# Article information:

Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks - ScienceDirect
<https://www.sciencedirect.com/science/article/pii/S1574013721000113>

# Article summary:

1. Cyber-Physical Systems (CPS) rely on IoT, Software-defined Networks, and Cloud Computing for communication and feedback loops.

2. IoT devices contribute to denial of service attacks, and SDx solutions have vulnerabilities due to less secure IoT devices and high-volume network traffic.

3. The paper presents a vulnerability analysis of security solutions for CPS, recommends the use of Fog Computing, and discusses ongoing research for resiliency, performance, and scalability.

# 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 provides a comprehensive survey on vulnerability analysis of security solutions for Software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. However, the article seems to have a bias towards promoting the use of Fog Computing as one of the architectural layers for overcoming vulnerabilities without providing sufficient evidence to support this claim. The article also fails to explore potential risks associated with the adoption of Cyber-Physical Systems and does not present a balanced view of both sides of the argument.

Furthermore, the article focuses solely on Distributed Denial of Service (DDoS) and IoT-based DDoS attacks, neglecting other types of cyber threats that could potentially harm Cyber-Physical Systems. The article also lacks consideration for ethical and legal implications associated with the use of these systems.

Additionally, while the article acknowledges that IoT devices are contributing to denial-of-service attacks, it fails to address the root cause of this issue - insecure IoT devices. Instead, it suggests that SDx paradigm has offered effective solution approaches to catastrophic IoT-based DDoS attacks without addressing how these solutions can address insecure IoT devices.

Overall, while the article provides valuable insights into vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks, it lacks depth in exploring potential risks associated with these systems and presents a biased view towards promoting Fog Computing as a solution without sufficient evidence.

# Topics for further research:

* Potential risks associated with Cyber-Physical Systems
* Balanced view of both sides of the argument
* Other types of cyber threats to Cyber-Physical Systems
* Ethical and legal implications of using these systems
* Insecure IoT devices as the root cause of DDoS attacks
* Depth in exploring potential risks and solutions for Cyber-Physical Systems

# Report location:

<https://www.fullpicture.app/item/21d3a7c40d2aa7b09ab75d436d1be14f>