



### REVIEWER'S REPORT

**Manuscript No.: IJAR-56000**

**Title: A Robust Hybrid Approach for Intrusion Detection in Dynamic and Heterogeneous IoT Environments**

**Recommendation:**

**Accept**

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

**Reviewer Name: Dr. Ashish Yadav**

### *Detailed Reviewer's Report*

**Reviewer's Comment for Publication.**

Acceptance Comment are mentioned below suitable for the paper titled "A Robust Hybrid Approach for Intrusion Detection in Dynamic and Heterogeneous IoT Environments"

**Reviewer Comments: Accept**

**Reviewer Comments –**

#### **1. Introduction**

The manuscript titled "A Robust Hybrid Approach for Intrusion Detection in Dynamic and Heterogeneous IoT Environments" addresses a highly relevant and timely research problem in the domain of IoT security. With the rapid expansion of heterogeneous IoT ecosystems and the associated increase in cyber threats, the need for robust, adaptive, and scalable intrusion detection systems is critical. The authors clearly motivate the research by highlighting key limitations of existing IDS solutions, such as poor generalization, sensitivity to class imbalance, and challenges in handling large-scale heterogeneous traffic. The problem statement is well-defined, and the objectives are clearly articulated. Overall, the introduction effectively establishes the significance of the study and justifies the proposed hybrid deep learning approach.

#### **2. Literature Review**

The literature review is comprehensive and well-structured, covering traditional machine learning, deep learning, and hybrid IDS approaches for IoT environments. The authors critically analyze existing methods and clearly identify gaps related to adaptability in dynamic environments, imbalance handling, and feature selection inefficiencies. The discussion demonstrates strong domain knowledge and appropriately positions the proposed AE-CNN-BiLSTM-Attention framework as an advancement over prior work. The inclusion of recent and relevant studies strengthens the novelty claim and provides a solid theoretical foundation for the proposed methodology.

#### **3. Solution Approach**

## REVIEWER'S REPORT

The proposed solution is methodologically sound and technically robust. The integration of AutoEncoders, CNN, BiLSTM, and an attention mechanism is well-justified, leveraging the strengths of each component for feature representation, spatial-temporal learning, and contextual relevance. The preprocessing pipeline is a notable strength, particularly the use of five complementary feature selection techniques and the majority voting strategy to derive optimal feature subsets. The handling of outliers via IQR-based winsorization and class imbalance correction using AE-based synthetic data generation is appropriate and innovative. The overall architecture is clearly described, reproducible, and well-aligned with the challenges of dynamic and heterogeneous IoT traffic.

### 4. Results and Discussion

The experimental evaluation is extensive and convincing, utilizing the large-scale NF-ToN-IoT-V2 dataset. The reported results demonstrate strong performance across all key metrics, including accuracy, sensitivity, specificity, F1-score, and MCC. The comparison between the two feature subsets (28 and 20 features) is insightful and highlights the effectiveness of the majority voting-based feature selection strategy. The discussion effectively interprets the results, emphasizing robustness, generalization, and balanced detection capability. The achieved performance metrics are competitive and, in several aspects, superior to existing approaches reported in the literature.

### 5. Conclusion

The conclusion succinctly summarizes the key contributions and findings of the study, reinforcing the effectiveness and applicability of the proposed hybrid IDS framework. The authors successfully demonstrate that their approach offers a robust, scalable, and generalizable solution for intrusion detection in dynamic IoT environments. The work has clear practical relevance and strong potential for real-world deployment. Future research directions are implied and logically extend from the current work.