# Article information:

Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models - PMC  
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9103313/>

# Article summary:

1. DDoS attacks are a major threat to IoT devices and networks, with an increase of 31% in advanced targeted attacks in Q3 2021 compared to the same period in 2020.

2. Low-rate and high-rate DDoS attacks have different characteristics, with low-rate attacks being more inconspicuous but still capable of disrupting services.

3. Machine learning and deep learning models can be used to build effective intrusion detection systems for identifying DDoS and DoS attacks over IoT networks, with Decision Tree and Multi-layer Perceptron models performing best.

# Article rating:

Appears strongly imbalanced: The article is written in a biased or one-sided way, and the information it provides is not trustworthy enough to be considered a reliable source. You should consult other sources to find reliable information on the presented issues.

# Article analysis:

该文章提出了一种基于机器学习和深度学习模型的入侵检测系统，用于检测物联网设备中的传输层和应用层DDoS攻击。然而，该文章存在以下问题：

1. 偏见来源：该文章没有考虑到物联网设备本身的安全漏洞，而将焦点放在了DDoS攻击上。这可能会导致读者忽略了其他潜在的安全威胁。

2. 片面报道：该文章只关注了Bot-IoT数据集，并没有考虑其他数据集或真实世界中的情况。这可能会导致结果不够准确或适用性不足。

3. 缺失考虑点：该文章没有考虑到DDoS攻击背后的动机和目的。例如，攻击者可能试图窃取敏感信息或破坏特定组织或国家的基础设施。

4. 主张缺失证据：该文章声称使用机器学习和深度学习模型可以有效地检测DDoS攻击，但并未提供足够的证据来支持这一主张。例如，作者没有说明如何处理类别不平衡问题以及如何选择最佳特征集。

5. 未探索反驳：该文章没有探讨其他方法或技术来检测DDoS攻击，也没有探讨可能的反驳或限制。这可能会导致读者对该方法的有效性和适用性产生怀疑。

6. 宣传内容：该文章似乎在宣传机器学习和深度学习模型的优越性，而忽略了其他方法或技术的潜力。这可能会导致读者对该领域的发展和创新产生误解。

综上所述，该文章存在一些偏见、片面报道、缺失考虑点、主张缺失证据、未探索反驳和宣传内容等问题。因此，读者应该保持批判思维并谨慎评估其结论。

# Topics for further research:

* IoT设备安全漏洞
* 其他数据集或真实世界情况
* DDoS攻击的动机和目的
* 类别不平衡问题和最佳特征集选择
* 其他检测DDoS攻击的方法或技术
* 其他方法或技术的潜力

# Report location:

<https://www.fullpicture.app/item/1cc454a5b29151ca7feb6c6653446dda>