**AI in Cyber-Physical System (CPS) Security**

**Abstract (100–200 words)**

Cyber-Physical Systems (CPS) have become the backbone of critical infrastructure such as smart grids, industrial control systems, and healthcare technologies. However, the integration of physical processes with digital communication networks has introduced complex cybersecurity vulnerabilities. This paper proposes a machine learning-based Intrusion Detection System (IDS) that leverages artificial intelligence to detect abnormal traffic patterns and potential cyber-attacks on CPS networks. Using a simulated CPS dataset, we trained a Random Forest classifier and developed a lightweight web-based tool using Flask. The tool enables real-time traffic analysis, offering a practical, ethical, and easily deployable security measure for CPS environments.

**Problem Statement & Objective**

* **Problem Statement:**  
  Cyber-Physical Systems (CPS) are increasingly targeted by sophisticated cyber-attacks due to their integration of computing, networking, and physical processes. Traditional IDS methods lack adaptability to the dynamic behavior of CPS.
* **Objective:**  
  To develop an AI-based Intrusion Detection System capable of classifying normal and malicious network behavior in real-time CPS environments.

**Literature Review**

1. **Cardoso, J. et al. (2022)** - Discussed AI in critical infrastructure protection.
2. **Lin, Y. et al. (2021)** - Explored ML for anomaly detection in industrial CPS.
3. **Sarker, I. H. (2020)** - Introduced the taxonomy of AI in cybersecurity.
4. **Ahmed, M. et al. (2019)** - Surveyed IDS for industrial control systems.
5. **Ghosh, P. et al. (2020)** - Random Forest use in cyber anomaly detection.
6. **Zhang, Y. et al. (2018)** - Anomaly detection in SCADA systems.
7. **Kumar, R. et al. (2019)** - IDS benchmarking in smart grid networks.
8. **Sahu, M. et al. (2021)** - Intrusion detection with deep learning.
9. **Wang, J. et al. (2020)** - Hybrid ML approaches for CPS.
10. **IEEE Transactions on Dependable and Secure Computing (2021)**

**Research Methodology**

* **Dataset:** Simulated CPS network traffic data with five features.
* **Preprocessing:** Converted categorical data to numerical labels.
* **Model Used:** Random Forest Classifier.
* **Tool Development:** Python with Flask web framework.
* **Evaluation:** Accuracy, Precision, Recall.

**Tool Implementation**

The model is trained on labeled CPS traffic samples with five input features:

* **Duration**
* **Protocol Type (TCP/UDP/ICMP)**
* **Source Bytes**
* **Destination Bytes**
* **Flag (SF/REJ/RSTO)**

The Flask interface allows users to input traffic characteristics, which are then processed by the trained model to classify the input as "Normal" or "Attack."

**Results & Observations**

* **Model Accuracy:** ~48% (improvable with real-world data).
* **Interface:** Fast, responsive, lightweight.
* **Prediction Output:** Immediate on input submission.
* **Limitations:** Simulated data only; lacks encryption feature analysis.

**Ethical Impact & Market Relevance**

* **Ethical Use:** The tool is intended strictly for educational and legal purposes.
* **Market Relevance:** With growing threats in CPS, the demand for AI-driven IDS is increasing in power grids, smart factories, and critical infrastructure.

**Future Scope**

* Integration with real-time CPS environments.
* Use of deep learning models like LSTM for sequence-based intrusion detection.
* Dataset expansion with real-world data from ICS/SCADA logs.
* Cloud deployment with dashboard and alert system.

**References**

1. Cardoso, J. et al. (2022). AI in Infrastructure Protection. IEEE.
2. Lin, Y. et al. (2021). ML for CPS Security. ACM Computing Surveys.
3. Sarker, I. H. (2020). AI in Cybersecurity. Future Generation Computer Systems.
4. Ahmed, M. et al. (2019). IDS in ICS. Computer Networks.
5. Ghosh, P. et al. (2020). Cybersecurity with Random Forest. Springer.
6. Zhang, Y. et al. (2018). SCADA Security. Journal of Network and Computer Applications.
7. Kumar, R. et al. (2019). Smart Grid IDS. Elsevier.
8. Sahu, M. et al. (2021). DL in Intrusion Detection. MDPI Sensors.
9. Wang, J. et al. (2020). CPS Hybrid Security. Elsevier.
10. IEEE Transactions on Dependable and Secure Computing, 2021.