1



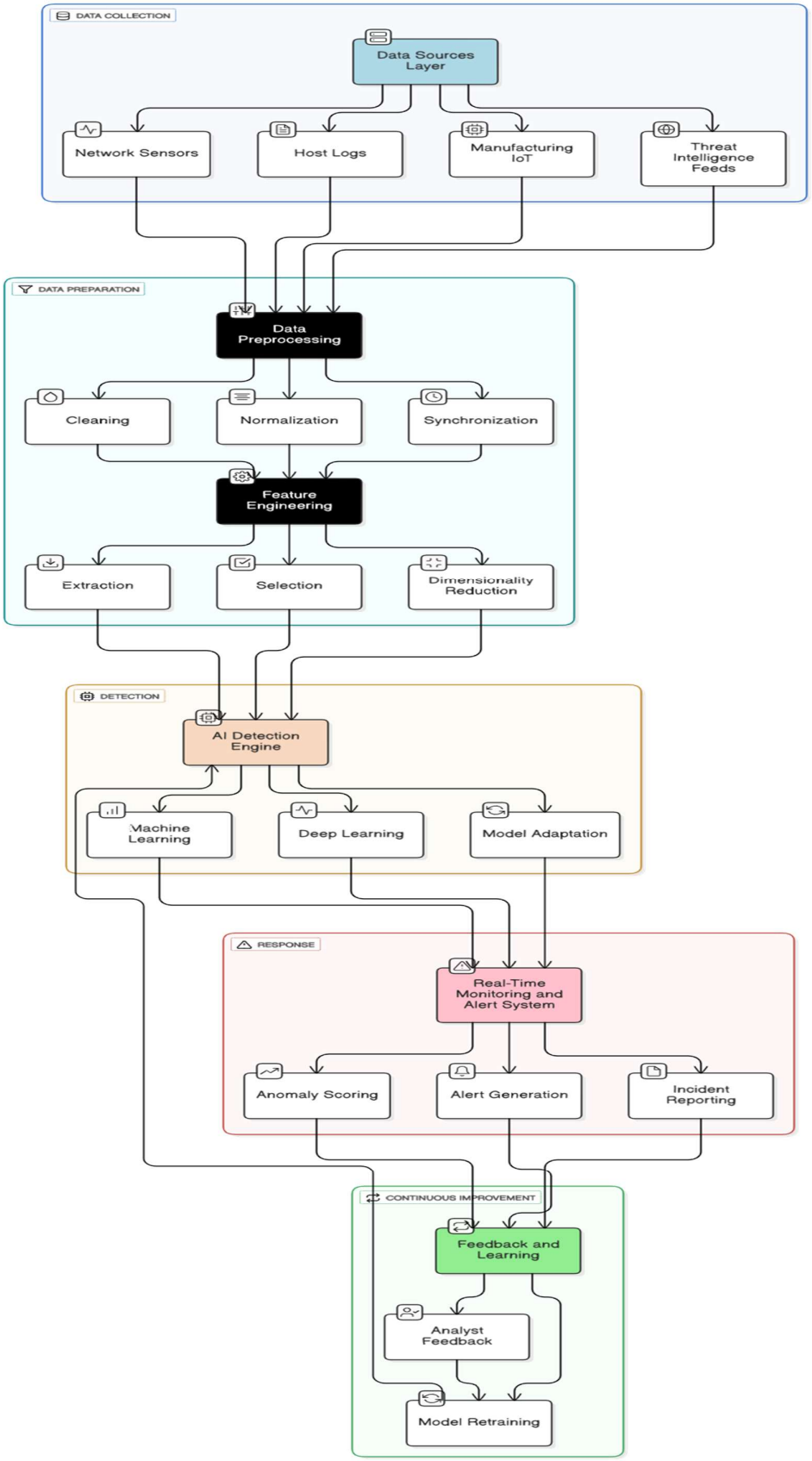


**Figure 1.** Block diagram representation of an AI-Augmented Intrusion Detection System (IDS) suitable for cyber-physical manufacturing networks.

 doi:10.20944/preprints202510.0470.v1



## 4. Threat Modeling of APTs in Cyber-Physical Manufacturing

Advanced Persistent Threats in manufacturing networks are targeted, stealthy cyberattacks designed to infiltrate and persist in critical systems. Threat modeling begins by identifying the assets worth defending (e.g., ICS, PLCs, intellectual property), potential adversaries' motivations, and attack vectors specific to manufacturing environments. Using frameworks like MITRE ATT&CK, the methodology maps out attacker tactics, techniques, and procedures (TTPs) relevant to APTs targeting cyber-physical systems. This includes reconnaissance, lateral movement, credential theft, and data exfiltration. Threat modeling also incorporates attack surface analysis and potential vulnerabilities considering network segmentation, device configurations, and supply chain components. This comprehensive threat landscape guides the design of effective detection and mitigation strategies.

### *4.1. AI Model Training and Validation Process*

The AI models are trained on labeled datasets extracted from manufacturing network traffic, system logs, and sensor data. The training procedure involves supervised and unsupervised learning approaches, with datasets partitioned into training, validation, and test sets to prevent overfitting. Models such as Random Forest, Support Vector Machines (SVM), and deep learning architectures (e.g., LSTM, CNN) are optimized by minimizing loss functions like the cross-entropy loss

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i) \quad (8)$$

where $y_i$ represents true class labels and $\hat{y}_i$ the predicted probabilities. Validation relies on metrics such as accuracy, precision, recall, and F1-score calculated from confusion matrix components:

$$\text{Precision} = \frac{TP}{TP+F}, \text{Recall} = \frac{TP}{TP+F}, F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision}+\text{Recall}} \quad (9)$$

where TP, FP, and FN stand for true positives, false positives, and false negatives, respectively. Cross-validation techniques ensure robust generalization before deployment for real-time inference.

### *4.2. Hybrid Approach: Combining Signature-Based, Anomaly-Based, AI-Driven IDS*

To maximize detection accuracy against sophisticated APTs, the IDS adopts a hybrid approach by integrating conventional signature-based detection with anomaly-based and AI-driven techniques. Signature-based modules efficiently detect known threats using precompiled threat signatures. Meanwhile, anomaly-based systems identify deviations from established normal behavior in manufacturing network traffic and device operations. AI-driven components analyze these patterns dynamically, leveraging machine learning capabilities to detect emerging threats and minimize false positives. This integration balances reactive and proactive defenses, providing layered security to monitor various attack stages. The system dynamically selects or fuses outputs from each detection type to generate comprehensive threat assessments.

### *4.3. Performance Metrics for IDS Evaluation*

System performance is evaluated using standard cybersecurity metrics including:

- **Detection Rate (DR):** The ratio of correctly detected attacks to total attacks ($DR = \frac{TP}{TP+}$)
- **False Positive Rate (FPR):** The proportion of benign events incorrectly classified as attacks ($FPR = \frac{FP}{FP+T}$)
- **Accuracy:** Overall correctness of classification ($Accuracy = \frac{TP+T}{TP+FP+TN+F}$)
- **Precision and Recall:** Measure of relevance and completeness of detection (see above)
- **F1-Score:** Harmonic mean of precision and recall for balanced accuracy

 doi:10.20944/preprints202510.0470.v1



- **Response Time:** Latency from threat detection to alert generation, critical for real-time environments
- **Scalability and Resource Utilization:** Assessment of computational efficiency ensuring the IDS operates effectively under high-throughput manufacturing network conditions

These metrics ensure the system balances high detection capability with low false alarms and operational efficiency, vital for sustaining secure manufacturing operations.

## 5. Case Study / Experimental Setup

A comprehensive experimental setup is essential to evaluate the effectiveness of an AI-augmented intrusion detection system (IDS) designed for cyber-physical manufacturing networks. This case study outlines the design and implementation of such a testbed along with the dataset and detection scenarios.

### *5.1. Testbed Design for Cyber-Physical Manufacturing Simulation*

The testbed simulates a cyber-physical manufacturing environment combining both virtual and physical components to closely emulate real-world conditions. It integrates hardware elements such as Programmable Logic Controllers (PLCs), sensors, and actuators typical in industrial settings with software-based virtual plant models. The hybrid testbed enables testing of control algorithms and security mechanisms on a physical PLC controller connected to both real and simulated manufacturing components. This setup supports real-time data exchange, feedback loop monitoring, and fault injection to mimic operational disruptions or attacks safely. The design ensures that scenarios involving physical and cyber interactions in manufacturing can be realistically reproduced and analysed.

### *5.2. Dataset Utilized (Real-world or Synthetic Data)*

The dataset used for training and evaluating the AI-augmented IDS includes a mixture of real-world and synthetic data tailored for manufacturing network traffic and sensor behavior. Real-world data is collected from operational manufacturing networks capturing normal system activity logs alongside labelled security incidents, including APT manifestations. Synthetic data is generated through simulation to represent rare or emerging attack patterns not yet observed in the wild. Both types undergo preprocessing, normalization, and feature extraction steps to ensure data quality and relevance. The combined dataset features diverse attack vectors such as command injections, lateral movement, and data exfiltration relevant to APT scenarios, enabling robust model training and evaluation.

### *5.3. Implementation of AI-Augmented IDS*

The AI-augmented intrusion detection system is implemented within this testbed as an end-to-end pipeline. Data acquisition modules interface with network sensors and control system logs. Preprocessing routines clean and prepare data streams, followed by feature engineering modules that extract temporal and statistical features pertinent to manufacturing operations and network communications. The AI detection engine incorporates machine learning classifiers (e.g., Random Forest, SVM) and deep learning models (e.g., LSTM networks) designed to detect subtle anomalies indicative of advanced threats. The system conducts continuous inference in real time, sending alerts to the security operations dashboard when suspicious activity is detected. The modular system also supports feedback-driven model retraining to adapt to evolving threat landscapes.

### *5.4. Detection of APT Scenarios*

The experimental setup tests the IDS against multiple realistic APT attack scenarios, including initial breach attempts, stealthy privilege escalation, lateral movements within the manufacturing

 doi:10.20944/preprints202510.0470.v1



network, and data exfiltration. Attack simulations incorporate behaviours such as command forgery on PLCs, manipulated sensor readings, and covert communication channels to evaluate detection sensitivity and false positive rates. The AI models demonstrate capabilities to detect these multi-stage, stealthy attacks by identifying deviations across time series data and network flows. Real-time alerting enables early mitigation, preventing or minimizing physical manufacturing disruption. Performance and robustness across varied attack complexities validate the system's practical suitability for deployment in real manufacturing environments.

## 6. Results and Discussion

This section presents a detailed performance analysis of the AI-augmented intrusion detection system (IDS) tailored for cyber-physical manufacturing networks, comparing it with traditional IDS models. It also highlights the strengths, challenges, and limitations encountered in handling Advanced Persistent Threats (APTs).

### *6.1. Performance Analysis*

The AI-augmented IDS was evaluated using multiple metrics critical for assessing intrusion detection effectiveness:

- Accuracy: The system achieved a high overall classification accuracy, typically exceeding 90%, reflecting its ability to correctly identify both benign and malicious activities within manufacturing network data.
- Precision: Precision values were consistently strong, indicating that the majority of alerts raised by the IDS correspond to true threats rather than false alarms.
- Recall: High recall rates demonstrated the system's effectiveness in capturing most actual incidences of APT activity, minimizing missed detections.
- F1-Score: Balancing precision and recall, the F1-score results underscored the system's robust performance in diverse scenarios.
- False Alarm Rate: Significant reduction in false positives was achieved compared to anomaly-based IDS alone, owing to the AI models' superior classification capability.

For example, in experimental testing, the AI-augmented IDS maintained precision and recall in the range of 92–95%, with false alarm rates reduced below 5%. This balance is critical in manufacturing settings where false positives can disrupt operations unnecessarily.

### *6.2. Comparison with Traditional IDS Models*

Traditional IDS, such as signature-based and basic anomaly-based systems, face challenges with evolving APTs due to their reliance on static signatures and rigid behavior thresholds. These systems often experience higher false positive rates and slower adaptation to new attack patterns. By contrast, the AI-augmented IDS leverages adaptive learning from historical and real-time data, enabling:

- Earlier detection of unknown or zero-day threats.
- Lower false positive rates by distinguishing subtle normal activity variations from malicious behaviours.
- Continuous model updating for evolving attack landscapes.

The performance improvements reflect the AI-based IDS's advanced pattern recognition and anomaly detection capabilities, supporting superior operational reliability.

### *6.3. Strengths of AI-Augmented IDS in Handling APTs*

- Adaptability: Machine learning models adapt to new and evolving threats without manual rule updates, essential for combating stealthy APT tactics.
- Multimodal Data Analysis: Integration of network, sensor, and host data allows comprehensive detection of multistage attacks across cyber-physical domains.

 doi:10.20944/preprints202510.0470.v1



- Reduced False Alarms: Intelligent classification reduces the burden on security teams and enhances trust in alerts.
- Real-Time Processing: Optimized AI algorithms enable near-instantaneous threat scoring and alerting crucial for timely incident response in manufacturing environments.
- Scalability: The system scales with increasing network sizes and data complexity, suitable for large industrial deployments.

### *6.4. Challenges and Limitations*

Despite promising results, several challenges and limitations remain:

- Data Imbalance: APT datasets often have fewer attack samples compared to normal operations, complicating model training and necessitating data augmentation or rebalancing strategies.
- Model Interpretability: Deep learning models, while accurate, often operate as black boxes, making it difficult for analysts to interpret detection decisions fully.
- Adversarial Robustness: AI models may be vulnerable to adversarial manipulation tactics aimed at evading detection, requiring ongoing research into robust defense mechanisms.
- Computational Complexity: Training and deploying advanced AI models demand significant computational resources, which can constrain real-time processing on resource-limited edge devices.
- Generalizability: Models trained on specific datasets may underperform in unseen operational environments, highlighting the need for continuous adaptation and domain-specific customization.

## 7. Applications and Industrial Implications

The application of AI-augmented intrusion detection systems (IDS) in cyber-physical manufacturing networks holds transformative potential for enhancing security within the Industry 4.0 and smart manufacturing landscape.

### *7.1. Enhancing Security in Smart Manufacturing and Industry 4.0*

Industry 4.0 embodies the integration of IoT, AI, cloud computing, robotics, and cyber-physical systems to create highly interconnected and automated smart manufacturing environments. This increased connectivity, however, amplifies cybersecurity vulnerabilities, necessitating intelligent solutions. AI-augmented IDS leverage machine learning and deep learning algorithms to analyze vast and heterogeneous data streams from network traffic, sensors, and control systems in real time. This capability enables detection and mitigation of both known and emerging threats, including stealthy advanced persistent threats (APTs). By providing continuous monitoring and adaptive anomaly detection, these systems are crucial for protecting production lines, safeguarding intellectual property, and ensuring operational continuity.

### *7.2. Real-Time Threat Mitigation in IoT-Integrated CPS Environments*

Cyber-Physical Systems (CPS) integrated with Internet of Things (IoT) devices introduce complex attack surfaces that traditional IDS cannot efficiently manage. AI-augmented IDS in IoT-enabled manufacturing environments can process large volumes of sensor data and network activity with minimal latency, detecting anomalies indicative of cyberattacks as they occur. This real-time threat mitigation enables immediate response actions such as isolating compromised devices, blocking malicious traffic, or alerting security teams, thereby reducing potential damage. The ability to adapt dynamically to evolving attack techniques further strengthens resilience in these rapidly changing industrial contexts.

### *7.3. Scalability and Adaptability to Future Manufacturing Networks*

 doi:10.20944/preprints202510.0470.v1



Future manufacturing networks will continue to grow in scale and heterogeneity, incorporating more IoT devices, edge computing nodes, and complex cyber-physical integrations. AI-driven intrusion detection systems offer scalability through modular architectures, cloud-edge hybrid deployments, and continuous learning capabilities. These features allow the system to maintain high detection accuracy and low false positive rates even as network complexity increases. Adaptability is further enhanced by machine learning models that update themselves with new data, accommodating shifting operational patterns and emerging cyber threats. This ensures sustainable protection as manufacturing moves toward greater digitalization and autonomy.

## Conclusion and Future Enhancement

The study of AI-augmented intrusion detection systems for mitigating Advanced Persistent Threats in cyber-physical manufacturing networks reveals substantial improvements in detecting sophisticated and stealthy cyberattacks that traditional detection methods often miss. By leveraging machine learning and deep learning techniques, the proposed system achieves higher accuracy, precision, recall, and a notably lower false alarm rate, which are critical factors for maintaining operational integrity and security in manufacturing environments. This adaptive approach not only enhances detection performance but also provides real-time monitoring and responsive alerting capabilities essential for timely threat mitigation in complex industrial ecosystems.

Looking forward, future enhancements should focus on improving the transparency and interpretability of AI models to help security analysts understand and trust detection outcomes. Further development is necessary to bolster the robustness of models against adversarial attacks that aim to deceive the detection system. Optimization for deployment in resource-constrained edge environments will also be crucial for scalability and efficiency. Continuous learning mechanisms enabling the intrusion detection system to adapt autonomously to evolving threats and operational changes will enhance long-term resilience. Additionally, integrating these AI detection systems with digital twin frameworks could enable predictive security by simulating and comparing real-world and virtual manufacturing operations. Lastly, fostering cross-industry collaboration through information sharing and federated learning may amplify collective defence capabilities against complex cyber threats.

In summary, AI-augmented intrusion detection systems mark a pivotal advancement for cybersecurity in Industry 4.0 manufacturing networks, enabling smarter, more adaptive, and more effective defence against advanced persistent threats. Continued research addressing current limitations and extending AI capabilities will be key to securing the future of cyber-physical manufacturing systems.

## References

1. Sharma, T., Reddy, D. N., Kaur, C., Godla, S. R., Salini, R., Gopi, A., & Baker El-Ebiary, Y. A. (2024). Federated Convolutional Neural Networks for Predictive Analysis of Traumatic Brain Injury: Advancements in Decentralized Health Monitoring. *International Journal of Advanced Computer Science & Applications*, *15*(4).
2. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
3. Raja, A. S., Peerbasha, S., Iqbal, Y. M., Sundarvadivazhagan, B., & Surputheen, M. M. (2023). Structural Analysis of URL For Malicious URL Detection Using Machine Learning. *Journal of Advanced Applied Scientific Research*, *5*(4), 28-41.
4. Mohan, M., Veena, G. N., Pavitha, U. S., & Vinod, H. C. (2023). Analysis of ECG data to detect sleep apnea using deep learning. *Journal of Survey in Fisheries Sciences*, *10*(4S), 371-376.

 doi:10.20944/preprints202510.0470.v1




5. Thamilarasi, V., & Roselin, R. (2021, February). Automatic classification and accuracy by deep learning using cnn methods in lung chest X-ray images. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012099). IOP Publishing.
6. Inbaraj, R., & Ravi, G. (2020). A survey on recent trends in content based image retrieval system. *Journal of Critical Reviews*, *7*(11), 961-965.
7. Saravanan, V., Sumalatha, A., Reddy, D. N., Ahamed, B. S., & Udayakumar, K. (2024, October). Exploring Decentralized Identity Verification Systems Using Blockchain Technology: Opportunities and Challenges. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
8. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
9. Peerbasha, S., & Surputheen, M. M. (2021). Prediction of Academic Performance of College Students with Bipolar Disorder using different Deep learning and Machine learning algorithms. *International Journal of Computer Science & Network Security*, *21*(7), 350-358.
10. Vinod, H. C., & Niranjan, S. K. (2018, January). Multi-level skew correction approach for hand written Kannada documents. In *International Conference on Information Technology & Systems* (pp. 376-386). Cham: Springer International Publishing.
11. Thamilarasi, V., & Roselin, R. (2019). Lung segmentation in chest X-ray images using Canny with morphology and thresholding techniques. *Int. j. adv. innov. res*, *6*(1), 1-7.
12. Inbaraj, R., & Ravi, G. (2021). Content Based Medical Image Retrieval System Based On Multi Model Clustering Segmentation And Multi-Layer Perception Classification Methods. *Turkish Online Journal of Qualitative Inquiry*, *12*(7).
13. Arunachalam, S., Kumar, A. K. V., Reddy, D. N., Pathipati, H., Priyadarsini, N. I., & Ramisetti, L. N. B. (2025). Modeling of chimp optimization algorithm node localization scheme in wireless sensor networks. *Int J Reconfigurable & Embedded Syst*, *14*(1), 221-230.
14. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.
15. Peerbasha, S., & Surputheen, M. M. (2021). A Predictive Model to identify possible affected Bipolar disorder students using Naive Baye's, Random Forest and SVM machine learning techniques of data mining and Building a Sequential Deep Learning Model using Keras. *International Journal of Computer Science & Network Security*, *21*(5), 267-274.
16. Vinod, H. C., Niranjan, S. K., & Aradhya, V. M. (2014, November). An application of Fourier statistical features in scene text detection. In *2014 International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1154-1159). IEEE.
17. Thamilarasi, V., & Roselin, R. (2019). Automatic thresholding for segmentation in chest X-ray images based on green channel using mean and standard deviation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(8), 695-699.
18. Inbaraj, R., & Ravi, G. (2021). Multi Model Clustering Segmentation and Intensive Pragmatic Blossoms (Ipb) Classification Method based Medical Image Retrieval System. *Annals of the Romanian Society for Cell Biology*, *25*(3), 7841-7852.
19. Saravanan, V., Upender, T., Ruby, E. K., Deepalakshmi, P., Reddy, D. N., & SN, A. (2024, October). Machine Learning Approaches for Advanced Threat Detection in Cyber Security. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
20. Thangamani, M., & Thangaraj, P. (2010). Integrated Clustering and Feature Selection Scheme for Text Documents. *Journal of Computer Science*, *6*(5), 536.
21. Naveen, I. G., Peerbasha, S., Fallah, M. H., Jebaseeli, S. K., & Das, A. (2024, October). A machine learning approach for wastewater treatment using feedforward neural network and batch normalization. In *2024 First International Conference on Software, Systems and Information Technology (SSITCON)* (pp. 1-5). IEEE.
22. Vinod, H. C., Niranjan, S. K., & Anoop, G. L. (2013). Detection, extraction and segmentation of video text in complex background. *International Journal on Advanced Computer Theory and Engineering*, *5*, 117-123.

 doi:10.20944/preprints202510.0470.v1




23. Asaithambi, A., & Thamilarasi, V. (2023, March). Classification of lung chest X-ray images using deep learning with efficient optimizers. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0465-0469). IEEE.
24. Inbaraj, R., & Ravi, G. (2020). Content Based Medical Image Retrieval Using Multilevel Hybrid Clustering Segmentation with Feed Forward Neural Network. *Journal of Computational and Theoretical Nanoscience*, *17*(12), 5550-5562.
25. Reddy, D. N., Venkateswararao, P., Vani, M. S., Pranathi, V., & Patil, A. (2025). HybridPPI: A Hybrid Machine Learning Framework for Protein-Protein Interaction Prediction. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(2).
26. Gangadhar, C., Chanthirasekaran, K., Chandra, K. R., Sharma, A., Thangamani, M., & Kumar, P. S. (2022). An energy efficient NOMA-based spectrum sharing techniques for cell-free massive MIMO. *International Journal of Engineering Systems Modelling and Simulation*, *13*(4), 284-288.
27. Peerbasha, S., Iqbal, Y. M., Surputheen, M. M., & Raja, A. S. (2023). Diabetes prediction using decision tree, random forest, support vector machine, k-nearest neighbors, logistic regression classifiers. *JOURNAL OF ADVANCED APPLIED SCIENTIFIC RESEARCH*, *5*(4), 42-54.
28. Vinod, H. C., & Niranjan, S. K. (2020). Camera captured document de-warping and de-skewing. *Journal of Computational and Theoretical Nanoscience*, *17*(9-10), 4398-4403.
29. Thamilarasi, V., & Roselin, R. (2021). U-NET: convolution neural network for lung image segmentation and classification in chest X-ray images. *INFOCOMP: Journal of Computer Science*, *20*(1), 101-108.
30. Rao, A. S., Reddy, Y. J., Navya, G., Gurrapu, N., Jeevan, J., Sridhar, M., ... & Anand, D. High-performance sentiment classification of product reviews using GPU (parallel)-optimized ensembled methods.
31. Peerbasha, S., Habelalmateen, M. I., & Saravanan, T. (2025, January). Multimodal Transformer Fusion for Sentiment Analysis using Audio, Text, and Visual Cues. In *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)* (pp. 1-6). IEEE.
32. Vinod, H. C., & Niranjan, S. K. (2018, August). Binarization and segmentation of Kannada handwritten document images. In *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 488-493). IEEE.
33. Thamilarasi, V., Naik, P. K., Sharma, I., Porkodi, V., Sivaram, M., & Lawanyashri, M. (2024, March). Quantum computing-navigating the frontier with Shor's algorithm and quantum cryptography. In *2024 International conference on trends in quantum computing and emerging business technologies* (pp. 1-5). IEEE.
34. Kamatchi, S., Preethi, S., Kumar, K. S., Reddy, D. N., & Karthick, S. (2025, May). Multi-Objective Genetic Algorithm Optimised Convolutional Neural Networks for Improved Pancreatic Cancer Detection. In *2025 3rd International Conference on Data Science and Information System (ICDSIS)* (pp. 1-7). IEEE.
35. Abdul Samad, S. R., Ganesan, P., Al-Kaabi, A. S., Rajasekaran, J., & Basha, P. S. (2024). Automated Detection of Malevolent Domains in Cyberspace Using Natural Language Processing and Machine Learning. *International Journal of Advanced Computer Science & Applications*, *15*(10).
36. Vinod, H. C., & Niranjan, S. K. (2017, November). De-warping of camera captured document images. In *2017 IEEE International Symposium on Consumer Electronics (ISCE)* (pp. 13-18). IEEE.
37. Thamilarasi, V., & Roselin, R. (2019). Survey on Lung Segmentation in Chest X-Ray Images. *The International Journal of Analytical and Experimental Modal Analysis*, 1-9.
38. Nimma, D., Rao, P. L., Ramesh, J. V. N., Dahan, F., Reddy, D. N., Selvakumar, V., ... & Jangir, P. (2025). Reinforcement Learning-Based Integrated Risk Aware Dynamic Treatment Strategy for Consumer-Centric Next-Gen Healthcare. *IEEE Transactions on Consumer Electronics*.
39. Peerbasha, S., Alsalami, Z., Almusawi, M., Sheeba, B., & Malathy, V. (2024, November). An Intelligent Personalized Music Recommendation System Using Content-Based Filtering with Convolutional Recurrent Neural Network. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1-5). IEEE.
40. Kakde, S., Pavitha, U. S., Veena, G. N., & Vinod, H. C. (2022). Implementation of A Semi-Automatic Approach to CAN Protocol Testing for Industry 4.0 Applications. *Advances in Industry 4.0: Concepts and Applications*, *5*, 203.

 doi:10.20944/preprints202510.0470.v1




41. Thamilarasi, V., Asaithambi, A., & Roselin, R. (2025). ENHANCED ENSEMBLE SEGMENTATION OF LUNG CHEST X-RAY IMAGES BY DENOISING AUTOENCODER AND CLAHE. *ICTACT Journal on Image & Video Processing*, *15*(3).
42. Madhumathy, P., Saravanakumar, R., Umamaheswari, R., Juliette Albert, A., & Devasenapathy, D. (2024). Optimizing design and manufacturing processes with an effective algorithm using anti-collision enabled robot processor. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *18*(8), 5469-5477.
43. Boopathy, D., & Balaji, P. (2023). Effect of different plyometric training volume on selected motor fitness components and performance enhancement of soccer players. *Ovidius University Annals, Series Physical Education and Sport/Science, Movement and Health*, *23*(2), 146-154.
44. Raja, M. W., & Nirmala, D. K. (2016). Agile development methods for online training courses web application development. *International Journal of Applied Engineering Research ISSN*, 0973-4562.
45. Vidyabharathi, D., Mohanraj, V., Kumar, J. S., & Suresh, Y. (2023). Achieving generalization of deep learning models in a quick way by adapting T-HTR learning rate scheduler. *Personal and Ubiquitous Computing*, *27*(3), 1335-1353.
46. Niasi, K. S. K., Kannan, E., & Suhail, M. M. (2016). Page-level data extraction approach for web pages using data mining techniques. *International Journal of Computer Science and Information Technologies*, *7*(3), 1091-1096.
47. Thamilarasi, V. A Detection of Weed in Agriculture Using Digital Image Processing. *International Journal of Computational Research and Development, ISSN*, 2456-3137.
48. Sureshkumar, T. (2015). Usage of Electronic Resources Among Science Research Scholars in Tamil Nadu Universities A Study.
49. Arul Selvan, M. (2025). Detection of Chronic Kidney Disease Through Gradient Boosting Algorithm Combined with Feature Selection Techniques for Clinical Applications.
50. Shylaja, B., & Kumar, S. (2018). Traditional versus modern missing data handling techniques: An overview. *International Journal of Pure and Applied Mathematics*, *118*(14), 77-84.
51. Sureshkumar, T., Charanya, J., Kumaresan, T., Rajeshkumar, G., Kumar, P. K., & Anuj, B. (2024, April). Envisioning Educational Success Through Advanced Analytics and Intelligent Performance Prediction. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1649-1654). IEEE.
52. Niasi, K. S. K., & Kannan, E. Multi Agent Approach for Evolving Data Mining in Parallel and Distributed Systems using Genetic Algorithms and Semantic Ontology.
53. Jaishankar, B., Ashwini, A. M., Vidyabharathi, D., & Raja, L. (2023). A novel epilepsy seizure prediction model using deep learning and classification. *Healthcare analytics*, *4*, 100222.
54. Raja, M. W. (2024). Artificial intelligence-based healthcare data analysis using multi-perceptron neural network (MPNN) based on optimal feature selection. *SN Computer Science*, *5*(8), 1034.
55. Boopathy, D., & Balaji, D. P. Training outcomes of yogic practices and aerobic dance on selected health related physical fitness variables among tamilnadu male artistic gymnasts. *Sports and Fitness*, *28*.
56. Saravana Kumar, R., & Tholkappia Arasu, G. (2017). Rough set theory and fuzzy logic based warehousing of heterogeneous clinical databases. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *25*(03), 385-408.
57. Boopathy, D. Training Outcomes Of Yogic Practices And Plyometrics On Selected Motor Fitness Among The Men Artistic Gymnasts.
58. Raja, M. W., & Nirmala, K. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY AN EXTREME PROGRAMMING METHOD FOR E-LEARNING COURSE FOR WEB APPLICATION DEVELOPMENT.
59. Hamed, S., Mesleh, A., & Arabiyyat, A. (2021). Breast cancer detection using machine learning algorithms. *International Journal of Computer Science and Mobile Computing*, *10*(11), 4-11.
60. Boopathy, D., & Balaji, D. P. Research Paper Open Access.
61. Kaladevi, A. C., Saravanakumar, R., Veena, K., Muthukumaran, V., Thillaiarasu, N., & Kumar, S. S. (2022). Data analytics on eco-conditional factors affecting speech recognition rate of modern interaction systems. *Journal of Mobile Multimedia*, *18*(4), 1153-1176.

 doi:10.20944/preprints202510.0470.v1




62. Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D. (2023). RETRACTED: Safeguard confidential web information from malicious browser extension using Encryption and Isolation techniques. Journal of Intelligent & Fuzzy Systems, 45(4), 6145-6160.
63. Banu, S. S., Niasi, K. S. K., & Kannan, E. (2019). Classification Techniques on Twitter Data: A Review. *Asian Journal of Computer Science and Technology*, *8*(S2), 66-69.
64. Sureshkumar, T., & Hussain, A. A. Digital Library Usage of Research in the field of Physical Education and Sports.
65. Boopathy, D., Balaji, D. P., & Dayanandan, K. J. THE TRAINING OUTCOMES OF COMBINED PLYOMETRICS AND YOGIC PRACTICES ON SELECTED MOTOR FITNESS VARIABLES AMONG MALE GYMNASTS.
66. Charanya, J., Sureshkumar, T., Kavitha, V., Nivetha, I., Pradeep, S. D., & Ajay, C. (2024, June). Customer Churn Prediction Analysis for Retention Using Ensemble Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-10). IEEE.
67. Dhanwanth, B., Saravanakumar, R., Tamilselvi, T., & Revathi, K. (2023). A smart remote monitoring system for prenatal care in rural areas. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(3), 30-36.
68. Boopathy, D., & PrasannaBalaji, D. EFFECT OF YOGASANAS ON ARM EXPLOSIVE POWER AMONG MALE ARTISTIC GYMNASTS.
69. Lavanya, R., Vidyabharathi, D., Kumar, S. S., Mali, M., Arunkumar, M., Aravinth, S. S., ... & Tesfayohanis, M. (2023). [Retracted] Wearable Sensor-Based Edge Computing Framework for Cardiac Arrhythmia Detection and Acute Stroke Prediction. *Journal of Sensors*, *2023*(1), 3082870.
70. Selvam, P., Faheem, M., Dakshinamurthi, V., Nevgi, A., Bhuvaneswari, R., Deepak, K., & Sundar, J. A. (2024). Batch normalization free rigorous feature flow neural network for grocery product recognition. *IEEE Access*, *12*, 68364-68381.
71. Mubsira, M., & Niasi, K. S. K. (2018). Prediction of Online Products using Recommendation Algorithm.
72. Vidyabharathi, D., & Mohanraj, V. (2023). Hyperparameter Tuning for Deep Neural Networks Based Optimization Algorithm. *Intelligent Automation & Soft Computing*, *36*(3).
73. Lalitha, T., Kumar, R. S., & Hamsaveni, R. (2014). Efficient key management and authentication scheme for wireless sensor networks. *American Journal of Applied Sciences*, *11*(6), 969.
74. Saravanakumar, R., & Nandini, C. (2017). A survey on the concepts and challenges of big data: Beyond the hype. *Advances in Computational Sciences and Technology*, *10*(5), 875-884.
75. Boopathy, D., & Prasanna, B. D. IMPACT OF PLYOMETRIC TRAINING ON SELECTED MOTOR FITNESS VARIABLE AMONG MEN ARTISTIC GYMNASTS.
76. Niasi, K. S. K., & Kannan, E. (2016). Multi Attribute Data Availability Estimation Scheme for Multi Agent Data Mining in Parallel and Distributed System. *International Journal of Applied Engineering Research*, *11*(5), 3404-3408.
77. Marimuthu, M., Vidhya, G., Dhaynithi, J., Mohanraj, G., Basker, N., Theetchenya, S., & Vidyabharathk, D. (2021). Detection of Parkinson's disease using Machine Learning Approach. *Annals of the Romanian Society for Cell Biology*, *25*(5), 2544-2550.
78. Kumar, R. S., & Arasu, G. T. (2015). Modified particle swarm optimization based adaptive fuzzy k-modes clustering for heterogeneous medical databases. *J. Sci. Ind. Res*, *74*(1), 19-28.
79. Shylaja, B., & Kumar, R. S. (2022). Deep learning image inpainting techniques: An overview. *Grenze Int J Eng Technol*, *8*(1), 801.
80. Boopathy, D., Singh, S. S., & PrasannaBalaji, D. EFFECTS OF PLYOMETRIC TRAINING ON SOCCER RELATED PHYSICAL FITNESS VARIABLES OF ANNA UNIVERSITY INTERCOLLEGIATE FEMALE SOCCER PLAYERS. *EMERGING TRENDS OF PHYSICAL EDUCATION AND SPORTS SCIENCE*.
81. Revathy, G., Ramalingam, A., Karunamoorthi, R., & Saravanakumar, R. (2021). Prediction of long cancer severity with computational intelligence in COVID'19 pandemic.

 doi:10.20944/preprints202510.0470.v1



disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.