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-51835** Date: 24/05/2025

Title: ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: THE CONTRIBUTION OF GPT AND BERT IN THREAT DETECTION AND INCIDENT ANALYSIS

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

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

Originality: The paper addresses a relevant topic by proposing the combined use of BERT and GPT for cybersecurity threat detection. While integrating these models is a growing area of research, the novelty lies in their hybrid application for both classification and report generation. However, similar ideas have been previously explored in academic and industrial contexts.
Technical Quality: The methodology is sound, using the CIC-IDS2017 dataset and employing established models with appropriate evaluation metrics. However, the technical descriptions (especially the mathematical formulations and architecture) are relatively high-level and could benefit from deeper analysis of limitations, model tuning strategies, and computational trade-offs.
Clarity: The overall structure is clear and logically organized, but the writing quality needs improvement in grammar, punctuation, and flow. There are also formatting issues, like typos (e.g., "Eras" instead of "Epochs" in Table 1) and inconsistent referencing. Some figures and tables could be better integrated and explained.
Significance: The results—particularly 97.2% accuracy and low false positive rates—are promising. The practical implications for SOC analysts and potential real-time deployment give the work good significance. However, broader applicability beyond the CIC-IDS2017 dataset isn't fully addressed.

Reviewer Name: Mr. Aditya Nivas Magdum **Date:** 24/05/2025

Reviewer's Comment for Publication.

(*To be published with the manuscript in the journal*)

The paper is timely and addresses an increasingly important domain, proposing a novel integration of natural language processing models for improved detection accuracy and analyst support. The technical foundation of the work is solid, employing the CIC-IDS2017 dataset and appropriate evaluation metrics such as accuracy, recall, F1-score, and false positive rate. The experimental results, particularly a classification accuracy of 97.2% and a reduced false positive rate of 2.1%, suggest meaningful improvements over existing approaches. The inclusion of GPT for report generation adds practical value, potentially aiding SOC analysts with actionable insights.
However, the manuscript would benefit from improvements in writing clarity and formatting consistency. Some sections, such as the mathematical formulations and implementation details, could be expanded to enhance transparency and reproducibility. Additionally, the novelty could be strengthened by further distinguishing the proposed method from prior hybrid AI systems in cybersecurity.
Overall, this is a commendable and promising contribution that warrants publication with minor revisions focused on presentation and depth of technical explanation.

Detailed Reviewer's Report