## 

**Individual In-depth Report**

**Member name:** [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu)

**Evaluated by:** [Avani Mundra](mailto:amudra@asu.edu)

**Date:** Oct 9, 2023

**Tasks Assigned:**

* Reviewed the paper titled “A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View".

**Summary:**

* The study thoroughly discusses the threats in this area as well as the appropriate countermeasures. It uses a data-driven perspective.
* They carefully examine a range of security risks that affect machine learning systems, including data poisoning, adversarial assaults, and model inversion.
* Additionally, the paper provides a methodical examination of defensive strategies, ranging from basic tactics like access control and encryption to more complex ones like adversarial training and anomaly detection.
* This survey is an essential tool for both researchers and practitioners since it clarifies the complex landscape of machine learning security.
* They gain a deep awareness of the difficulties and developments in protecting machine learning systems, which helps to further the development of this important area.
* The research emphasizes the value of taking a proactive, data-driven strategy to defend machine learning against new threats.

**Outcome:**

* The study offers a data-driven analysis of security threats and solutions in machine learning. It provides a thorough resource for academics and professionals working in this developing topic.

**References:**

[1] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu and V. C. M. Leung, "A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View," in *IEEE Access*, vol. 6, pp. 12103-12117, 2018, doi: 10.1109/ACCESS.2018.2805680.

**Evaluation of Report**

**Evaluation summary with justification.**

The summary of the report is holistic and concise. It covers the problem statement in detail and discusses the importance of the paper and solution with respect to the problem statement. It assesses the security risks associated with the model and provides a data driven analysis.

**The quality of the major result(s) with justification.**  
The quality of the major results discussed in the paper is appropriate. The results and outcomes have been discussed in detail.

**The usefulness of the paper to the overall project.**   
The paper is highly relevant to the overall project and analyzes information assurance and security related to suspicious activities in social media.

**Other comments**

No comment

**Evaluation Approval  
  
Evaluation by:** [Avani Mundra](mailto:amudra@asu.edu) **Date:** Oct 9, 2023

**Is the written report of the in-depth study complete with all the major result(s) of the paper(s)? If not, provide as many examples of the major result(s) missing in the written report as possible. (in bullet form). [Normally within 100 words]**

* Yes, all major results of the paper are covered.
* The in-depth study report is complete.

**Is each section of the guidelines sufficiently completed? If not, point out what is missing. [Normally within 40 words].**

Yes, each section of the guidelines is sufficiently completed.

**Is the quality of this version of the written report satisfactory? If not, then why not? [Normally within 40 words]**

Yes, the quality of this written report is satisfactory.

**Approval.  
  
Approved by:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) **Date: 10/9/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

The quality of this written in-depth study report and Evaluation report is satisfactory. The evaluation report signifies correct evaluation and the report itself justifies the project topic.