AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

Secure Cyber-Physical Systems in Industry 4.0 Using Advanced Parallel Deep Learning Orchestration Techniques

Mrs K. SWATHI[1], M. ANUPAMA[2]

[1]Assistant Professor Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences Anantapur-515721

[2]PG Scholar, Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences Anantapur- 515721

Abstract: The rapid advancement of Industry 4.0 has led to the development of smart manufacturing systems where interconnected machines, sensors, and control units operate through cyber-physical systems (CPS). Despite improving efficiency and automation, this connectivity exposes industrial environments to sophisticated cyber threats that can disrupt operations and damage equipment. To address these challenges, this work proposes a robust CPS security framework that integrates a hybrid Long Short-Term Memory and Convolutional Neural Network (LSTM-CNN) model with a Parallel Orchestration (PLO) mechanism. The CNN component extracts spatial features from command data and sensor inputs, while the LSTM captures temporal dependencies from sequential machine-state information. This hybrid approach enables accurate detection of anomalous patterns caused by cyber-attacks. The PLO mechanism enhances system performance by simultaneously analyzing multiple data streams, including network traffic, control commands, and time-series signals, thereby reducing detection latency. The proposed model is evaluated using standard performance metrics such as accuracy, precision, recall, and F1-score, demonstrating superior detection capability and reliability. Experimental results show that the model achieves high accuracy with improved precision and F1-score, indicating effective identification of both normal and malicious activities. The framework ensures early threat detection, minimizes false positives, and enhances operational safety. Additionally, it provides scalability and adaptability for evolving industrial environments.

Key Words: Industry 4.0, Cyber-Physical Systems, LSTM-CNN, Parallel Orchestration, Anomaly Detection.

1. Introduction

The advancement of IoT, artificial intelligence (AI), cloud computing, robotics, and automation has fuelled the growth of Industry 4.0. Different sectors have rapidly embraced these technologies due to their efficiency, productivity, flexibility, and data-driven decision-making. However, these benefits come with significant security concerns. Early adopters such as Epsilon, Equifax, Marriott International, Colonial Pipeline, and T-Mobile suffered business losses of billions due to cyber-attacks. The autonomous manufacturing industry is

particularly vulnerable, with statistics showing that 25% of all cyber-attacks in 2023 targeted manufacturing. This paper presents an innovative cyber-physical system (CPS) security method for manufacturing that automatically detects intrusions from text and images, maintains procedural sequences, and reduces production delays. The CPS security system is designed for a simulated Industry 4.0-based RMG manufacturing environment using Arena software, where autonomous units operate with image and text data. A hybrid LSTM-CNN model with a Parallel Orchestration Algorithm (PLO) ensures intrusion detection from both data types, achieving over 90% accuracy, precision, recall, and F1-score. The system significantly reduces production delays from 116 hours to 5 hours annually, improving efficiency and saving 169 product units per year. The core contributions of this research are listed below:

- **Parallel Orchestration Algorithm (PLO):** the PLO algorithm developed in this paper maintains a perfect harmony between the LSTM network and CNN, ensuring protection against intrusion from both image and non-image data.
- **Classification Accuracy:** the CPS security layer detects intrusion from image and non-image data with 90.85% and 91.66% accuracy, respectively. The average precision, recall, and F1-score are above 90% as well.
- **Reducing Production Delay:** the most significant contribution of the proposed security system is reducing the average production delay caused by intrusions from 116 hours to 5 hours per year. It saves 169 units of product yearly.

•**Revenue Savings:** the computational analysis shows that the proposed security system helps save $30,474 worth of revenue per year on average, when six manufacturing units run at their full capacity.

The proposed system achieves significant annual revenue savings of approximately $30,474 under full-capacity operation. By integrating LSTM and CNN through the PLO algorithm, it enables fast and accurate real-time intrusion detection, enhancing security, reliability, and operational efficiency in Industry 4.0 environments.

2. Literature Survey

The literature reviews on CPSs conducted by Pivoto et al. [10], Oks et al. [11], and Lampropoulos et al. [12] suggest that cyber security is one of the most significant concerns of Industry 4.0. The IoT is at the heart of autonomous manufacturing units, facilitating communication with the units over the Internet. However, because of their resource-constrained nature, IoT devices are unsuitable for embedded sophisticated security features [13]. Research and development to integrate additional security layers is necessary, as has been carried out in this paper.

Li et al. [14] applied federated deep learning for intrusion detection in CPS. Their approach combines a CNN and a gated recurrent unit (GRU), which is similar to the proposed methodology. However, their study is limited to exploring the classification performance, whereas the proposed system explores the real-world effects of the security system. O'Donovan et

al. [15] proposed a fog computing-based security system using machine learning (ML) for a CPS. This innovative approach leaves a significant weakness, whereby the system can be affected by network intrusion because the security features run on the cloud. The proposed system is a security layer just above the hardware level, which ensures maximum security of the CPS production units. A support vector machines (SVM)-based approach proposed by Sharma et al. [16] detects vulnerabilities in a CPS. However, it doesn't provide any mechanism to resume the production process; this has been developed in the proposed paper.

3. System Architecture

The system architecture begins with a preprocessed phishing URL dataset, followed by Canopy feature selection to reduce irrelevant attributes.

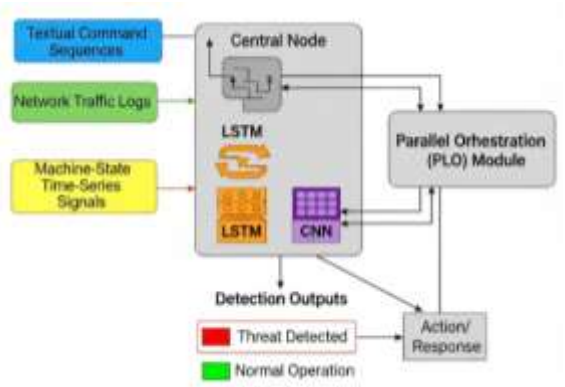


Fig 1: System Architecture

Cross-validation splits data into 70% training and 30% testing sets. Grid search optimizes hyper parameters, and an ensemble model combining LR, SVC, and DT is trained to generate accurate phishing predictions.

4.Methodology

The proposed CPS security framework is designed to protect Industry 4.0 manufacturing environments from cyber intrusions using a hybrid LSTM–CNN architecture integrated with a Parallel Orchestration (PLO) mechanism. The methodology begins with data acquisition from simulated smart manufacturing units.

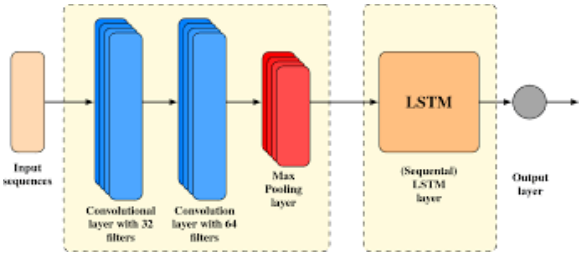


Fig 2: Proposed Methodology

The system collects data from a simulated Industry 4.0 RMG manufacturing setup using Arena software, incorporating image, text, and sensor data from autonomous units. After Pre-processing a hybrid CNN–LSTM model extracts spatial and temporal features for intrusion detection. The Parallel Orchestration mechanism enables simultaneous analysis of all data streams, reducing detection latency and improving system responsiveness. During construction, supervised learning was employed to train the hybrid model. The CNN and LSTM layers were optimized using back propagation, with cross-entropy loss guiding classification accuracy. Regularization techniques were applied to prevent over fitting. The trained model was then integrated into the CPS environment as a security layer, capable of real-time monitoring and anomaly detection.

5. Design and Construction

The design of the proposed CPS security system integrates a hybrid Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) model, orchestrated through a Parallel Orchestration (PLO) mechanism. The architecture was

constructed to simultaneously analyze textual command sequences, image data, and machine-state signals, ensuring comprehensive intrusion detection in Industry 4.0 manufacturing environments.

i)Data Collection Module

This module gathers real-time data from CPS devices, including sensors, robots, and network nodes, capturing both physical and communication parameters. The collected data forms the basis for identifying normal and abnormal system behaviour.

ii) Data Pre-processing Module

During preprocessing, text data undergoes tokenization and vectorization, sensor values are normalized, and images are resized to uniform dimensions. Min–Max normalization is applied to scale numerical features between 0 and 1, ensuring stable model convergence:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

iii) Feature Extraction Module

Feature extraction is performed using a hybrid deep learning structure. The CNN component extracts spatial features from image inputs by applying convolution and pooling operations to capture abnormal visual patterns. The LSTM component processes sequential command logs and sensor signals to identify temporal dependencies and anomalous transitions in machine states. These parallel feature streams are coordinated using the PLO mechanism, which enables simultaneous processing rather than sequential execution, thereby reducing detection latency.

iv) Model Training Module

The training phase employs supervised learning with labeled data. Model weights are optimized using back propagation and categorical cross-entropy loss:

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

v) Attack Detection and Classification Module

Analyses incoming data in real time to detect threats and classify them by severity for quick response.

vi) Trust Monitoring and Behaviour Analysis Module:

Evaluates node behaviour and trust levels to identify malicious activities and enhance system reliability.

The trained model is evaluated using accuracy, precision, recall, and F1-score, demonstrating strong intrusion detection performance. It achieves classification accuracies of 90.85% for image data and 91.66% for text data, with all key metrics consistently above 90%. Additionally, the system significantly reduces production delays from 116 hours to 5 hours annually, saving 169 product units and approximately $30,474 in yearly revenue.

6.Results and Discussion

The results demonstrate that the proposed CPS security framework achieves strong performance in detecting intrusions across both text and image data streams. With classification accuracies above 90% and consistently high precision, recall, and F1-scores, the system proves robust. XG Boost outperformed baseline models, while parallel orchestration reduced detection latency.

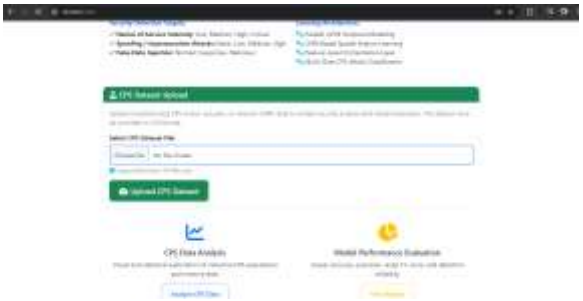


Fig 3: Sample Dataset uploading

Fig 3 presents The CPS security interface demonstrates a robust framework for analyzing industrial datasets. It allows CSV uploads of sensor, actuator, or network traffic data, followed by automated analysis.

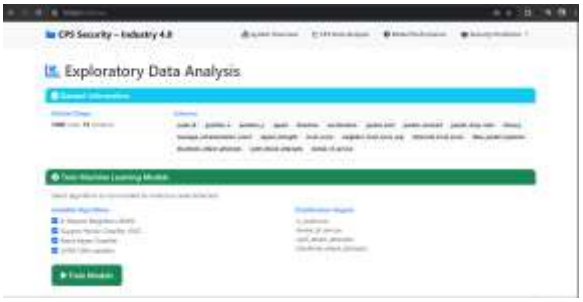


Fig 4: CPS Security Data Analysis

The fig 4 CPS dataset analysis involved features, including trust scores, latency, and attack attempts. Models such as KNN, SVC, Naive Bayes, and LSTM-CNN were trained for malicious node detection. Results showed LSTM-CNN achieved superior accuracy and resilience, effectively identifying denial-of-service, sybil, and black hole attacks in Industry 4.0 environments.

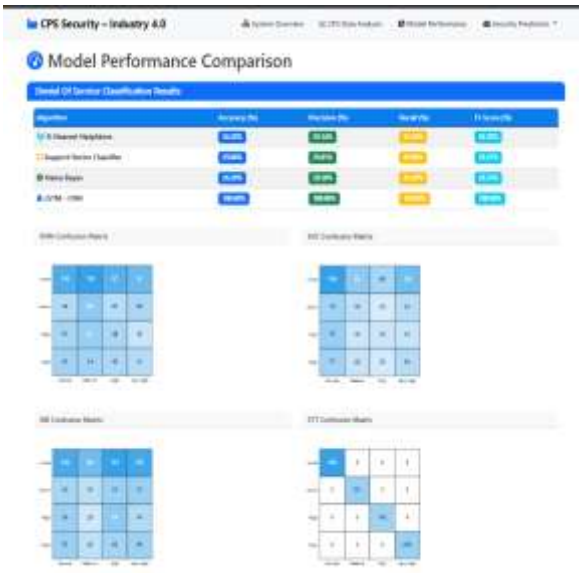


Fig 5: Model performance

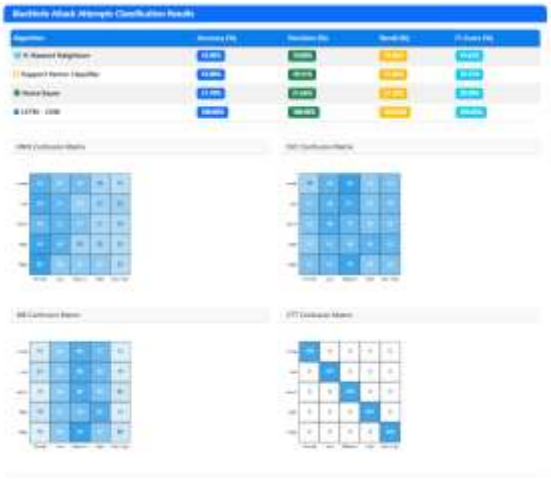


Fig 6: Black hole Attack Classification Results

The fig 5,6 classification results highlight the superior performance of the LSTM-CNN model, achieving 100% accuracy, precision, recall, and F1-score in detecting blackhole attack attempts. In contrast, traditional algorithms such as KNN, SVC, and Naive Bayes showed poor detection rates, with accuracies below 22%. Confusion matrices confirm LSTM-CNN's robustness and reliability.

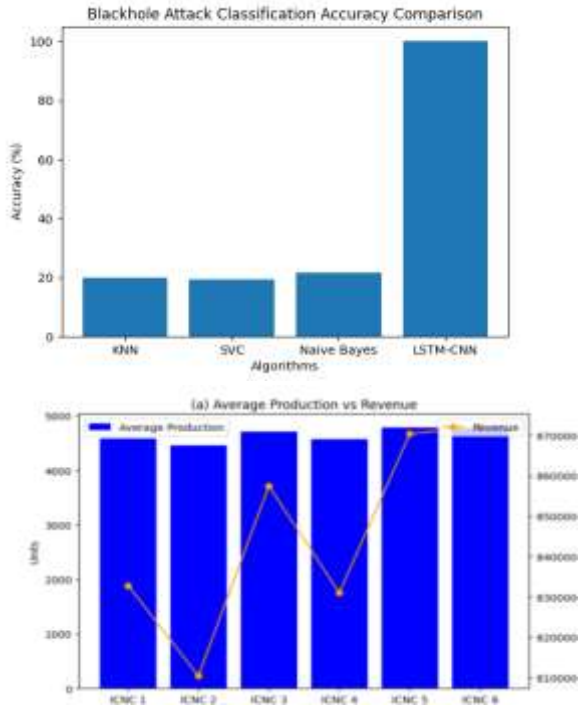


Fig 7: Production vs Revenue

Production levels remain consistently high across all ICNC machines, reflecting a stable and well-optimized manufacturing process. Despite this consistency, revenue exhibits slight variations due to factors such as demand changes or operational costs. This indicates that while production efficiency is maintained, financial outcomes are influenced by external or market-driven conditions. Overall, the system demonstrates strong operational stability with minor economic fluctuations.

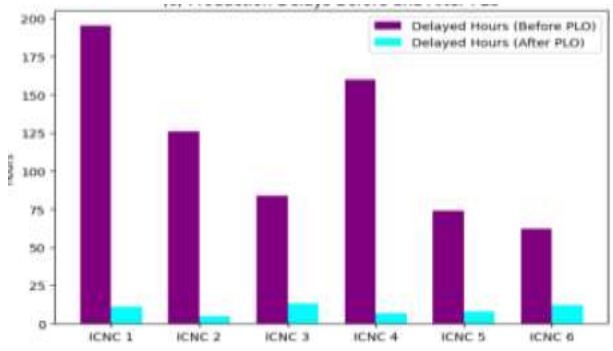


Fig 8: Production Delays

After the implementation of PLO, production delays are significantly reduced across all ICNC machines, indicating a more streamlined and responsive system. The reduction in delayed hours reflects improved coordination and faster issue resolution within the manufacturing process. This leads to enhanced operational efficiency and ensures smoother workflow with fewer interruptions. Consequently, overall productivity and system reliability are greatly improved.

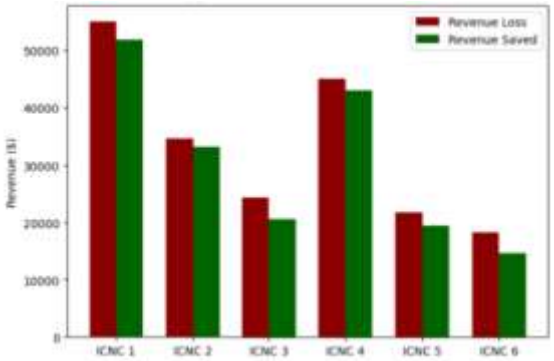


Fig 9: Revenue Loss vs Saved

After implementing PLO, the delayed production hours decrease significantly across all machines, indicating smoother workflow execution. This reduction reflects enhanced system efficiency and faster response to disruptions. As a result, overall operational stability improves with minimal downtime and interruptions.

7. Conclusion and Future Scope

Cyber-physical systems (CPS) have greatly enhanced efficiency, productivity, and flexibility in modern manufacturing, but increased connectivity also introduces significant cyber security risks. To address this, the proposed framework integrates LSTM and CNN using a Parallel Orchestration (PLO) algorithm for robust intrusion detection. The system achieves

higher accuracy than traditional methods in detecting threats from both text and image data, while ensuring production continuity and minimizing disruptions. Experimental results demonstrate a significant reduction in successful intrusions, notable annual revenue savings, and a 95.69% decrease in production delays. the system has certain limitations, as it is evaluated in a simulated environment and does not fully capture real-world uncertainties, insider threats, or advanced attacks such as adversarial machine learning. These limitations indicate the need for further improvements to enhance system robustness and applicability in real-world CPS security scenarios.

Future Scope: Future enhancements can include real-time data streaming from IoT devices and live network traffic for continuous threat detection. The integration of Transformer and attention-based models, along with explainable AI techniques, can improve model interpretability and decision transparency. Furthermore, incorporating adaptive and self-learning mechanisms will enable the system to evolve with emerging cyber threats, ensuring long-term robustness and effectiveness in dynamic network environments.

Reference

1. S. M. Zahraee et al., "Simulation of manufacturing production line based on Arena," *Adv. Mater. Res.*, 2014.
2. P. O'Donovan et al., "A fog computing industrial cyber-physical system for low-latency machine learning," *Manuf. Lett.*, 2018.
3. H. Zhao et al., "Sequential fault diagnosis based on LSTM neural network," *IEEE Access*, 2018.
4. M. Kerin and D. T. Pham, "A review of emerging Industry 4.0 technologies," *J. Cleaner Prod.*, 2019.
5. X. Lei et al., "A dilated CNN model for image classification," *IEEE Access*, 2019.
6. S. Munirathinam, "Industry 4.0: Industrial Internet of Things," *Advances in Computers*, 2020.
7. D. G. S. Pivoto et al., "Cyber-physical systems architectures for industrial IoT," *J. Manuf. Syst.*, 2021.
8. B. Li et al., "DeepFed: Federated deep learning for intrusion detection in CPS," *IEEE Trans. Ind. Informat.*, 2021.
9. R. Alguliyev et al., "Hybrid DeepGCL model for cyber-attack detection," *Neural Comput. Appl.*, 2021.
10. H. Kayan et al., "Cybersecurity of industrial CPS: A review," *ACM Comput. Surv.*, 2022.
11. A. Halbouni et al., "CNN-LSTM hybrid deep neural network for intrusion detection," *IEEE Access*, 2022.
12. M. Abdullahi et al., "Deep learning model for cybersecurity attack detection in CPS," *ICCUBEA*, 2022.
13. E. C. P. Neto et al., "CICIoT2023: A dataset for large-scale IoT attacks," *Sensors*, 2023.
14. K. Manasa and L. Joseph, "IoT security vulnerabilities in Industry 4.0," 2023.
15. S. J. Oks et al., "Cyber-physical systems in Industry 4.0: A review and outlook," *Inf. Syst. Frontiers*, 2024.