# Article information:

Machine learning with adversaries | Proceedings of the 31st International Conference on Neural Information Processing Systems  
<https://dl.acm.org/doi/10.5555/3294771.3294783>

# Article summary:

1. The article studies the resilience of distributed implementations of Stochastic Gradient Descent (SGD) to Byzantine failures.

2. Current approaches cannot tolerate a single Byzantine failure, so a new aggregation rule is proposed that satisfies a resilience property and is provably Byzantine-resilient.

3. Experimental evaluations of the proposed algorithm are reported on.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article provides an in-depth analysis of the resilience of distributed implementations of Stochastic Gradient Descent (SGD) to Byzantine failures, and proposes a new aggregation rule that is provably resilient to such failures. The authors provide evidence for their claims through experimental evaluations, which adds to the trustworthiness and reliability of the article. However, there are some potential biases in the article that should be noted. For example, the authors focus solely on SGD and do not consider other machine learning algorithms or frameworks, which could lead to one-sided reporting or unsupported claims about SGD's superiority over other methods. Additionally, there is no discussion of possible risks associated with using SGD in distributed systems, nor any exploration of counterarguments or alternative solutions to the problem at hand. Finally, it is unclear whether all sides have been presented equally in terms of potential benefits and drawbacks associated with using SGD in distributed systems.

# Topics for further research:

* Machine learning algorithms comparison
* Distributed systems risks
* Alternative solutions to Byzantine failures
* Benefits and drawbacks of using SGD
* Counterarguments to using SGD in distributed systems
* Resilience of other machine learning frameworks to Byzantine failures

# Report location:

<https://www.fullpicture.app/item/9ca8fae4c10da6d68cccf24c22a27382>