INDEXING RECOMMENDATIONS

Christoph P. Neumann

Proper Indexing as a Multi-Level Challenge

Your University Homepage:
Publication List » PDF Link

PDF

PDF

PDF

PDF + TeX

About RG: a DOI from RG is provided only for preprints and technical reports, but not for already published peer-reviewed papers (articles and inproceedings); in case of doubt, use Zenodo or figshare.

About arXiv: you can submit a previously published peer-reviewed paper to arXiv, as long as you provide TeX sources and clearly reference the original publication details, using its "journal reference" field (even for conference proceedings).

Computer Science > Cryptography and Security

Security Challenges for Cloud or Fog Computing-Based AI Applications

Amir Pakmehr, Andreas Aßmuth, Christoph P. Neumann, Gerald Pirkl

Security challenges for Cloud or Fog-based machine learning services pose several concerns. Securing the underlying Cloud or Fog services is essential, as successful attacks against these services, on which machine learning applications rely, can lead to significant impairments of these applications. Because the requirements for AI applications can also be different, we differentiate according to whether they are used in the Cloud or in a Fog Computing network. This then also results in different threats or attack possibilities. For Cloud platforms, the responsibility for security can be divided between different parties. Security deficiencies at a lower level can have a direct impact on the higher level where user data is stored. While responsibilities are simpler for Fog Computing networks, by moving services to the edge of the network, we have to secure them against physical access to the devices. We conclude by outlining specific information security requirements for AI applications.

Submission history

Bibliographic Tools	Code, Data, Media	Demos	Related Papers	About arXivLabs

Bibliographic and Citation Tools

Bibliographic Explorer (What is the Explorer?)

Litmaps (What is Litmaps?)

scite Smart Citations (What are Smart Citations?)

Which authors of this paper are endorsers?   Disable MathJax (What is MathJax?)

Access Paper:

- View PDF
- HTML (experimental)
- TeX Source
- Other Formats

view license

Current browse context:
cs.CR

< prev | next >

new | recent | 2310

Change to browse by:
cs
    cs.AI
    cs.DC
    cs.NI
    cs.SE

References & Citations

- NASA ADS
- Google Scholar
- Semantic Scholar

Export BibTeX Citation

Bookmark

DBLP:
(via arXiv)

SCHLOSS DAGSTUHL
Leibniz Center for Informatics

home | browse

[+]
[−] **Christoph P. Neumann**

> Home > Persons

[−] **Person information**

- *affiliation:* OTH Amberg-Weiden, Department of Electrical Engineering, Media and Computer Science, Amberg, Germany
- *affiliation (former, PhD 2012):* University of Erlangen-Nuremberg, Germany

[+] **Other persons with a similar name** ❓

[−] **2020 – today** ❓

2023

■ [i4] Amir Pakmehr, Andreas Aßmuth, Christoph P. Neumann, Gerald Pirkl:
Security Challenges for Cloud or Fog Computing-Based AI Applications. CoRR abs/2310.19459
(2023)

You Need an Endorser
(For Each Category, Individually!)

arXiv.org

Christoph Neumann is qualified to endorse.

Security Challenges for Cloud or Fog Computing-Based AI Applications

Christoph Neumann: Is registered as an author of this paper.
Can endorse for **cs.DC**. (why?)

(First, you need a submission! The getting-an-endorsement is part of the submission process. arXiv has documented this quite well.)