# Article information:

(PDF) DESIGN AND IMPLEMENTATION OF AN ARTIFICIAL INTELLIGENCE-BASED WEB APPLICATION FIREWALL MODEL
<https://www.researchgate.net/publication/335903047_DESIGN_AND_IMPLEMENTATION_OF_AN_ARTIFICIAL_INTELLIGENCE-BASED_WEB_APPLICATION_FIREWALL_MODEL>

# Article summary:

1. A hybrid learning-based web application firewall (WAF) model is proposed to prevent web-based attacks, using signature-based detection (SBD) and anomaly-based detection (ABD).

2. The ABD is implemented using artificial neural networks (ANN), allowing the model to adapt to zero-day attacks.

3. The proposed model achieved a high mean achievement percentage of 96.59% in testing and promises higher performance than existing studies.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article "Design and Implementation of an Artificial Intelligence-Based Web Application Firewall Model" proposes a hybrid learning-based web application firewall (WAF) model to prevent web-based attacks. The model uses signature-based detection (SBD) and anomaly-based detection (ABD), with ABD implemented using artificial neural networks (ANN). The proposed model is tested using open-source datasets, and the results show a high mean achievement percentage.

The article provides a comprehensive literature review of previous studies on preventing web-based attacks. However, it does not provide enough evidence to support the claim that the proposed model is superior to existing models. While the study shows promising results, it lacks exploration of counterarguments or potential risks associated with the proposed model.

The article also has some biases towards promoting the proposed model as an effective solution for preventing web-based attacks. It does not present both sides equally, focusing only on the advantages of the proposed model without discussing its limitations or potential drawbacks.

Overall, while the article presents an interesting approach to preventing web-based attacks, it would benefit from more balanced reporting and further exploration of potential risks and limitations associated with the proposed model.

# Topics for further research:

* Limitations of hybrid learning-based web application firewall models
* Risks associated with artificial neural network-based anomaly detection
* Comparison of signature-based detection and anomaly-based detection in web application firewalls
* Effectiveness of existing web application firewall models
* Evaluation metrics for web application firewall models
* Open-source datasets for testing web application firewall models

# Report location:

<https://www.fullpicture.app/item/c7dfd86b97c61c2570e5aa0ecc66485b>