Example: Recommendations and Compare/Contrast

Recommendation Use Cases

- For readers:
  - What should I read?
- For authors:
  - What should I cite?
- For conference organizers:
  - Who should review what?
- Finding experts:
  - Who knows? (Streeter & Lochbaum, 1998)

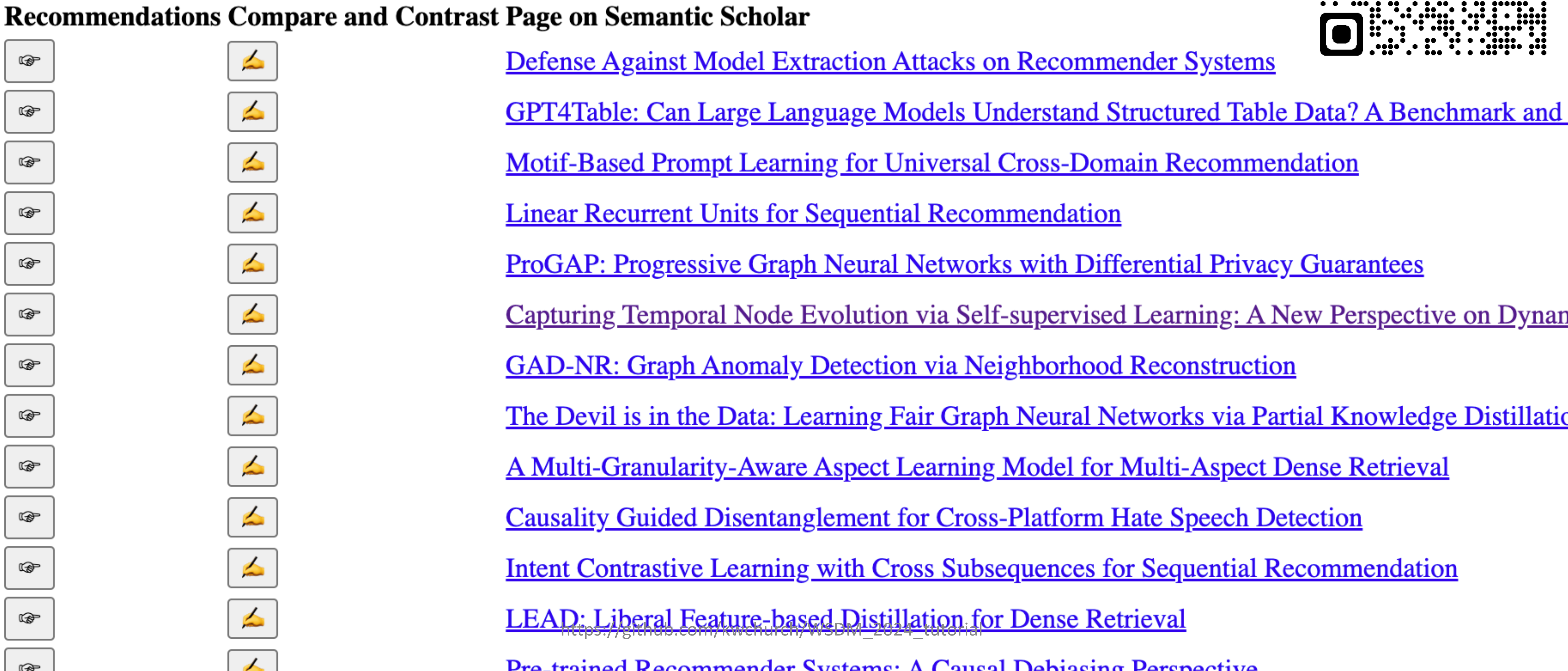
Semantic Scholar API

- https://api.semanticscholar.org/recommendations/v1/papers/forpaper/21321bad706a9f9dbb502588b0bb393cf15fa052?from=all-cs&fields=title,externalIds,citationCount
  - Semantic Scholar: A collection of 200M papers
  - query: 21321bad706a9f9dbb502588b0bb393cf15fa052
    - A paper id on Semantic Scholar
  - 200M papers → Specter embeddings
    - BERT-like vectors with 768 hidden dimensions
    - Mostly encodes titles and abstracts (with some fine-tuning on citation graph)
  - from=all-cs: limits search to computer science
    - about 10% of their collection of 200M papers
    - uses FAISS to find approximate nearest neighbors for query

Need to explain these topics before getting into this example

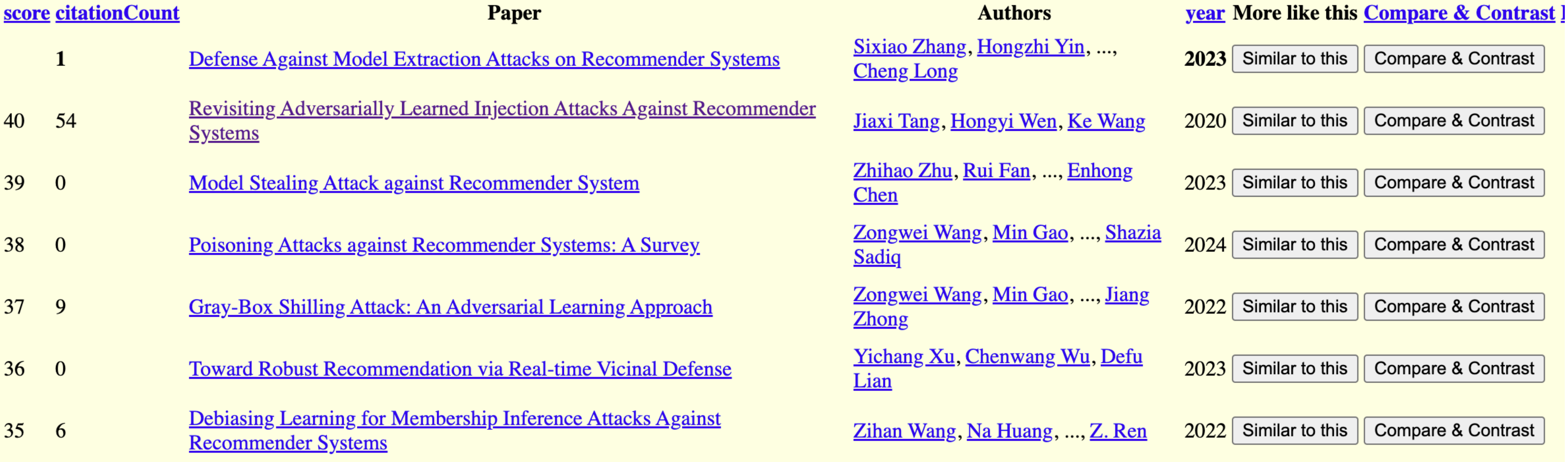
- BERT
- Specter
- Approximate Nearest Neighbors
- FAISS

WSDM-2024 Papers on arXiv



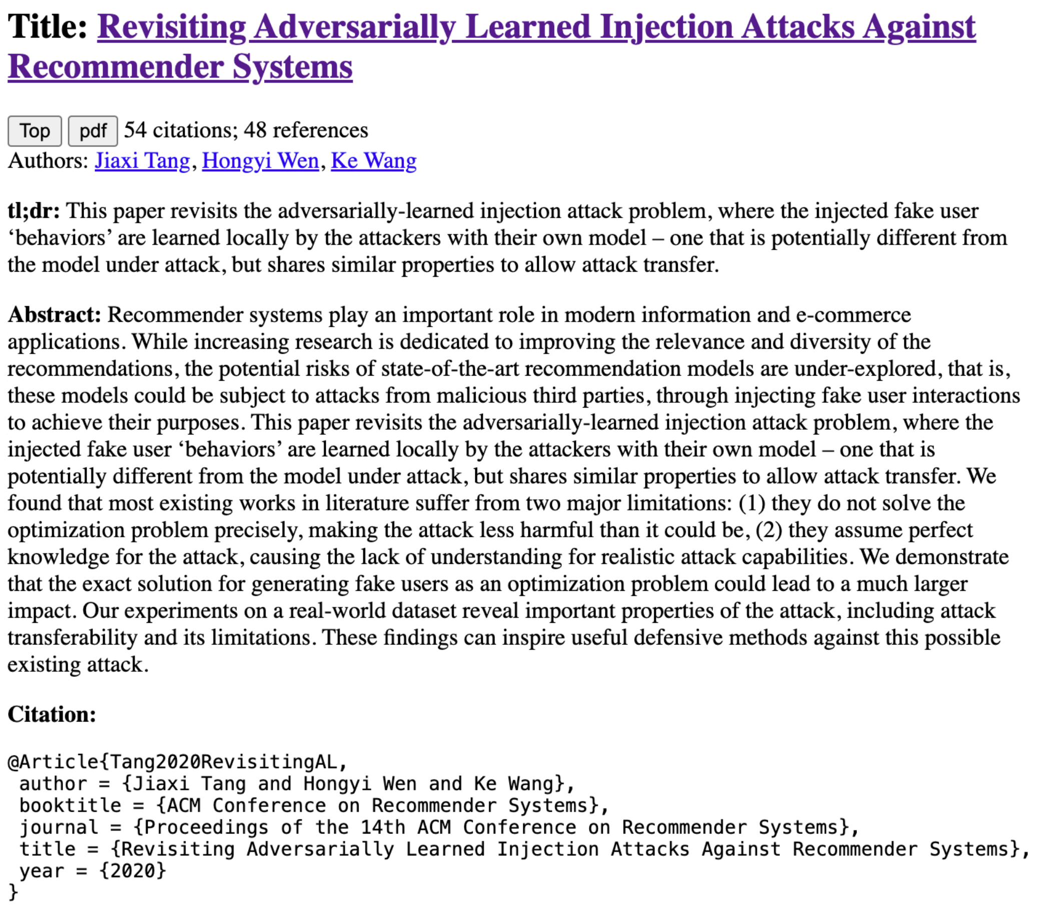
Recommendations	Compare and Contrast	Page on Semantic Scholar
☞	✍	Defense Against Model Extraction Attacks on Recommender Systems
☞	✍	GPT4Table: Can Large Language Models Understand Structured Table Data? A Benchmark and
☞	✍	Motif-Based Prompt Learning for Universal Cross-Domain Recommendation
☞	✍	Linear Recurrent Units for Sequential Recommendation
☞	✍	ProGAP: Progressive Graph Neural Networks with Differential Privacy Guarantees
☞	✍	Capturing Temporal Node Evolution via Self-supervised Learning: A New Perspective on Dynar
☞	✍	GAD-NR: Graph Anomaly Detection via Neighborhood Reconstruction
☞	✍	The Devil is in the Data: Learning Fair Graph Neural Networks via Partial Knowledge Distillatic
☞	✍	A Multi-Granularity-Aware Aspect Learning Model for Multi-Aspect Dense Retrieval
☞	✍	Causality Guided Disentanglement for Cross-Platform Hate Speech Detection
☞	✍	Intent Contrastive Learning with Cross Subsequences for Sequential Recommendation
☞	✍	LEAD: Liberal Feature-based Distillation for Dense Retrieval
☞	✍	Pre-trained Recommender Systems: A Causal Debiasing Perspective

Recommendations for a Paper in WSDM-2024



score	citationCount	Paper	Authors	year	More like this	Compare & Contrast]
	1	Defense Against Model Extraction Attacks on Recommender Systems	Sixiao Zhang, Hongzhi Yin, ..., Cheng Long	**2023**	Similar to this	Compare & Contrast
40	54	Revisiting Adversarially Learned Injection Attacks Against Recommender Systems	Jiaxi Tang, Hongyi Wen, Ke Wang	2020	Similar to this	Compare & Contrast
39	0	Model Stealing Attack against Recommender System	Zhihao Zhu, Rui Fan, ..., Enhong Chen	2023	Similar to this	Compare & Contrast
38	0	Poisoning Attacks against Recommender Systems: A Survey	Zongwei Wang, Min Gao, ..., Shazia Sadiq	2024	Similar to this	Compare & Contrast
37	9	Gray-Box Shilling Attack: An Adversarial Learning Approach	Zongwei Wang, Min Gao, ..., Jiang Zhong	2022	Similar to this	Compare & Contrast
36	0	Toward Robust Recommendation via Real-time Vicinal Defense	Yichang Xu, Chenwang Wu, Defu Lian	2023	Similar to this	Compare & Contrast
35	6	Debiasing Learning for Membership Inference Attacks Against Recommender Systems	Zihan Wang, Na Huang, ..., Z. Ren	2022	Similar to this	Compare & Contrast

Compare and Contrast



Title: Revisiting Adversarially Learned Injection Attacks Against Recommender Systems

Top | pdf | 54 citations; 48 references
Authors: Jiaxi Tang, Hongyi Wen, Ke Wang

tl;dr: This paper revisits the adversarially-learned injection attack problem, where the injected fake user ‘behaviors’ are learned locally by the attackers with their own model – one that is potentially different from the model under attack, but shares similar properties to allow attack transfer.

Abstract: Recommender systems play an important role in modern information and e-commerce applications. While increasing research is dedicated to improving the relevance and diversity of the recommendations, the potential risks of state-of-the-art recommendation models are under-explored, that is, these models could be subject to attacks from malicious third parties, through injecting fake user interactions to achieve their purposes. This paper revisits the adversarially-learned injection attack problem, where the injected fake user ‘behaviors’ are learned locally by the attackers with their own model – one that is potentially different from the model under attack, but shares similar properties to allow attack transfer. We found that most existing works in literature suffer from two major limitations: (1) they do not solve the optimization problem precisely, making the attack less harmful than it could be, (2) they assume perfect knowledge for the attack, causing the lack of understanding for realistic attack capabilities. We demonstrate that the exact solution for generating fake users as an optimization problem could lead to a much larger impact. Our experiments on a real-world dataset reveal important properties of the attack, including attack transferability and its limitations. These findings can inspire useful defensive methods against this possible existing attack.

Citation:

```
@Article{Tang2020RevisitingAL,
 author = {Jiaxi Tang and Hongyi Wen and Ke Wang},
 booktitle = {ACM Conference on Recommender Systems},
 journal = {Proceedings of the 14th ACM Conference on Recommender Systems},
 title = {Revisiting Adversarially Learned Injection Attacks Against Recommender Systems},
 year = {2020}
}
```

- Input: query + candidate
- Use prompts (chatbots)
  - Summary of candidate
  - Similarities of query & candidate
  - Differences of query & candidate

Output from Chatbot

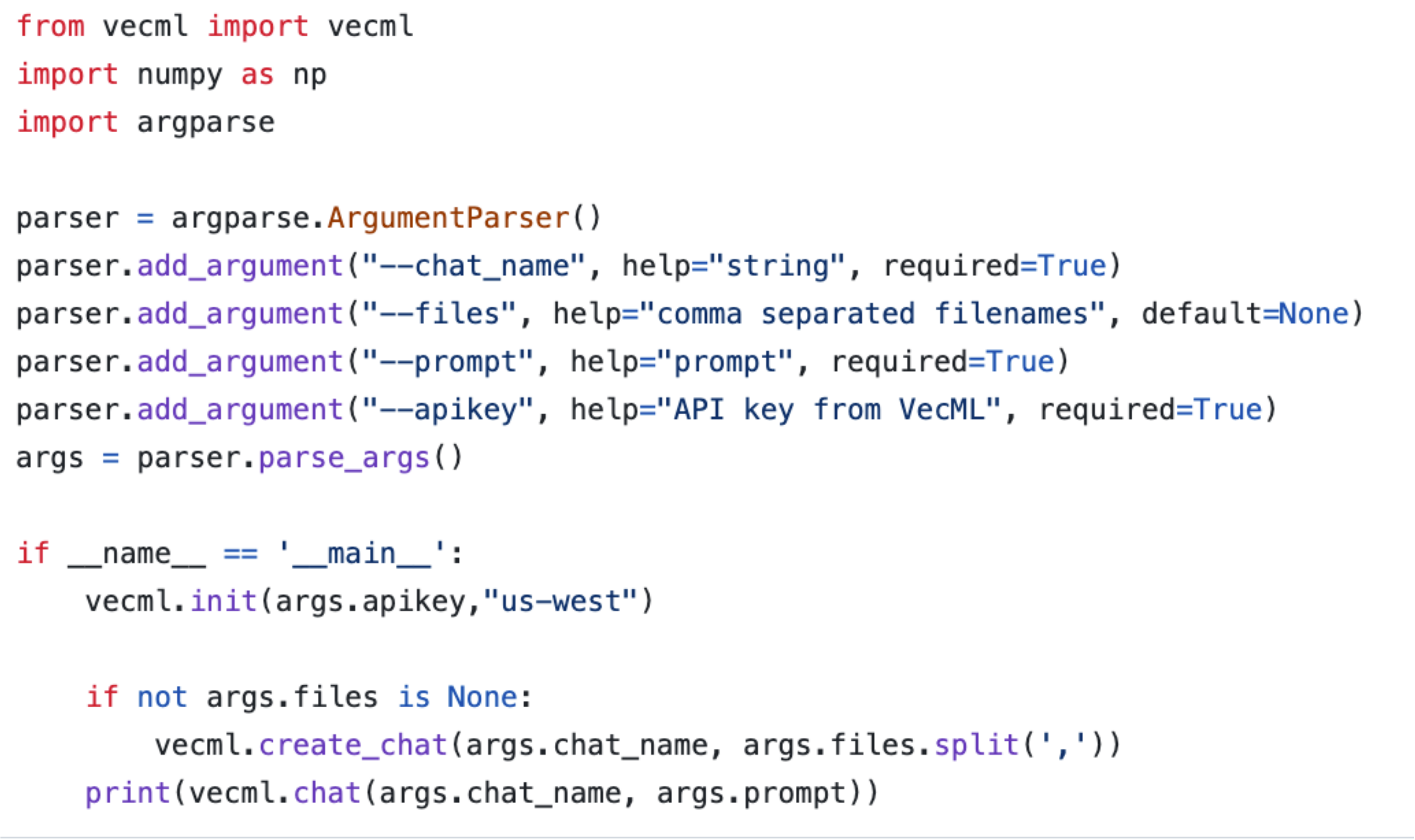
Similarities

- As an Assistant, I can tell you that both "Revisiting Adversarially Learned Injection Attacks Against Recommender Systems" and "Defense Against Model Extraction Attacks on Recommender Systems" focus on security aspects of recommender systems. The first paper explores injection attacks where the attacker manipulates the recommendation model by injecting malicious data, while the second paper deals with defending against model extraction attacks aimed at extracting sensitive information from the recommender system. Both papers highlight the importance of addressing security vulnerabilities in recommender systems to protect user data and maintain the integrity of the recommendation models.

Differences

- "Revisiting Adversarially Learned Injection Attacks Against Recommender Systems" focuses on exploring adversarially learned injection attacks against recommender systems, where the attacker has knowledge about the dataset used to train the target recommendation model. On the other hand, "Defense Against Model Extraction Attacks on Recommender Systems" focuses on strategies to defend against model extraction attacks, where attackers try to extract the architecture or parameters of a recommender system. The former paper deals with adversarial attacks, while the latter focuses on defense mechanisms against a different type of attack.

Chatbots are Super-Easy www.vecml.com



```python
from vecml import vecml
import numpy as np
import argparse

parser = argparse.ArgumentParser()
parser.add_argument("--chat_name", help="string", required=True)
parser.add_argument("--files", help="comma separated filenames", default=None)
parser.add_argument("--prompt", help="prompt", required=True)
parser.add_argument("--apikey", help="API key from VecML", required=True)
args = parser.parse_args()

if __name__ == '__main__':
    vecml.init(args.apikey,"us-west")

    if not args.files is None:
        vecml.create_chat(args.chat_name, args.files.split(','))
    print(vecml.chat(args.chat_name, args.prompt))
```

https://github.com/kwchurch/WSDM_2024_tutorial