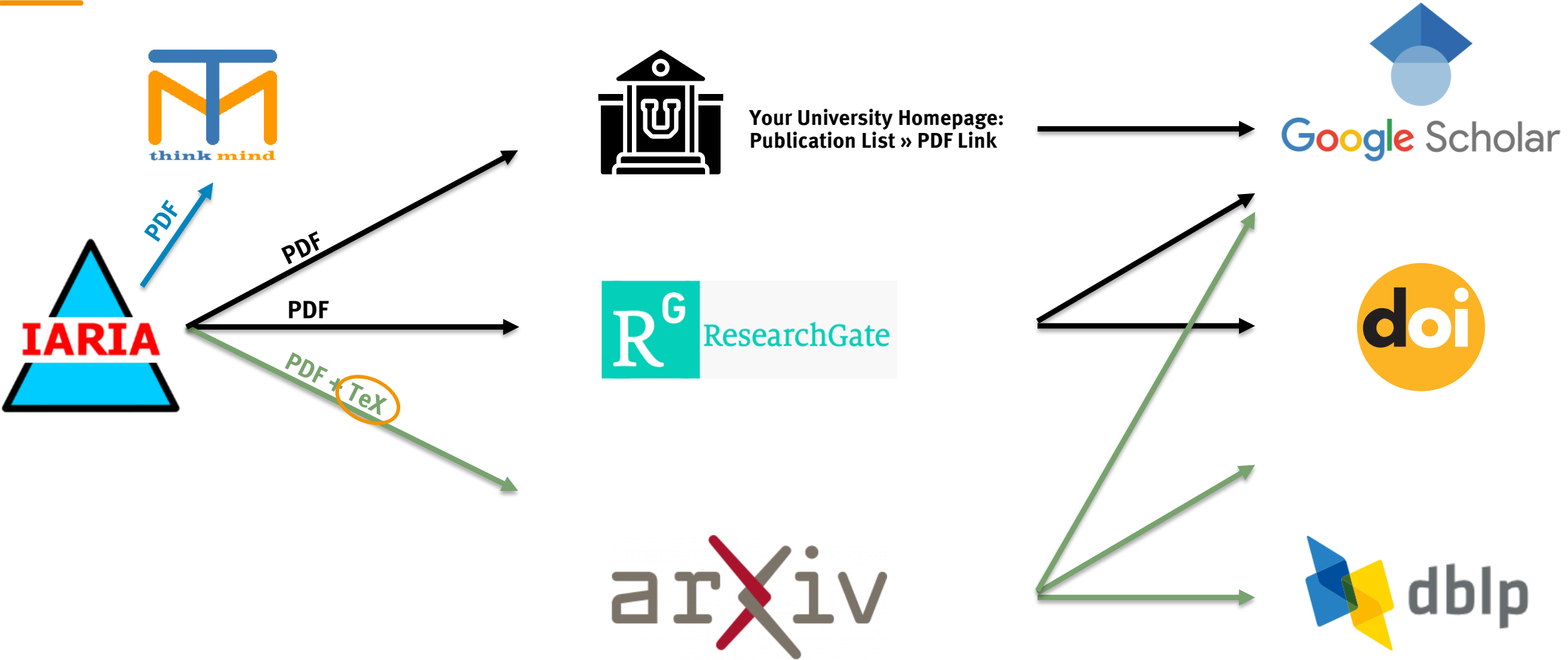


INDEXING RECOMMENDATIONS

Christoph P. Neumann
c.neumann@oth-aw.de



Proper Indexing as a Multi-Level Challenge



Computer Science > Cryptography and Security

[Submitted on 30 Oct 2023 (v1), last revised 20 Dec 2023 (this version, v3)]

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.

Subjects: **Cryptography and Security** (cs.CR); Artificial Intelligence (cs.AI); Distributed, Parallel, and Cluster Computing (cs.DC); Networking and Internet Architecture (cs.NI); Software Engineering (cs.SE)

Cite as: arXiv:2310.19459 [cs.CR]
(or arXiv:2310.19459v3 [cs.CR] for this version)

<https://doi.org/10.48550/arXiv.2310.19459>

Journal reference: Proc of the 14th International Conference on Cloud Computing, GRIDs, and Virtualization (Cloud Computing 2023), Nice, France, June 2023, pp. 21-29, ISSN 2308-4294

Submission history

From: Christoph Neumann [\[view email\]](#)
[v1] Mon, 30 Oct 2023 11:32:50 UTC (140 KB)
[v2] Fri, 3 Nov 2023 08:40:42 UTC (134 KB)
[v3] Wed, 20 Dec 2023 12:06:17 UTC (68 KB)

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






[+] 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](https://arxiv.org/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...)