

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 | Review 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. | The manuscript is crucial and effective for the scientific community. It helps to find upcoming vulnerabilities, attacks, and defences in Machine learning Model. This research is effective to building a strong prototype . | |
| Is the title of the article suitable? (If not please suggest an alternative title) | Adversarial attack on machine learning model by AI system: Explore vulnerability and their effective defence. | |
| 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. | The abstract of the article is sufficient and effective. | |
| 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 | |
| Is the language/English quality of the article suitable for scholarly communications? | yes | |
| <u>Optional/General</u> comments | No | |

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: | Rajesh Tanti |
| Department, University & Country | OP Jindal University, India |