Review Form 3

Journal Name:	**Journal of Engineering Research and Reports**
Manuscript Number:	**Ms_JERR_131309**
Title of the Manuscript:	**Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures**
Type of the Article	

General guidelines for the Peer Review process:

Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty'**, provided the manuscript is scientifically robust and technically sound.
To know the complete guidelines for the Peer Review process, reviewers are requested to visit this link:

https://r1.reviewerhub.org/general-editorial-policy/

Important Policies Regarding Peer Review

Peer review Comments Approval Policy: https://r1.reviewerhub.org/peer-review-comments-approval-policy/
Benefits for Reviewers: https://r1.reviewerhub.org/benefits-for-reviewers

Review Form 3

PART 1: Comments

	Reviewer's comment **Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.**	**Author's Feedback** *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Please write a few sentences regarding the importance of this manuscript for the scientific community. A minimum of 3-4 sentences may be required for this part.	➢ Provides a comprehensive analysis of adversarial threats, highlighting vulnerabilities at the data, model, and deployment levels in AI-driven systems. ➢ Offers quantitative insights into the effectiveness of adversarial attacks (FGSM, PGD, C&W) and countermeasures, using real-world datasets for robust evaluation. ➢ Recommends hybrid defense mechanisms and standardized evaluation benchmarks to improve AI model resilience against evolving adversarial threats. ➢ Contributes to the advancement of AI security practices, serving as a valuable reference for researchers, practitioners, and policymakers in AI security.	
Is the title of the article suitable? **(If not please suggest an alternative title)**	**Yes**, the current title, **"Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures,"** is clear and informative.	
Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.	**Yes,** the abstract is comprehensive, clearly presenting the study's objectives, methodology, key findings, and recommendations.	
Is the manuscript scientifically, correct? Please write here.	**Yes**	
Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.	**Yes,** the references provided are both **sufficient and recent**, with the majority of them published between **2021 and 2025**, which ensures the manuscript reflects current trends and advancements in AI security, adversarial attacks, and machine learning defenses. This is particularly important for a rapidly evolving field like AI security.	
Is the language/English quality of the article suitable for scholarly communications?	**Yes**	
Optional/General comments	The article presents a well-researched and insightful discussion, showcasing depth and dedication to the topic.	

PART 2:

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Are there ethical issues in this manuscript?	*(If yes, Kindly please write down the ethical issues here in details)*	

Reviewer Details:

Name:	**Sudhanshu Sekhar Tripathy**
Department, University & Country	**C.V Raman Global University Bhubaneswar Odisha, India**