ISSN: 2320-5407
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: **IJAR-53446** Date: 21-08-2025

Title: AI-Enhanced Intrusion Detection for Industry 4.0: A Cross-Regional Study on Mitigating Advanced Persistent Threats in Cyber-Physical Systems

Recommendation:
Accept as it is .....YES.....
Accept after minor revision.....
Accept after major revision .....
Do not accept (*Reasons below*) .....

Rating	Excel.	Good	Fair	Poor
Originality			✓	
Techn. Quality		✓		
Clarity			✓	
Significance		✓		

Reviewer Name: Mir Bilal

Reviewer's Comment for Publication.

General Assessment:

The manuscript addresses a highly relevant and timely issue in cybersecurity for Industry 4.0: the need for effective intrusion detection systems to counter Advanced Persistent Threats (APTs) in Cyber-Physical Systems (CPS). The integration of federated learning (FL), explainable AI (XAI), and quantum-resistant cryptography demonstrates both technical innovation and forward-looking relevance. The cross-regional validation strengthens the study's global applicability and positions it as a significant contribution to cybersecurity research and industrial practice.

Abstract:

The abstract is detailed, outlining the motivation, methodological innovations, key performance metrics, and ethical considerations of the proposed framework. Specific numerical results—such as 93.2% detection accuracy, 4.1% false positive rate, and bandwidth/energy reductions—underscore the study's rigor and practical impact. The mention of regional contexts (Kenya, India, USA) and field trials enhances the credibility and applicability of the work. Ethical safeguards, such as differential privacy and adherence to ITU-D guidelines, further strengthen the framework's robustness.

ISSN: 2320-5407
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

Introduction:

The introduction situates the research within the broader evolution of Industry 4.0 and its vulnerabilities. By referencing high-profile incidents such as the Colonial Pipeline ransomware attack, SolarWinds breach, and Stuxnet worm, the manuscript convincingly demonstrates the urgency of addressing APTs in CPS. The statistics provided—such as 47% of industrial firms reporting APT breaches in 2023—further highlight the scale of the problem and the need for adaptive solutions.

Significance of the Study:

The study is significant for its integration of three advanced technologies—FL for decentralized learning, XAI for interpretability, and quantum-resistant cryptography for long-term resilience. The emphasis on resource-constrained environments, particularly in African contexts, broadens the scope beyond technologically advanced economies, making the research inclusive and globally relevant.

Methodological Strengths:

The use of real-world datasets (SWaT) and synthetic APTs provides a strong empirical foundation. Cross-regional validation across Africa, Asia, and the West demonstrates the adaptability of the proposed system to varied infrastructural contexts. The explicit quantification of energy savings (52% in Africa), accuracy (>90% in low-bandwidth networks), operator trust (21–35% increases), and quantum resilience (96%) illustrates methodological rigor and practical outcomes.

Findings and Results:

The framework achieves substantial improvements over traditional IDS, including a 27% increase in detection accuracy, a reduction in false positives, and notable efficiency gains in bandwidth and energy consumption. The emphasis on operator trust, enhanced by XAI, reflects an important human-centered dimension often underexplored in cybersecurity research.

Discussion and Contribution:

The manuscript makes a clear contribution by proposing an integrated, AI-enhanced approach to intrusion detection that is effective across diverse global contexts. The ethical dimension, grounded in privacy protection and operator consent, strengthens the study's societal

ISSN: 2320-5407
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

relevance. By combining technical advancement with regional inclusivity and ethical responsibility, the research aligns with global cybersecurity priorities in Industry 4.0.

Overall Evaluation:

The manuscript is comprehensive, methodologically rigorous, and globally relevant. It successfully integrates advanced AI techniques with practical industrial security challenges and demonstrates measurable improvements in performance, efficiency, and trust.

Verdict:

The study represents a substantial contribution to cybersecurity, Industry 4.0 research, and AI applications in critical infrastructure protection. Its innovative framework and cross-regional validation highlight both academic value and practical significance for industrial resilience against APTs.