# Article information:

Machine learning with adversaries: byzantine tolerant gradient descent - 百度学术
[https://xueshu.baidu.com/usercenter/paper/show?paperid=fbd03ec88632485d3f5707eaad8e0de7=xueshu\_se=1](https://xueshu.baidu.com/usercenter/paper/show?paperid=fbd03ec88632485d3f5707eaad8e0de7&site=xueshu_se&hitarticle=1)

# Article summary:

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

2. It proposes Krum, an aggregation rule that satisfies a resilience property and is the first provably Byzantine-resilient algorithm for distributed SGD.

3. The article also reports on experimental evaluations of Krum.

# 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 is generally reliable and trustworthy, as it provides evidence for its claims in the form of theoretical proofs and experimental evaluations. The authors have taken into account potential risks such as software bugs, network asynchrony, biases in local datasets, and attackers trying to compromise the system when proposing their solution. Furthermore, they provide a detailed explanation of their proposed algorithm and its resilience property, which makes it easier to understand how it works and why it is resilient to Byzantine failures.

However, there are some points that could be improved upon. For example, the authors do not explore any counterarguments or alternative solutions to their proposed algorithm; this could be done by comparing Krum with other existing algorithms in terms of performance and resilience to Byzantine failures. Additionally, while the authors provide evidence for their claims in the form of theoretical proofs and experimental evaluations, they do not provide any evidence from real-world applications or scenarios where their algorithm has been tested or used successfully; this would help strengthen their argument further.

# Topics for further research:

* Byzantine Fault Tolerance
* Distributed Systems Resilience
* Krum Algorithm Performance
* Network Asynchrony
* Local Dataset Biases
* Real-World Application Testing

# Report location:

<https://www.fullpicture.app/item/c374e9b70572f6cb272e749e4f4eef01>