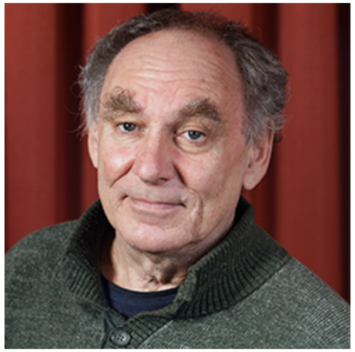
Large Language Models and Networking: What are the Challenges and Opportunities?

theNetworking Channel

Anshu Shrivastava
Rice U., ThirdAI

Elisa Bertino
Purdue U.



Jon Crowcroft
U. Cambridge
Turing Institute

Victor O.K. Li
U. Hong Kong

Ajit Patankar
Juniper Networks

Organiser: **Jim Kurose**
U. Massachusetts

© theNetworkingChannel 2023

Large Language Models and Networking: What are the Challenges and Opportunities

ThirdAI

Anshumali Shrivastava
Founder & CEO, ThirdAI Corp.
Associate Professor, Rice Computer Science.
anshu@thirdai.com

20th Sept,

GenAI/LLMs has our full Attention!

Generated by ChatGPT

- LLMs and ChatGPT are powerful AI technologies that can help enterprises streamline and automate a wide range of tasks, from customer service and support to content creation and marketing.

- They represent a powerful new tool for enterprises looking to stay ahead of the curve in an increasingly competitive and data-driven business landscape.

Early use case for almost all enterprises:

- ChatGPT Assistants on their “domain” text/data with Ownership of the process
- **In Future**: Customized to Fine-grained (or individual) level.

Many Challenges for Enterprises

- Manage Expectations Well

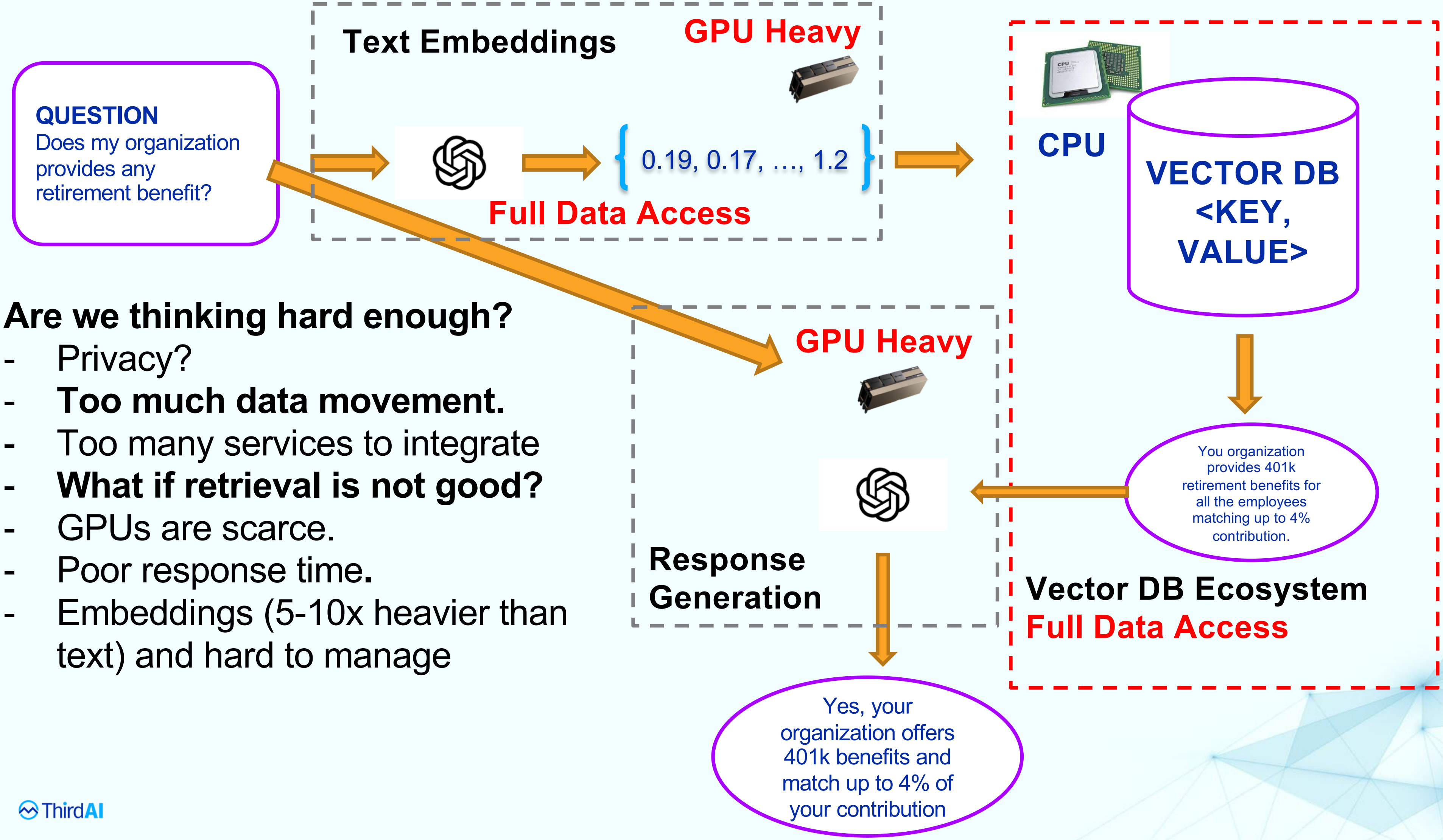
- Finding the Right Use Cases

- Understanding data privacy and data residency

- Careful with “essentially free” services in production.

- Putting LLM in production is very different and potentially much harder than making a demo.

Case Study RAG: Why Current Stack is Fundamentally Hard for Production!



Are we thinking hard enough?

- Privacy?
- **Too much data movement.**
- Too many services to integrate
- **What if retrieval is not good?**
- GPUs are scarce.
- Poor response time.
- Embeddings (5-10x heavier than text) and hard to manage

ThirdAI

Photoelectric Moment in AI: AI is about to be rewritten

1. Our understanding of AI/ML is challenged in a positive way.

2. This is the first iteration of LLMs and it will refine quickly

3. We will surely give LLMs (Mega-AI Models) full chance to solve our hardest problems. After all, what other ideas do we have that we have not tried.

Efficiency will be the guiding factor!

slices RI

PAWR Project Office

acm sigcomm

theNetworking Channel

Large Language Models and Networking Challenges and Opportunities

Elisa Bertino

Purdue U.

Opportunity

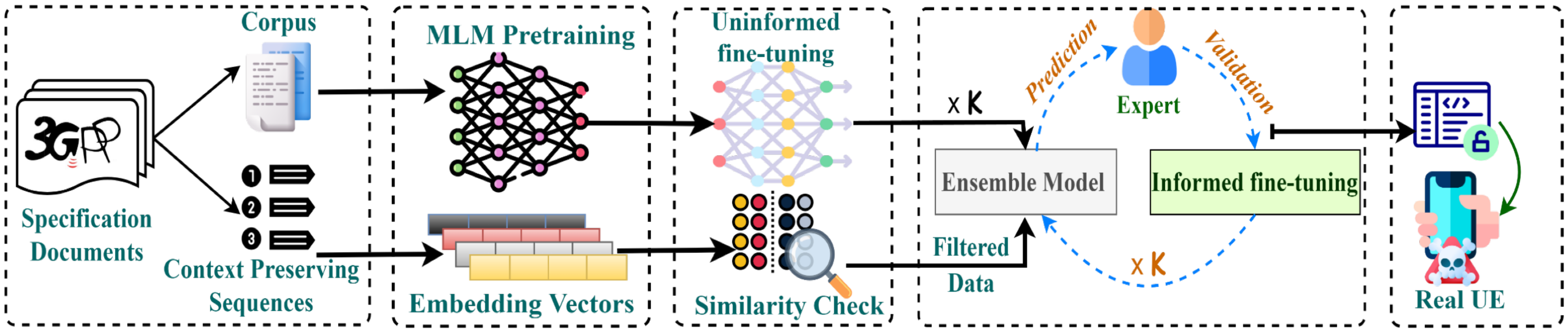
Automatic Vulnerability Detection through Conflicts from NL Cellular Protocol Specifications using LLM

theNetworking Channel

Challenges

- LLMs are not domain specific
- How do we know where to look for conflicting pairs?
- Formulation: How can LLMs detect inconsistencies?
- No-ground truth for supervised training

Solution Design



As part of the solution we created SPEC5G a dataset of NL sentences specific to 5G

© theNetworkingChannel 2023

Slide by Dr.Imtiaz Karim (Purdue University)

Opportunity

Automatic Generation of Code

Challenge: correctness of generated code

Initial evaluations [1] on GITHUB COPILOT

- Analysis carried out on code generated by Copilot in scenarios relevant to high-risk cybersecurity weaknesses (e.g. those from MITRE's "Top 25" 2021 CWE list)
- Copilot's performance evaluated on three distinct code generation axes—diversity of weaknesses, diversity of prompts, and diversity of domains
- A total of 1,689 programs were generated
- Of these, 40% were found to be vulnerable

[1] H. Pearce et al. "Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions" IEEE S&P, 2022

© theNetworkingChannel 2023

2021 CWE Top 25 Most Dangerous Software Weaknesses

theNetworking Channel

Rank	ID	Name	Score	2020 Rank Change
[1]	CWE-787	Out-of-bounds Write	65.93	+1
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.84	-1
[3]	CWE-125	Out-of-bounds Read	24.9	+1
[4]	CWE-20	Improper Input Validation	20.47	-1
[5]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19.55	+5
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19.54	0
[7]	CWE-416	Use After Free	16.83	+1
[8]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.69	+4
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	14.46	0
[10]	CWE-434	Unrestricted Upload of File with Dangerous Type	8.45	+5
[11]	CWE-306	Missing Authentication for Critical Function	7.93	+13
[12]	CWE-190	Integer Overflow or Wraparound	7.12	-1
[13]	CWE-502	Deserialization of Untrusted Data	6.71	+8
[14]	CWE-287	Improper Authentication	6.58	0
[15]	CWE-476	NULL Pointer Dereference	6.54	-2
[16]	CWE-798	Use of Hard-coded Credentials	6.27	+4
[17]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	5.84	-12
[18]	CWE-862	Missing Authorization	5.47	+7
[19]	CWE-276	Incorrect Default Permissions	5.09	+22
[20]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	4.74	-13
[21]	CWE-522	Insufficiently Protected Credentials	4.21	-3
[22]	CWE-732	Incorrect Permission Assignment for Critical Resource	4.2	-6
[23]	CWE-611	Improper Restriction of XML External Entity Reference	4.02	-4
[24]	CWE-918	Server-Side Request Forgery (SSRF)	3.78	+3
[25]	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	3.58	+6

© theNetworkingChannel 2023

HKU-Cambridge
AI to Advance Well-being
& Society (AI-WiSe)
Research Platform

HKU-AI WiSe

Shaping Large Language Models for Decision-making in Networking

Prof. Victor OK Li
Director, HKU-AI WiSe

Faculty of Engineering
THE UNIVERSITY OF HONG KONG

香 港 大 學
THE UNIVERSITY OF HONG KONG

Outline

- HKU-AI WiSe mission
- Advantages and limitations of Large Language Models (LLMs)
- LLMs can be used to support network decision-making
- Can LLMs answer causal questions to support decision-making?
- Can we make LLMs causal?
- Conclusion

Our Mission: AI for Social Good

Bring incremental and disruptive changes to the societies, by improving the health and quality-of-life of the people, through the innovation and adoption of AI and big data technologies.

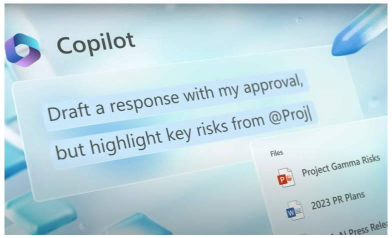
Innovations in AI and Big Data Technologies

Improving Health and Quality-of-life

Incremental and Disruptive Changes to the Societies

Advantages of LLMs

- Significant increase in performance at large model scale, showing some human-like language abilities [1]
- A key building block in many traditional natural language processing (NLP) tasks, such as machine translation and text summarization [2]
- Integrated into consumer AI to facilitate daily routine tasks
  - Productivity apps
  - Coding/writing assistant
  - …



[1] Wei, J., Tay, Y., Bommasani, R., Raffel, C., Zoph, B., Borgeaud, S., ... & Fedus, W. (2022). Emergent abilities of large language models. arXiv preprint arXiv:2206.07682.
[2] Min, B., Ross, H., Sulem, E., Veyseh, A. P. B., Nguyen, T. H., Sainz, O., ... & Roth, D. (2021). Recent advances in natural language processing via large pre-trained language models: A survey. arXiv preprint arXiv:2111.01243.

Limitations of LLMs

- However, they have limitations when used for decision-making
- Social biases and unfairness [1]
  - Trained on data biased towards certain groups of people
  - Results could be discriminatory towards those groups
- Hallucinations [2]
  - Giving answers that sound plausible and confident but are incorrect
  - Tend to generate factual statements that cannot be verified
- Unreliable reasoning capabilities [2]
  - ChatGPT is 63.41% accurate on average in 10 different reasoning categories.
  - Bad at performing complex tasks such as multi-hop reasoning
- Inconsistencies: giving inconsistent answers depending on the phrasing of prompts [3]

[1] Kasneci, E., Seßler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., ... & Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. Learning and Individual Differences, 103, 102274.
[2] Bang, Y., Cahyawijaya, S., Lee, N., Dai, W., Su, D., Wilie, B., ... & Fung, P. (2023). A multitask, multilingual, multimodal evaluation of ChatGPT on reasoning, hallucination, and interactivity. arXiv preprint arXiv:2302.04023.
[3] Krügel, S., Ostermaier, A., & Uhl, M. (2023). ChatGPT's inconsistent moral advice influences users' judgment. Scientific Reports, 13(1), 4569.

Can LLMs Help Network Operation and Decision-making?*

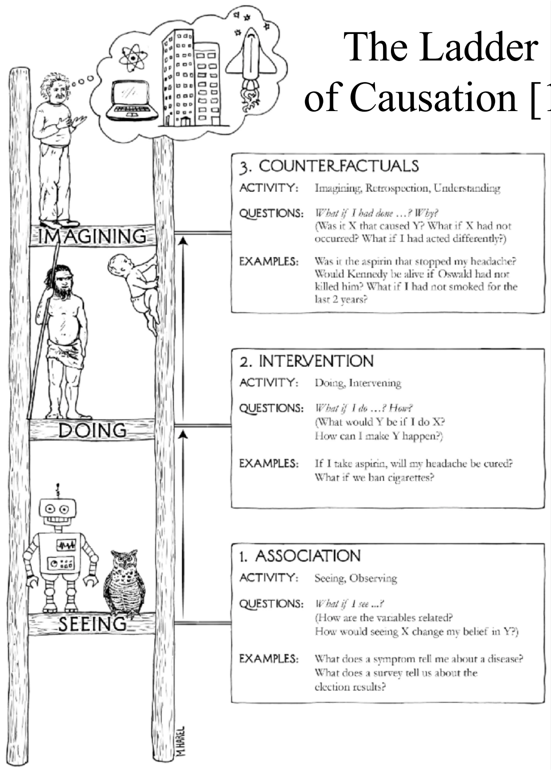
- Predictive Maintenance: LLMs can analyze data from network equipment and predict potential failures.
- Customer Service: LLMs can provide personalized customer support to subscribers.
- Network Optimization: LLMs can analyze network traffic data and identify areas where network capacity may need to be increased.
- Fraud Detection: LLMs can be used to analyze call and data usage patterns and identify potential instances of fraud.

*From ChatGPT

Can LLMs Answer Causal Questions?

- Scale is not everything
  - Trained on observational data only
  - Correlation does not imply causation
- It remains challenging for LLMs to
  - Understand causal relationships rather than correlations in data
  - Explain what causes a decision
- Answering causal questions is central in *human* decision-making, making humans unique from robots (see the Ladder of Causation)

The Ladder of Causation [1]

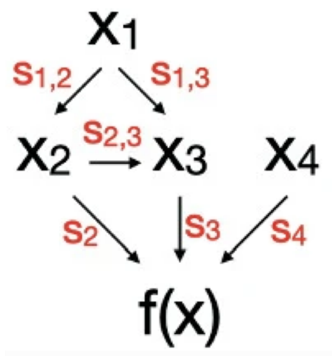


Can LLMs climb to the rung of causal reasoning?

[1] Pearl, J., & Mackenzie, D. (2018). The book of why: the new science of cause and effect. Basic books.

Causal Models

- Injecting causality into AI models
  - A causal graph: X->Y means X “causes” Y
  - Causal Shapley values: variable attribution guided by a causal graph [1]



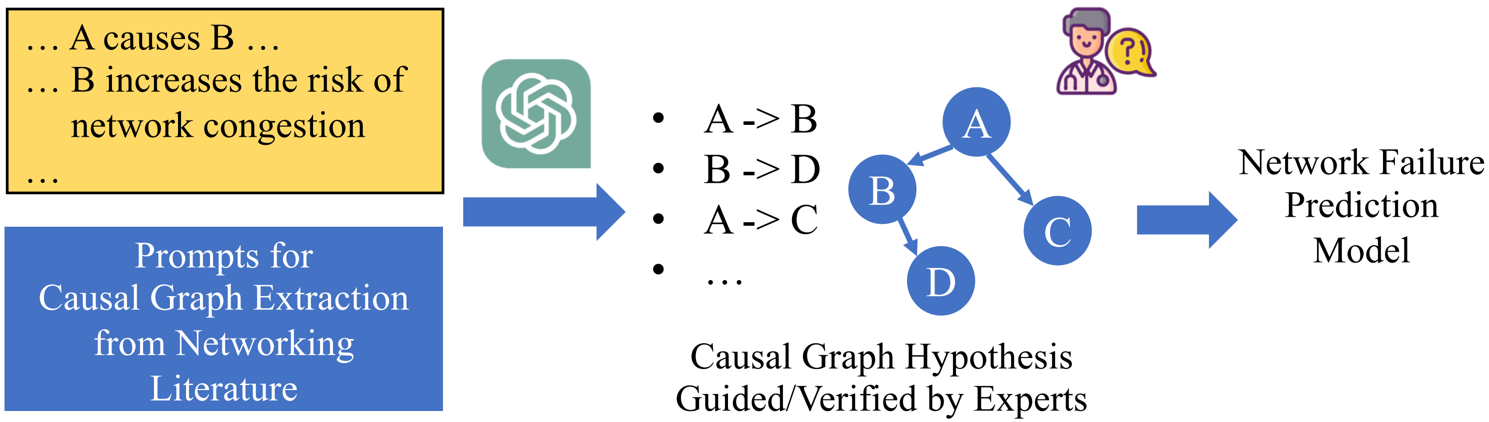
- “What-if” causal explanations [2]
  - Sufficient explanations: an action leading to a particular output, e.g., from X = x to Y = y
  - Counterfactual explanations: which variables would have had to be different for the outcome to be different?

[1] Holzinger, A., Saranti, A., Molnar, C., Biecek, P., & Samek, W. (2022, April). Explainable AI methods-a brief overview. In xxAI-Beyond Explainable AI: International Workshop, Held in Conjunction with ICML 2020, July 18, 2020, Vienna, Austria, Revised and Extended Papers (pp. 13-38).

[2] Beckers, S. (2022, June). Causal explanations and XAI. In Conference on Causal Learning and Reasoning (pp. 90-109). PMLR.

Can We Make LLMs Causal?

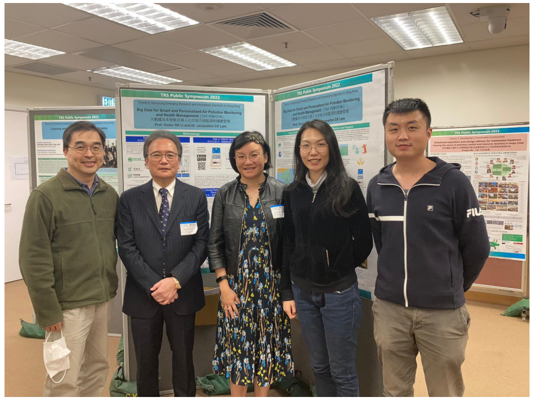
- ChatGPT can be used for text mining of existing networking literature, based on well-designed prompts
- Potential causal relationships between different network entities can be identified
- Such findings can be verified by networking experts



Conclusion

- AI is a tool to serve humans.
- LLMs have advantages and limitations.
- We need to understand how to best use this tool to our advantage.
- Human beings are unlikely to follow a decision without understanding the rationales.
- Explainability/interpretability is an important step towards trust in AI systems and making AI more useful in decision-making.

HKU-AI WiSe Team



Call for Papers

Special Issue of Data and Policy, Cambridge University Press

Generative AI for Sound Decision-Making: Challenges and Opportunities

Guest editors: Victor OK Li, Jacqueline CK Lam, and Jon Crowcroft

Paper submission deadline: December 5 2023

Publication: 2024

https://www.cambridge.org/core/journals/data-and-policy/announcements/call-for-papers/call-for-papers-generative-ai-for-sound-decision-making-challenges-and-opportunities

Next event: Lessons learned from 40+ years of the Internet

theNetworking Channel

Organizer: **Henning Schulzrinne**, Columbia U, National Telecommunications and Information Administration

Highlights from the May 2023 Dagstuhl Seminar

Lessons Learned From 40+ Years of the Internet

(May 01 – May 04, 2023)

© theNetworkingChannel 2023