



# **An Introduction of the Toolchain for Academic Researches**

余阳

2022-10-12

# Outline



2

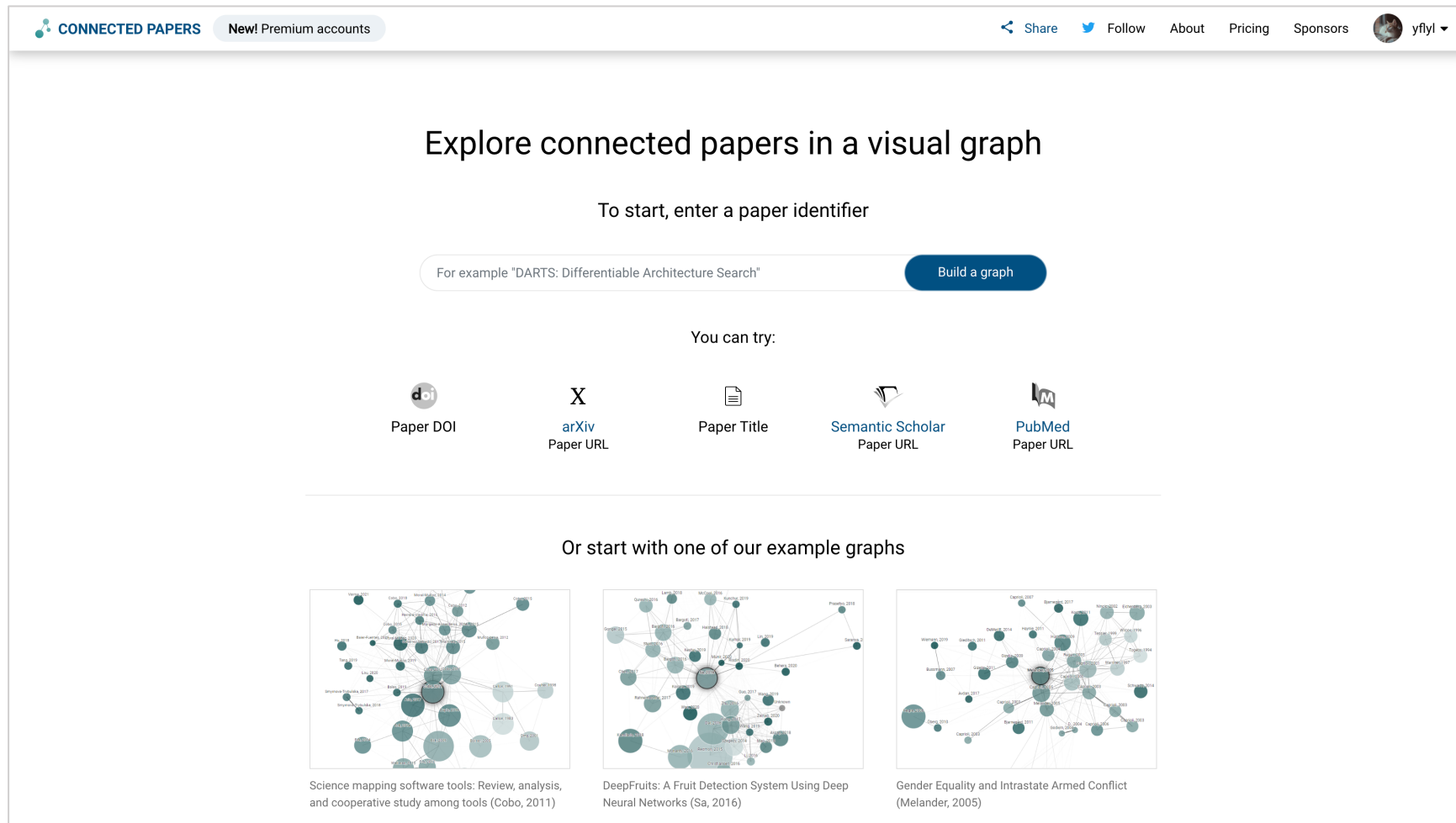
- **Introduction & Related Work**
- Methodology
- Experiments
- Conclusions

# Introduction & Related Work

3

## Investigate & Survey

### CONNECTED PAPERS



The screenshot shows the Connected Papers website interface. At the top, there is a navigation bar with the logo, the text "CONNECTED PAPERS", a link to "New! Premium accounts", and social media links for "Share", "Follow", "About", "Pricing", and "Sponsors". The main heading reads "Explore connected papers in a visual graph". Below this, it says "To start, enter a paper identifier" and provides a search input field with the example text "For example 'DARTS: Differentiable Architecture Search'" and a "Build a graph" button. Underneath, it lists "You can try:" with five options: "Paper DOI" (with a DOI icon), "arXiv Paper URL" (with an 'X' icon), "Paper Title" (with a document icon), "Semantic Scholar Paper URL" (with a Semantic Scholar icon), and "PubMed Paper URL" (with a PubMed icon). At the bottom, it says "Or start with one of our example graphs" and displays three example network graphs. Each graph is accompanied by a caption: "Science mapping software tools: Review, analysis, and cooperative study among tools (Cobo, 2011)", "DeepFruits: A Fruit Detection System Using Deep Neural Networks (Sa, 2016)", and "Gender Equality and Intrastate Armed Conflict (Melander, 2005)".

# Introduction & Related Work

4

## Investigate & Survey

### CONNECTED PAPERS

The screenshot displays the Connected Papers web application interface. At the top, there is a search bar and navigation options like 'Share', 'Follow', 'About', 'Pricing', and 'Sponsors'. The main content area is titled 'Parameter-Efficient Transfer from Sequential Behaviors for User Modeling and Recommendation'. Below the title, there is a search bar and an 'Expand' button. A list of related papers is shown on the left, including 'One Person, One Model, One World: Learning Continual User Representation without Forgetting' and 'A Generic Network Compression Framework for Sequential Recommender Systems'. The central part of the interface features a network graph where nodes represent papers and edges represent connections between them. The nodes are labeled with author names and years, such as 'Yuan, 2018', 'Wang, 2021', and 'Yuan, 2020'. The graph is color-coded by year, with a legend at the bottom showing a gradient from 2018 to 2022. On the right side, there is a detailed view of the selected paper, including its title, authors, year, and citation count. The text of the paper is visible, discussing inductive transfer learning and the PeterRec architecture.

# Introduction & Related Work

5

## ■ Investigate & Survey

### □ CONNECTED PAPERS

- *To create each graph, we analyze **an order of ~50,000 papers** and select the few dozen with the strongest connections to the origin paper.*
- *Connected Papers is not a citation tree.*
- **Similarity metric:** Co-citation and bibliographic coupling.
- **Algorithm:** Force directed graph.
- **Database:** Semantic Scholar Paper Corpus.
- **Pricing:** 5 free graphs per month, \$3 per month for unlimited graphs.

# Introduction & Related Work

6

## ■ Investigate & Survey

-  AI-Paper-Search (by MLNLP), Google Scholar, etc.

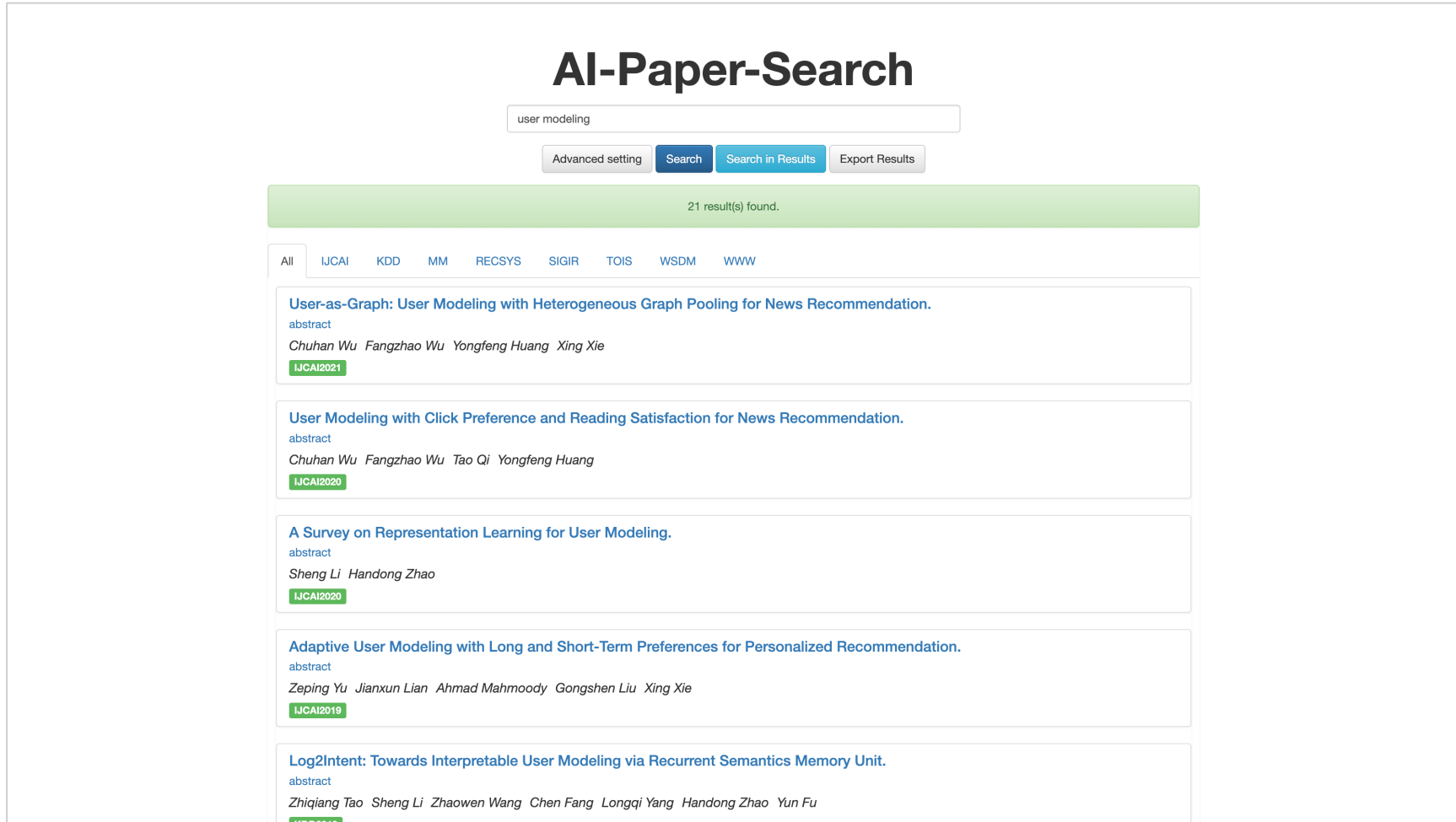


# Introduction & Related Work

7

## ■ Investigate & Survey

-  AI-Paper-Search (by MLNLP), Google Scholar, etc.



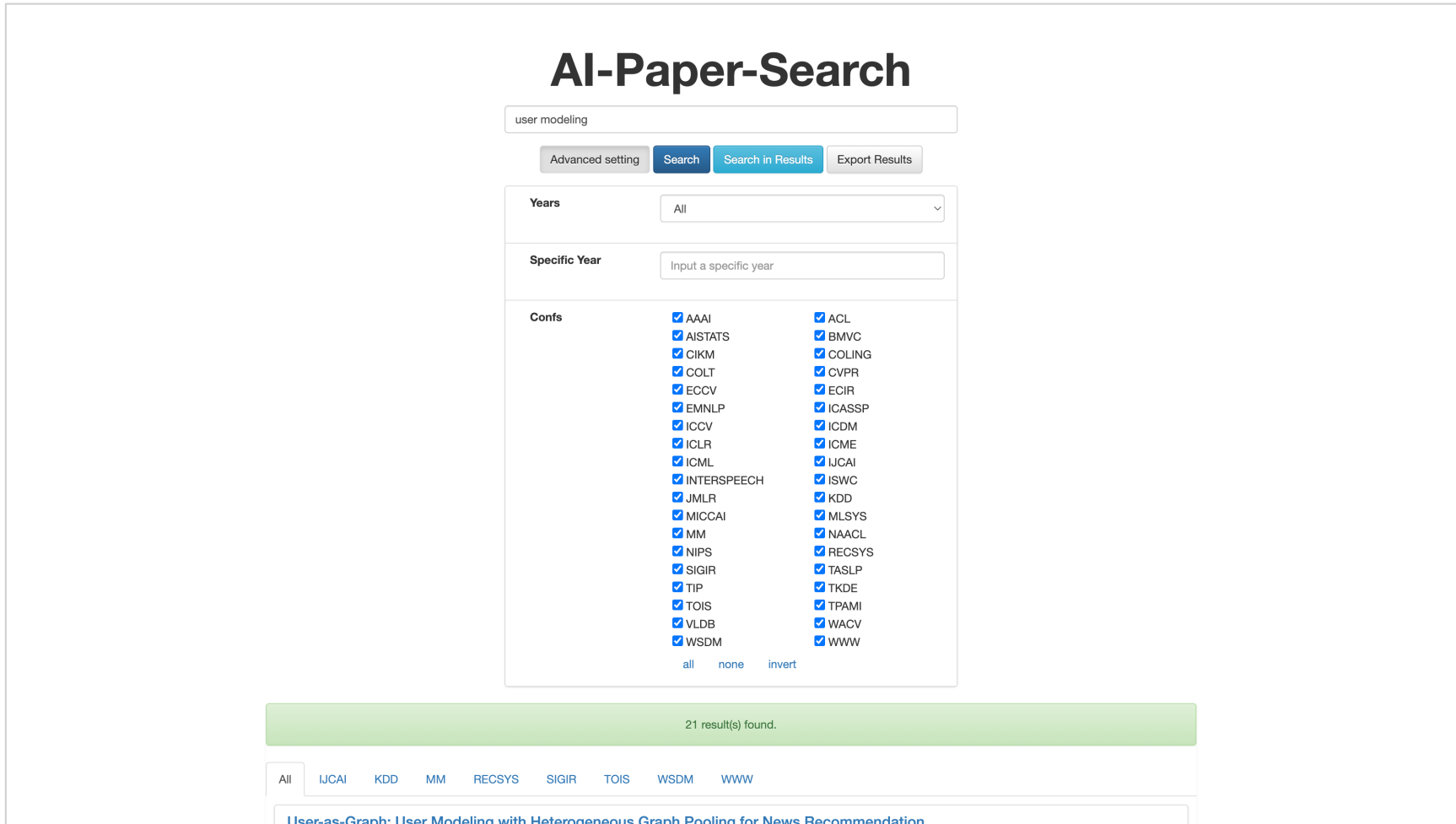
The screenshot displays the AI-Paper-Search interface. At the top, the title "AI-Paper-Search" is centered. Below it is a search input field containing the text "user modeling". To the right of the input field are four buttons: "Advanced setting", "Search", "Search in Results", and "Export Results". A green banner below the search bar indicates "21 result(s) found.". Below this banner is a navigation bar with tabs for "All", "IJCAI", "KDD", "MM", "RECSYS", "SIGIR", "TOIS", "WSDM", and "WWW". The main content area shows a list of search results, each with a title, an "abstract" link, author names, and a conference acronym in a green box. The results are:

- User-as-Graph: User Modeling with Heterogeneous Graph Pooling for News Recommendation.**  
abstract  
Chuhan Wu Fangzhao Wu Yongfeng Huang Xing Xie  
IJCAI2021
- User Modeling with Click Preference and Reading Satisfaction for News Recommendation.**  
abstract  
Chuhan Wu Fangzhao Wu Tao Qi Yongfeng Huang  
IJCAI2020
- A Survey on Representation Learning for User Modeling.**  
abstract  
Sheng Li Handong Zhao  
IJCAI2020
- Adaptive User Modeling with Long and Short-Term Preferences for Personalized Recommendation.**  
abstract  
Zeping Yu Jianxun Lian Ahmad Mahmoody Gongshen Liu Xing Xie  
IJCAI2019
- Log2Intent: Towards Interpretable User Modeling via Recurrent Semantics Memory Unit.**  
abstract  
Zhiqiang Tao Sheng Li Zhaowen Wang Chen Fang Longqi Yang Handong Zhao Yun Fu  
KDD2019

# Introduction & Related Work

## Investigate & Survey

- AI-Paper-Search (by MLNLP), Google Scholar, etc.



The screenshot shows the AI-Paper-Search interface. At the top, the search term "user modeling" is entered in a search box. Below the search box are buttons for "Advanced setting", "Search", "Search in Results", and "Export Results". There are also filters for "Years" (set to "All") and "Specific Year" (with a text input field). A "Confs" section lists 30 conference acronyms, each with a checked checkbox. At the bottom, a green bar indicates "21 result(s) found." and a navigation bar shows "All" selected, along with other conference acronyms: IJCAI, KDD, MM, RECSYS, SIGIR, TOIS, WSDM, WWW. A partial title of a search result is visible at the bottom: "User-as-Graph: User Modelina with Heterogeneous Graph Poolina for News Recommendation."

### AI-Paper-Search

user modeling

Advanced setting Search Search in Results Export Results

Years All

Specific Year Input a specific year

Confs

- AACL
- AISTATS
- CIKM
- COLT
- ECCV
- EMNLP
- ICCV
- ICLR
- ICML
- INTERSPEECH
- JMLR
- MICCAI
- MM
- NIPS
- SIGIR
- TIP
- TOIS
- VLDB
- WSDM
- ACL
- BMVC
- COLING
- CVPR
- ECIR
- ICASSP
- ICDDM
- ICME
- IJCAI
- ISWC
- KDD
- MLSYS
- NAACL
- RECSYS
- TASLP
- TKDE
- TPAMI
- WACV
- WWW

all none invert

21 result(s) found.

All IJCAI KDD MM RECSYS SIGIR TOIS WSDM WWW

User-as-Graph: User Modelina with Heterogeneous Graph Poolina for News Recommendation.



# Introduction & Related Work

9

## ■ Reference Management & Paper Reading

- **Zotero**: reference management
- **Zotero Connector**: browser plugin
- **Zotfile**: automatically rename and move PDF files
- **Nutstore**: synchronize across devices
- **PDF Expert**: access the synchronized files via WebDAV on Pad
- **Notion**: take notes



Zotero



Nutstore



PDF Expert

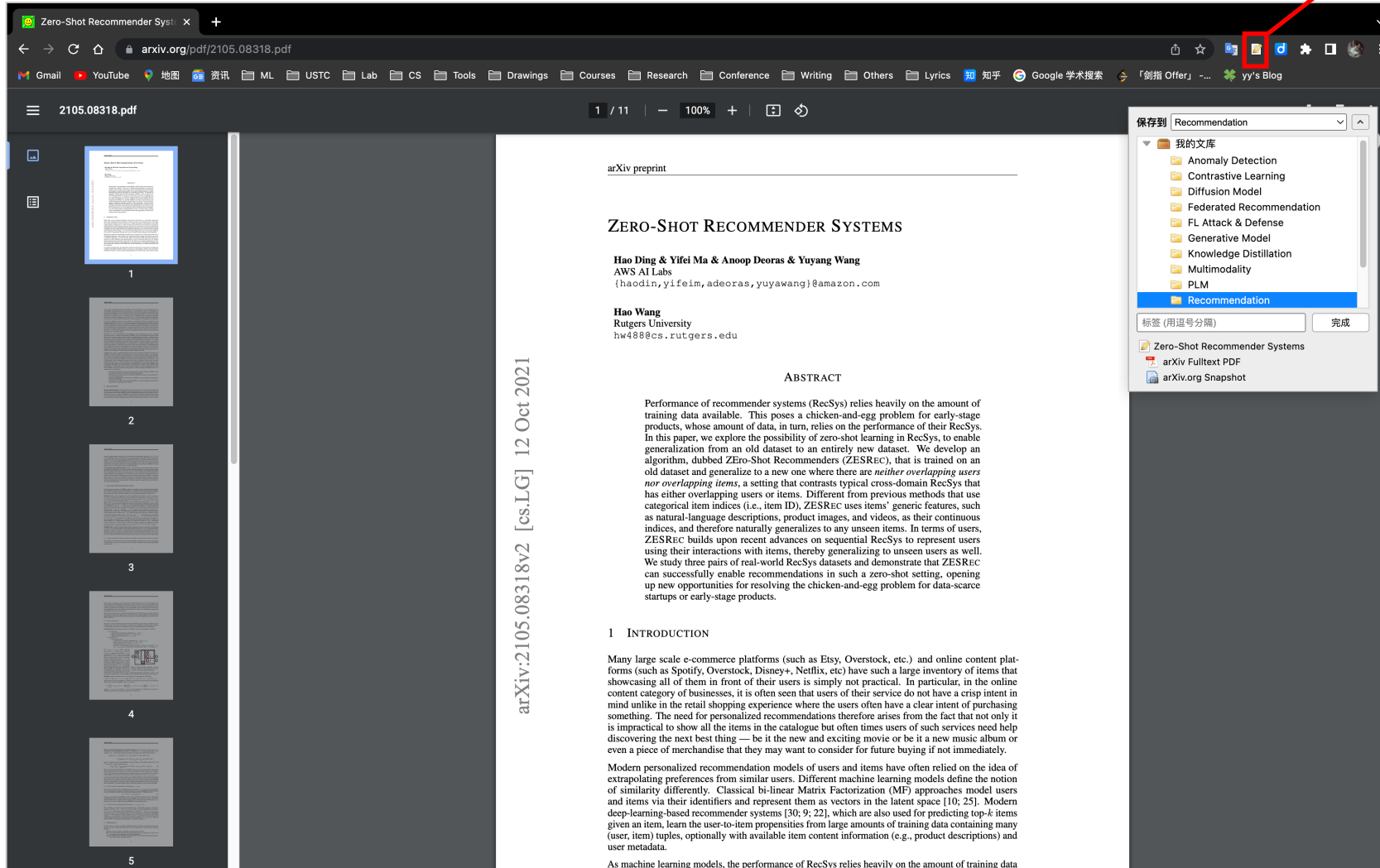


Notion

# Introduction & Related Work

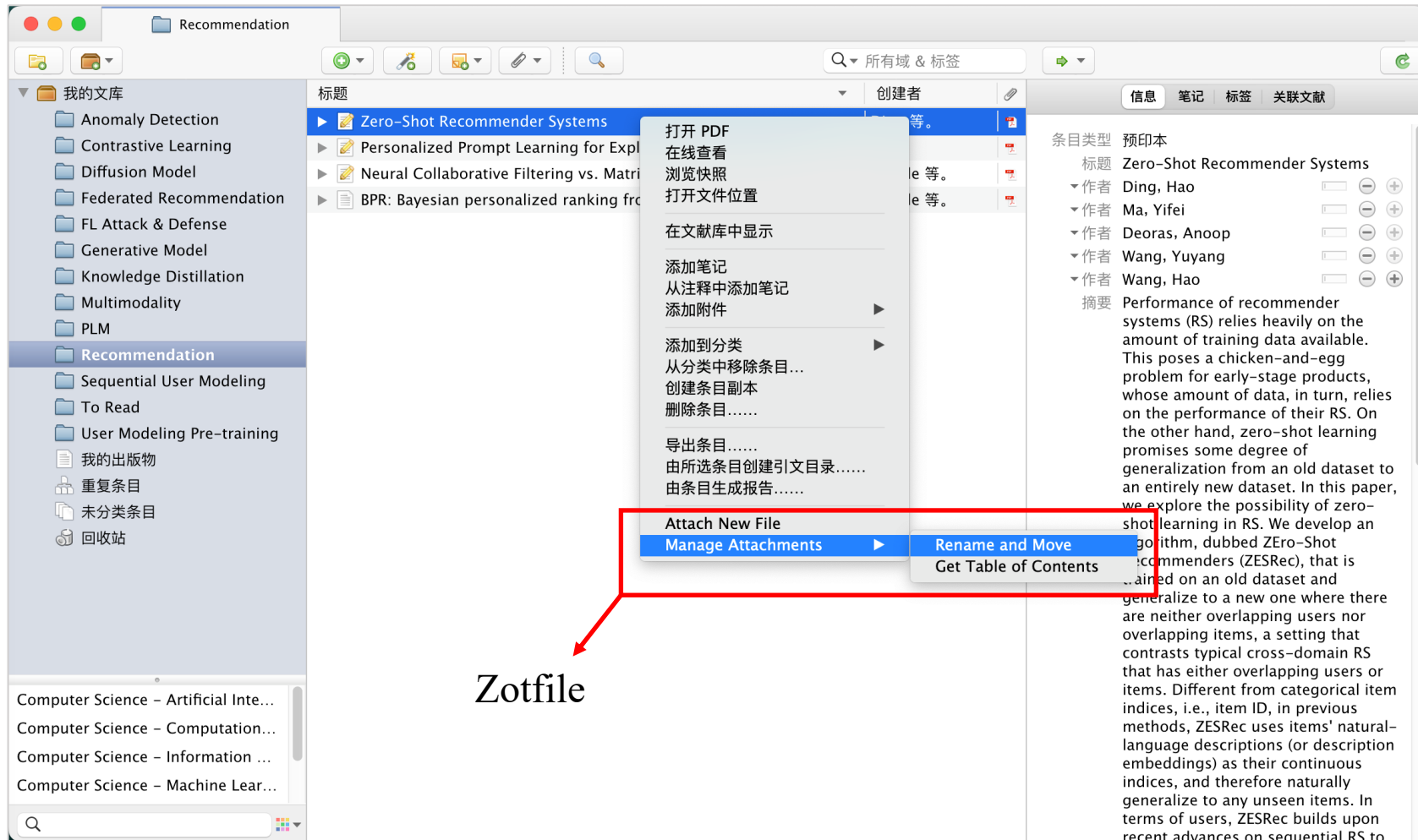
## Reference Management & Paper Reading

Zotero Connector



# Introduction & Related Work

## ■ Reference Management & Paper Reading

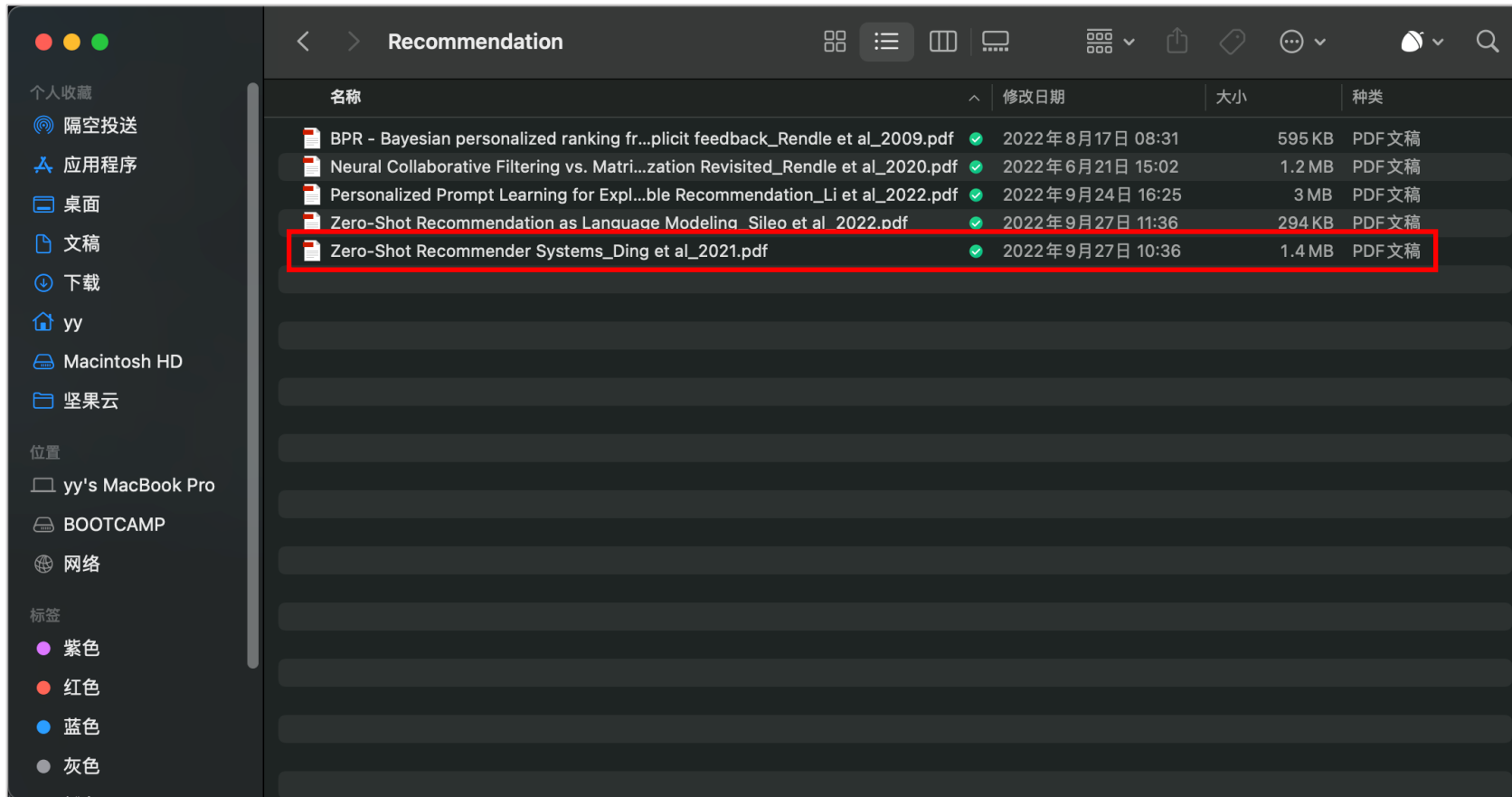


In Zotero

# Introduction & Related Work

12

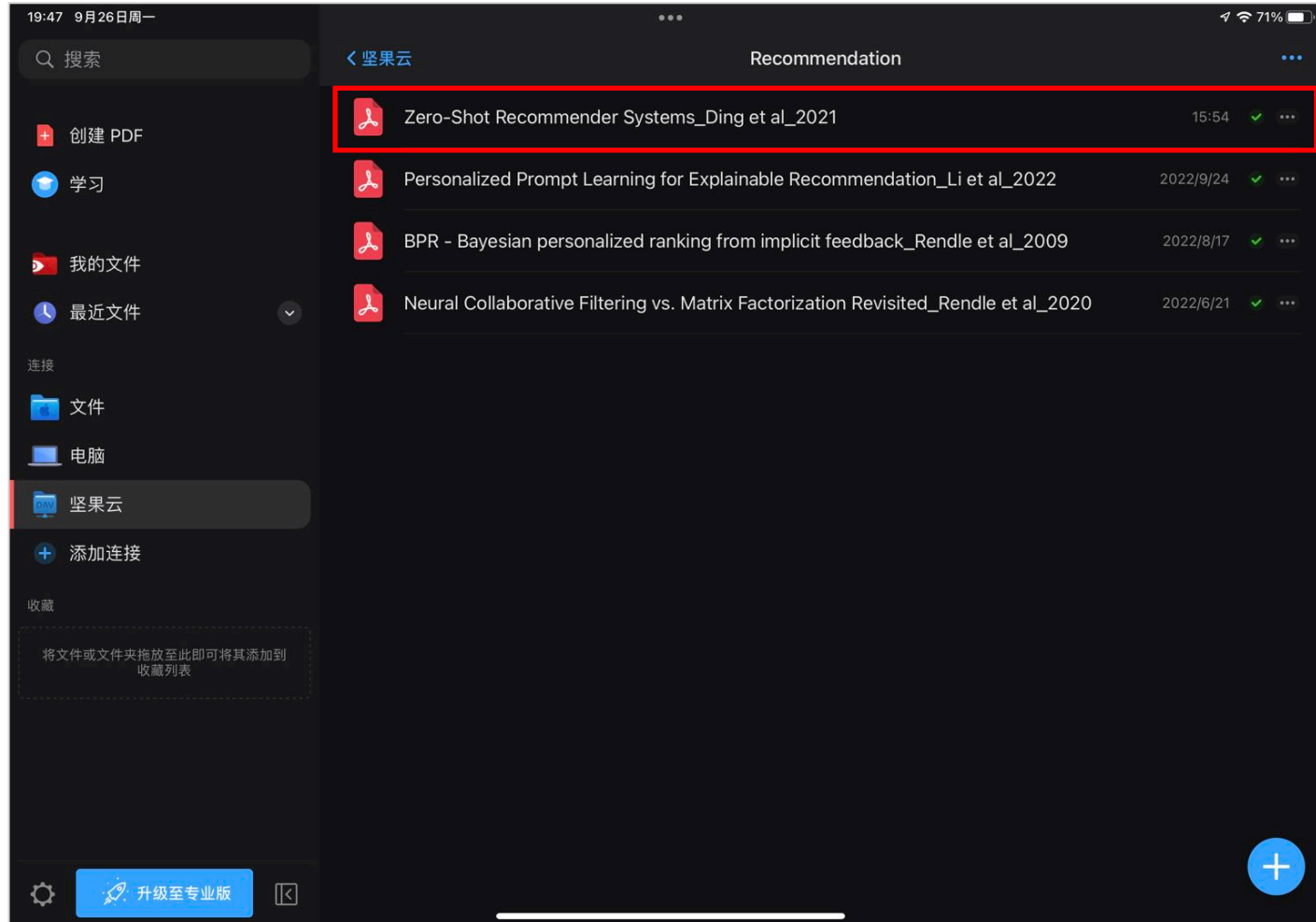
## ■ Reference Management & Paper Reading



# Introduction & Related Work

13

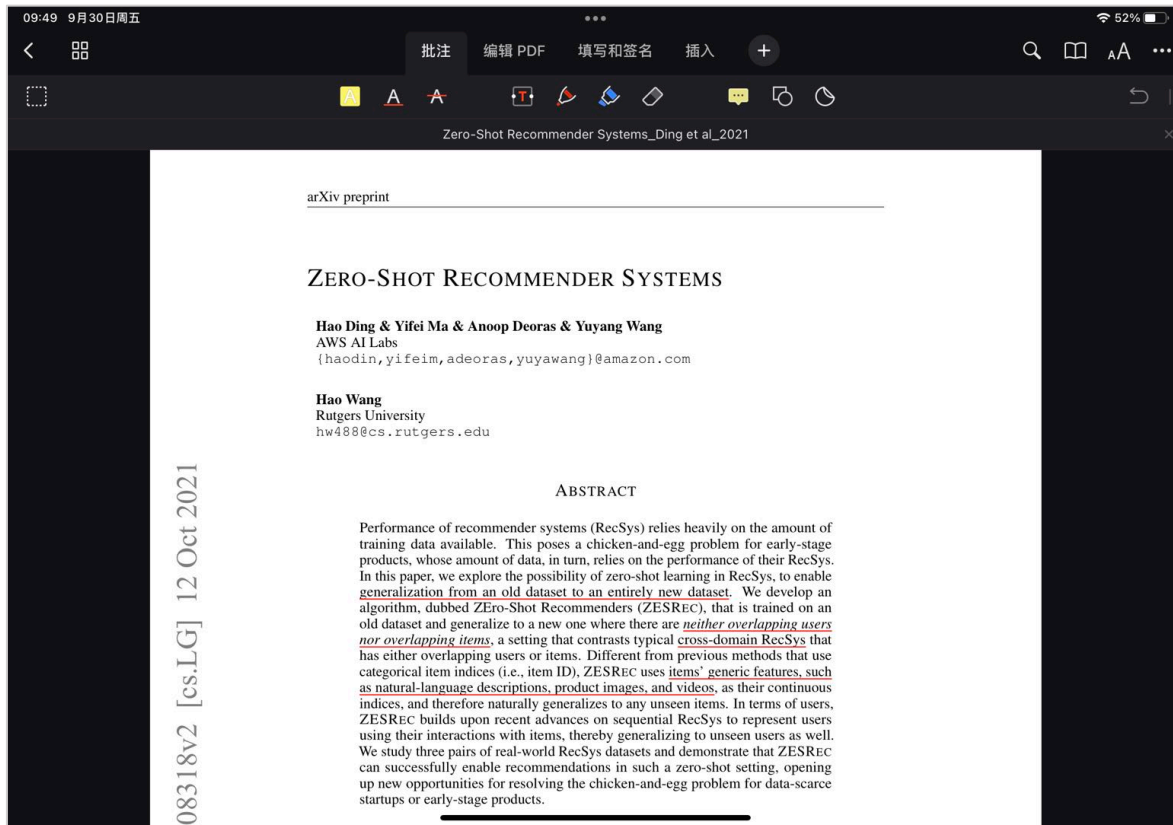
## ■ Reference Management & Paper Reading



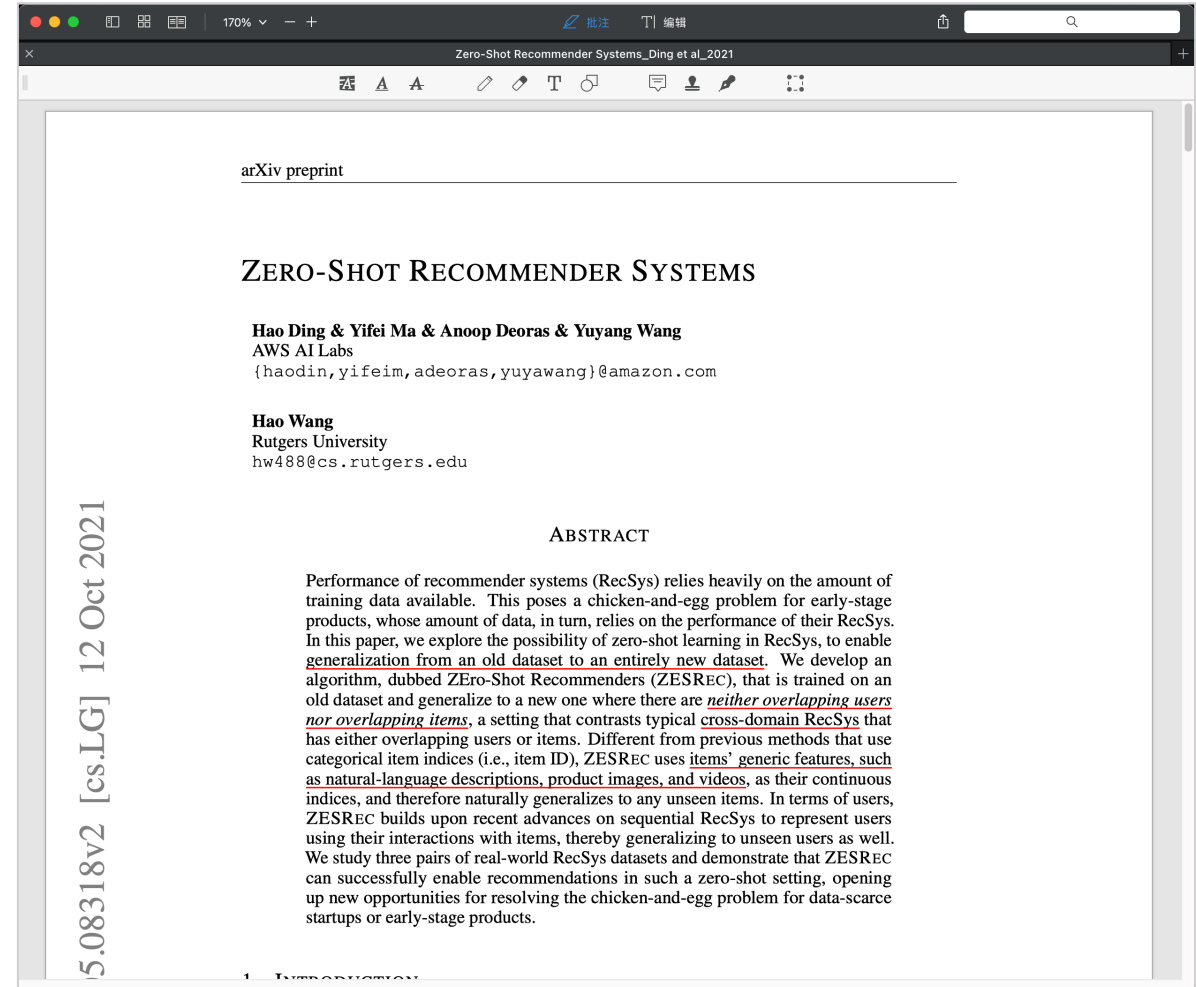
In PDF Expert  
on iPad

# Introduction & Related Work

## ■ Reference Management & Paper Reading



On iPad



On PC

# Outline



15

- Introduction & Related Work
- **Methodology**
- Experiments
- Conclusions

## ■ Drawing

### ▣ Illustrations



PPT



OmniGraffle (for Mac)



Visio (for Windows?)

### ▣ Icons





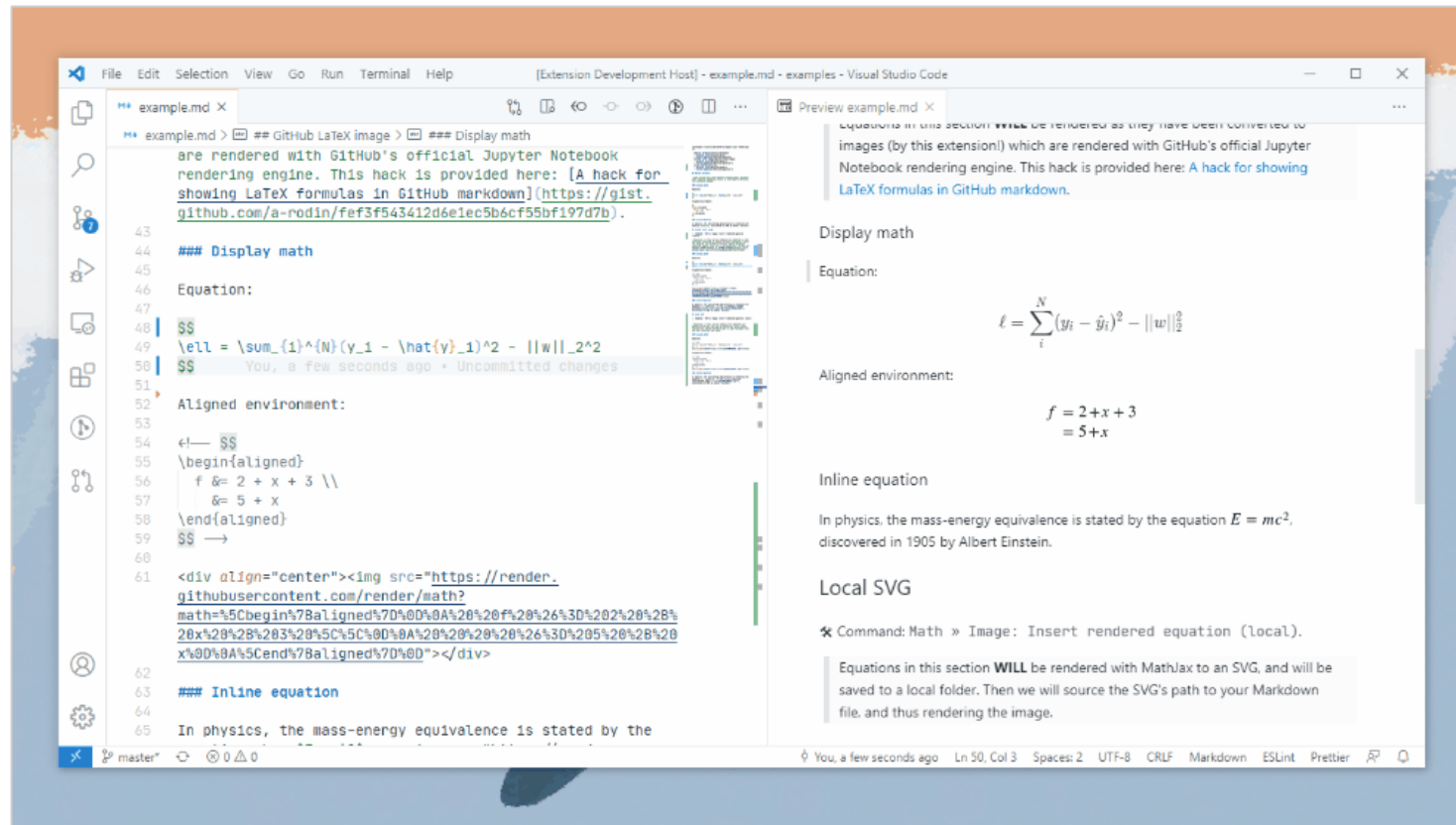
# Methodology

17

## ■ Drawing

### ▣ Equations in Illustrations

- **Math to Image:** Convert LaTeX equations into local SVGs. 👍





# Outline

18

- Introduction & Related Work
- Methodology
- **Experiments**
- Conclusions

## ■ Conducting Experiments

### ▣ Weights & Biases 👍

- Installation: `pip install wandb; wandb login;`
- Usage:

Track, compare, and visualize your ML models with 5 lines of code

Quickly and easily implement experiment logging by adding just a few lines to your script and start logging results. Our lightweight integration works with any Python script.

[TRY A LIVE NOTEBOOK →](#)

 ANY FRAMEWORK

 TENSORFLOW

 PYTORCH

 KERAS

 SCIKIT

 HUGGING FACE

 XGBOOST

```
import wandb

# 1. Start a new run
wandb.init(project="gpt-3")

# 2. Save model inputs and hyperparameters
config = wandb.config
config.learning_rate = 0.01

# 3. Log gradients and model parameters
wandb.watch(model)
for batch_idx, (data, target) in
    enumerate(train_loader):

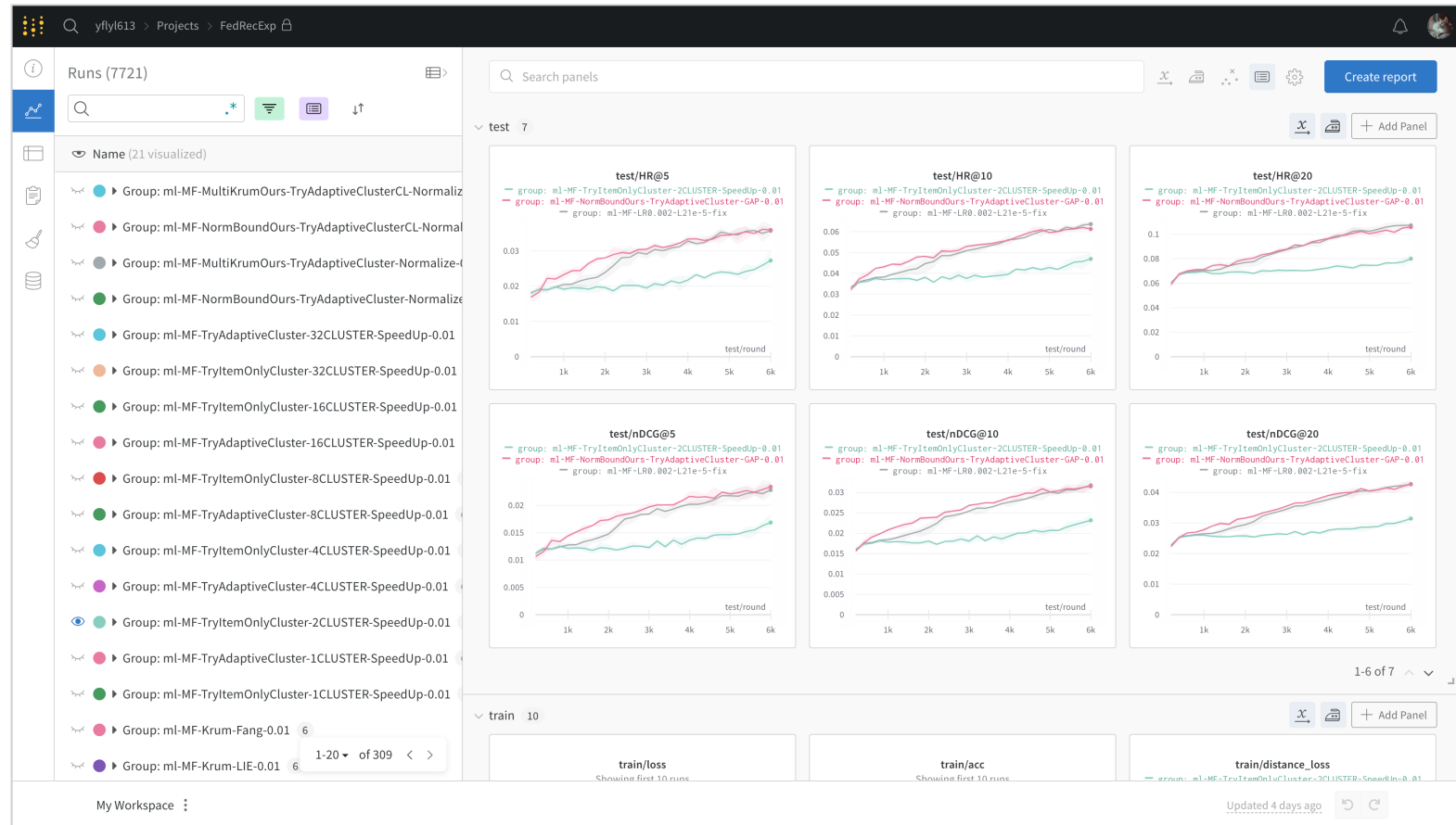
    if batch_idx % args.log_interval == 0:
# 4. Log metrics to visualize performance
wandb.log({"loss": loss})
```

# Experiments

## ■ Conducting Experiments

### ▣ Weights & Biases

#### ➤ Experiment tracking



## ■ Conducting Experiments


### ▣ Weights & Biases

- More than tracking ...

Explore the Weights & Biases platform



The diagram illustrates the features of the Weights & Biases platform. It consists of a dark grey rectangular background with five white hexagonal icons arranged horizontally. Each icon is accompanied by a title and a brief description below it. The icons are: a green flask for 'Experiments', a blue clipboard with a checkmark for 'Reports', three pink stacked disks for 'Artifacts', an orange grid for 'Tables', and a cyan gear with a lightning bolt for 'Sweeps'.

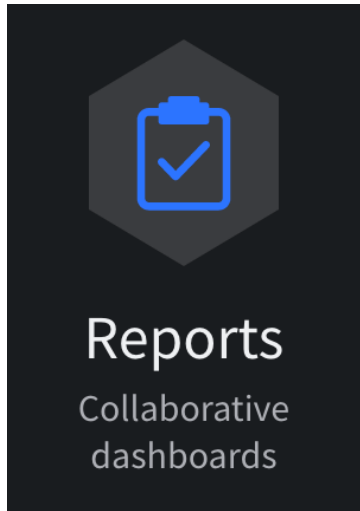
				
<b>Experiments</b>	<b>Reports</b>	<b>Artifacts</b>	<b>Tables</b>	<b>Sweeps</b>
Experiment tracking	Collaborative dashboards	Dataset and model versioning	Interactive data visualization	Hyperparameter optimization

# Experiments

## ■ Conducting Experiments

### □ Weights & Biases

#### ➤ Reports

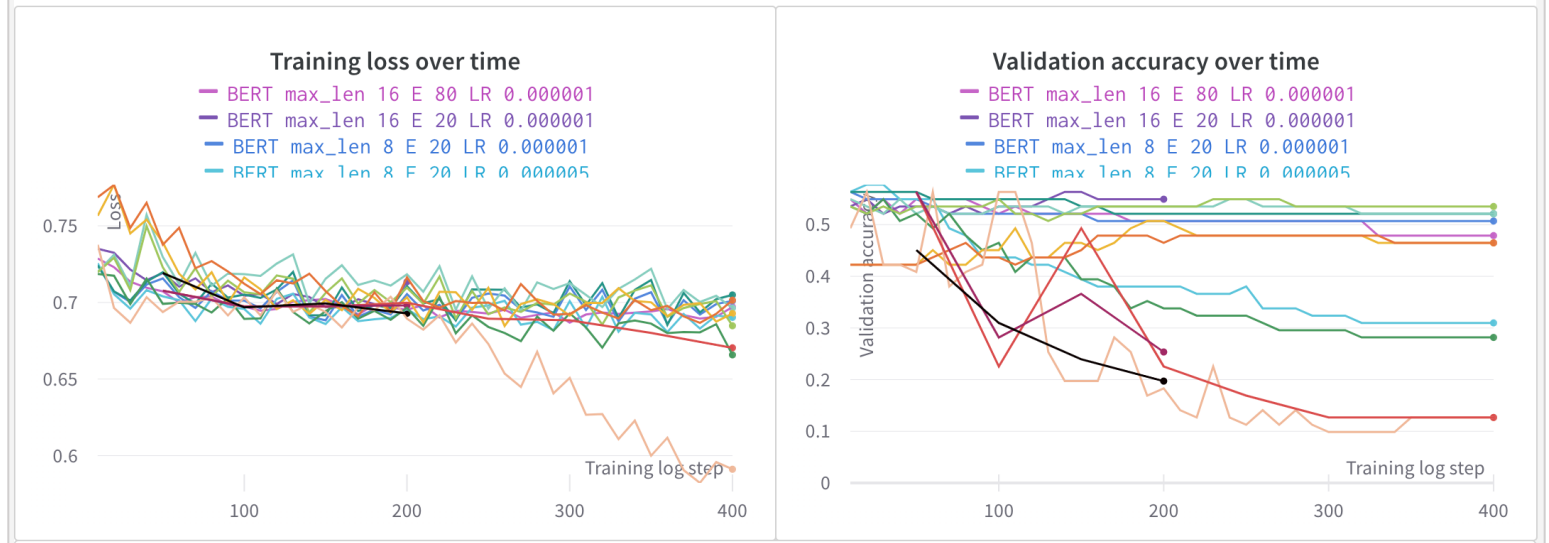


### ▼ First pass: Fine-tuning BERT baseline

### ▼ Short manual hyperparameter exploration

I started with the hyperparameter settings in the [example provided with Transformers](#). Based on the loss and validation accuracy (`eval_acc`) curves plotted in W&B after each run, I adjusted my model to improve performance from a **baseline `eval_acc` of 0.127** to **0.535 in fewer than 20 experiments**.

Below, you can see the training loss and validation accuracy curves plotted over time. The starting baseline is in black, and the rest of the runs are colored in rainbow order from red to purple based on their creation order: my earlier experiments are reds/oranges, and the later experiments are blues/purples. The legend shows the maximum sequence length (`max_len`), training epochs (E), and learning rate (LR) for each run. You can also expand the "BERT variants" run set at the end of this section to see more details about each run.



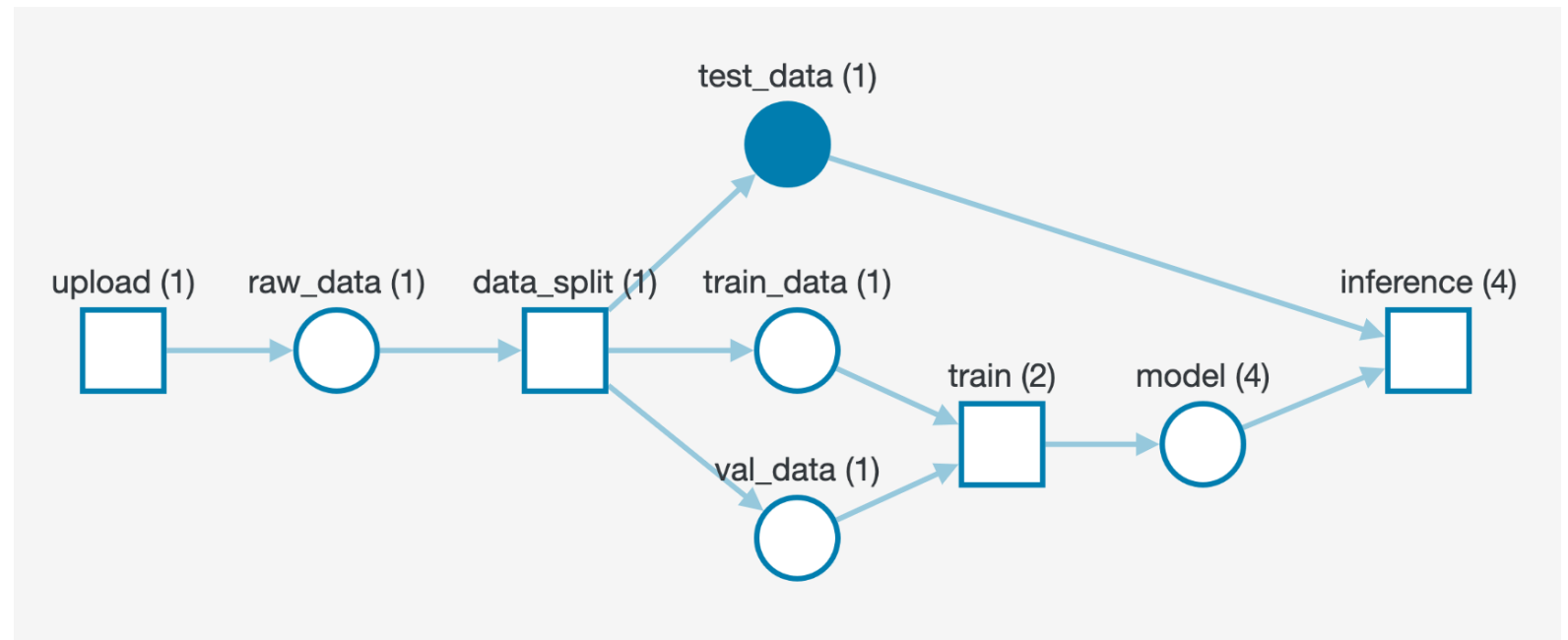
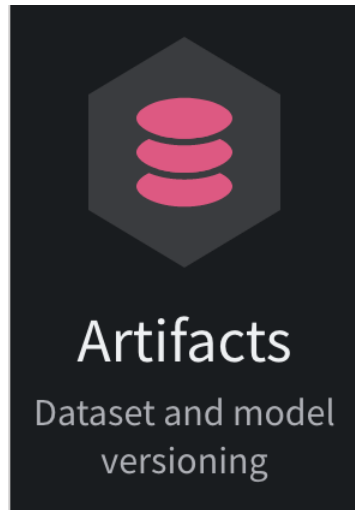
# Experiments

23

## ■ Conducting Experiments

### ▣ Weights & Biases

#### ➤ Artifacts

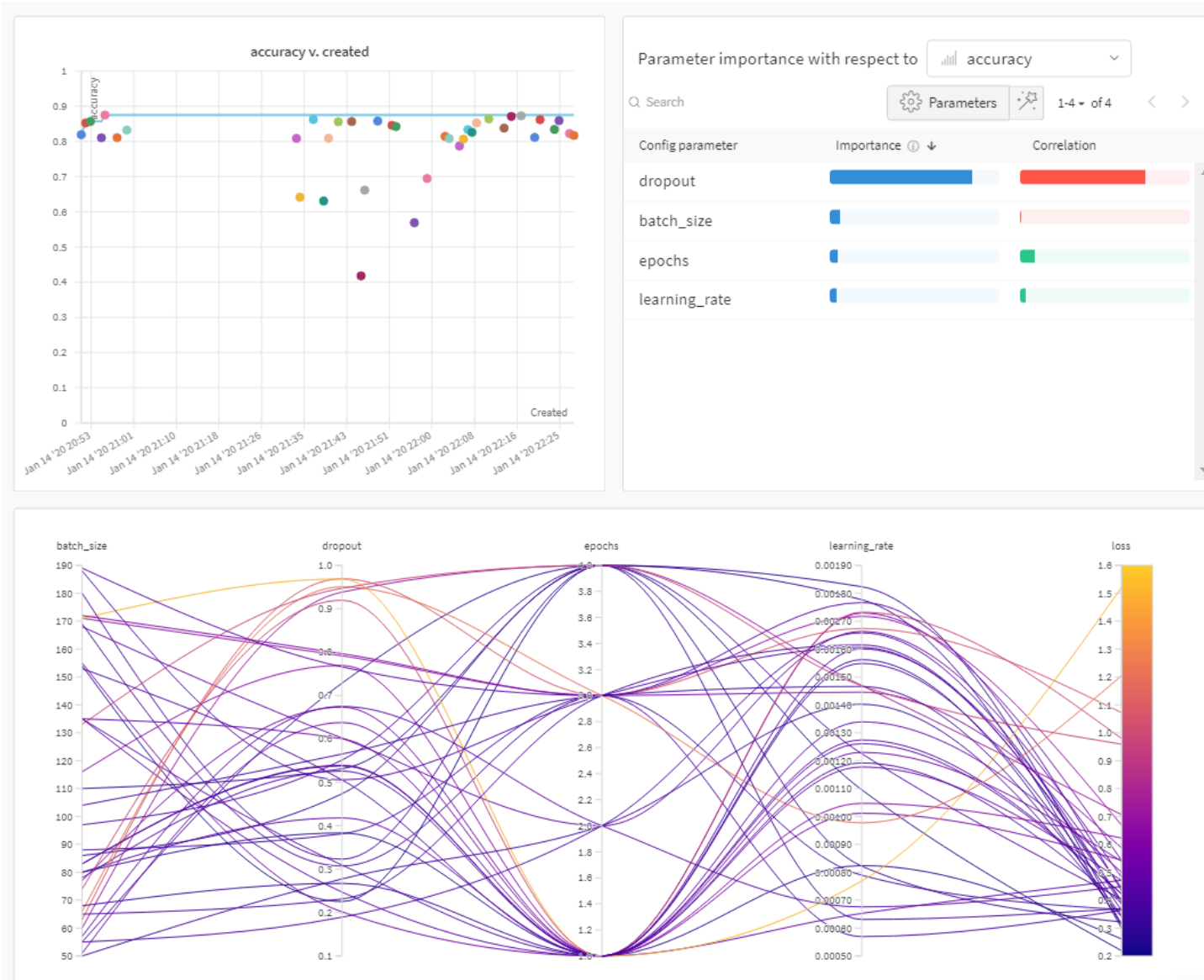
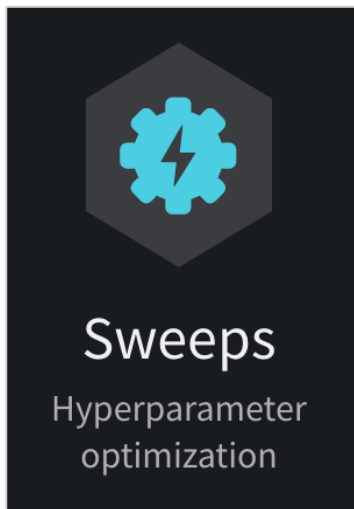


# Experiments

## ■ Conducting Experiments

### □ Weights & Biases

#### ➤ Sweeps





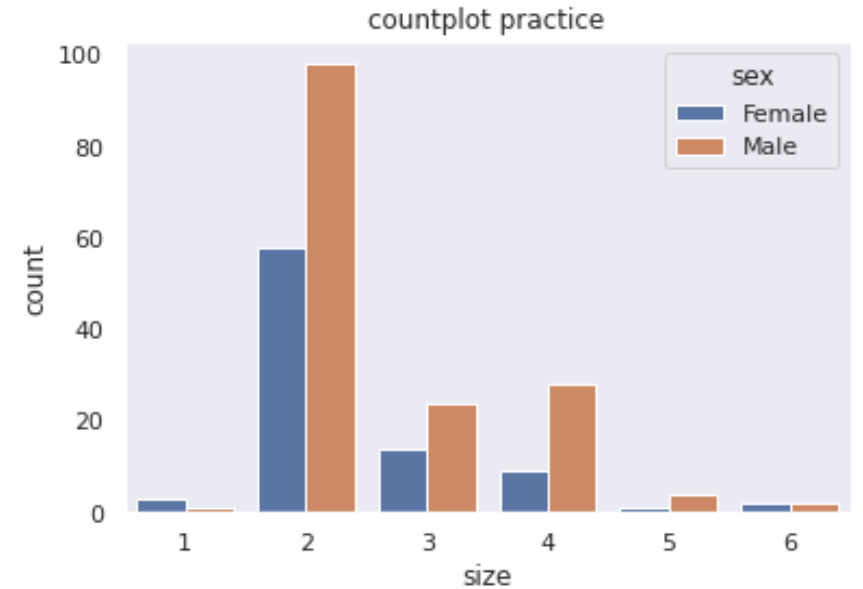
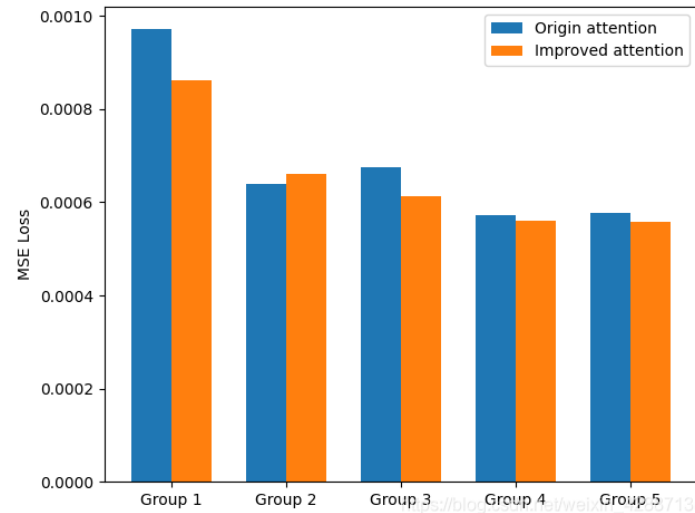
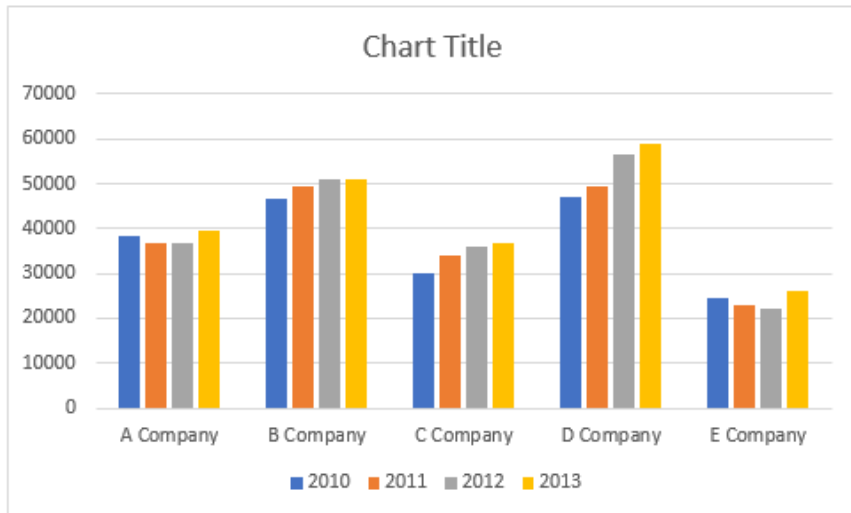
# Experiments



## ■ Experiment Results



seaborn



# Outline



26

- Introduction & Related Work
- Methodology
- Experiments
- **Conclusions**

## ■ Paper Writing with LaTeX

### □ Online LaTeX Editor (Overleaf)

#### ➤ Pros

- ✓ Easy to use (the environment is already installed).
- ✓ Easy for collaboration and synchronization.
- ✓ Track the document history automatically.

#### ➤ Cons

- ✓ Sometimes slow and unstable, especially near the DDL.



# Conclusions

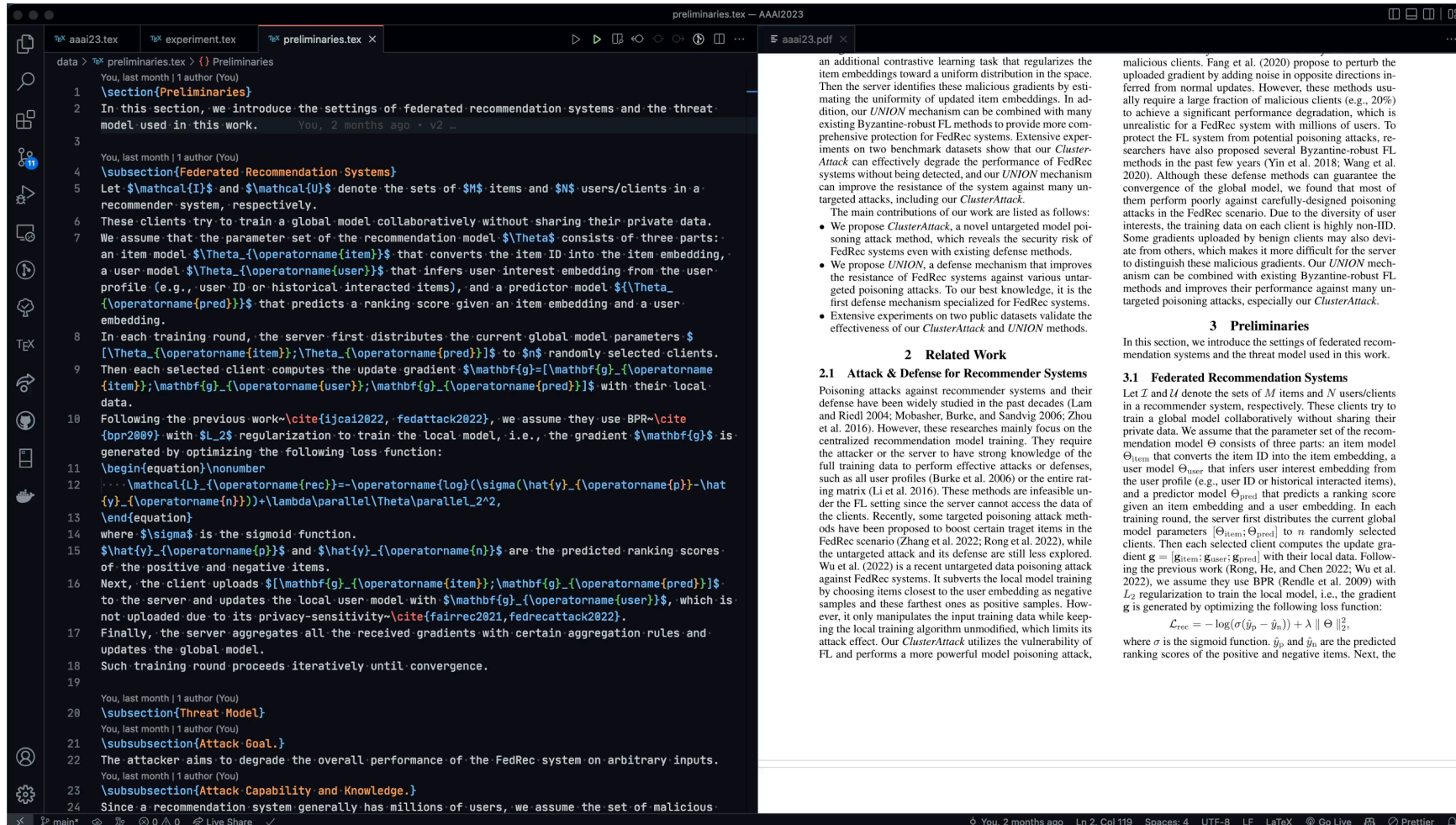
28

## ■ Paper Writing with LaTeX

- ▣ Local LaTeX Editor (MacTeX/TeX Live/MiKTeX + vscode LaTeX Workshop)
  - Pros
    - ✓ Fast and stable.
  - Cons
    - ✓ Setting up the environment for the first time may take some time.

## ■ Paper Writing with LaTeX

### □ Local LaTeX Editor (MacTeX/TeX Live/MiKTeX + vscode LaTeX Workshop)



The screenshot displays the VS Code LaTeX Workshop interface. On the left, the LaTeX source code for 'preliminaries.tex' is shown with line numbers 1 through 24. The code includes sections for Preliminaries, Federated Recommendation Systems, and Threat Model. It describes a federated recommendation system where clients train local models and upload gradients to a server. The server aggregates these gradients to update a global model. The document also discusses an attack goal and the attacker's knowledge.

On the right, the rendered PDF output is visible. It contains the following text:

an additional contrastive learning task that regularizes the item embeddings toward a uniform distribution in the space. Then the server identifies these malicious gradients by estimating the uniformity of updated item embeddings. In addition, our *UNION* mechanism can be combined with many existing Byzantine-robust FL methods to provide more comprehensive protection for FedRec systems. Extensive experiments on two benchmark datasets show that our *ClusterAttack* can effectively degrade the performance of FedRec systems without being detected, and our *UNION* mechanism can improve the resistance of the system against many untargeted attacks, including our *ClusterAttack*.

The main contributions of our work are listed as follows:

- We propose *ClusterAttack*, a novel untargeted model poisoning attack method, which reveals the security risk of FedRec systems even with existing defense methods.
- We propose *UNION*, a defense mechanism that improves the resistance of FedRec systems against various untargeted poisoning attacks. To our best knowledge, it is the first defense mechanism specialized for FedRec systems.
- Extensive experiments on two public datasets validate the effectiveness of our *ClusterAttack* and *UNION* methods.

**2 Related Work**

**2.1 Attack & Defense for Recommender Systems**

Poisoning attacks against recommender systems and their defense have been widely studied in the past decades (Lam and Riedl 2004; Mobasher, Burke, and Sandvig 2006; Zhou et al. 2016). However, these researches mainly focus on the centralized recommendation model training. They require the attacker or the server to have strong knowledge of the full training data to perform effective attacks or defenses, such as all user profiles (Burke et al. 2006) or the entire rating matrix (Li et al. 2016). These methods are infeasible under the FL setting since the server cannot access the data of the clients. Recently, some targeted poisoning attack methods have been proposed to boost certain target items in the FedRec scenario (Zhang et al. 2022; Kong et al. 2022), while the untargeted attack and its defense are still less explored. Wu et al. (2022) is a recent untargeted data poisoning attack against FedRec systems. It subverts the local model training by choosing items closest to the user embedding as negative samples and these farthest ones as positive samples. However, it only manipulates the input training data while keeping the local training algorithm unmodified, which limits its attack effect. Our *ClusterAttack* utilizes the vulnerability of FL and performs a more powerful model poisoning attack,

malicious clients. Fang et al. (2020) propose to perturb the uploaded gradient by adding noise in opposite directions inferred from normal updates. However, these methods usually require a large fraction of malicious clients (e.g., 20%) to achieve a significant performance degradation, which is unrealistic for a FedRec system with millions of users. To protect the FL system from potential poisoning attacks, researchers have also proposed several Byzantine-robust FL methods in the past few years (Yin et al. 2018; Wang et al. 2020). Although these defense methods can guarantee the convergence of the global model, we found that most of them perform poorly against carefully-designed poisoning attacks in the FedRec scenario. Due to the diversity of user interests, the training data on each client is highly non-IID. Some gradients uploaded by benign clients may also deviate from others, which makes it more difficult for the server to distinguish these malicious gradients. Our *UNION* mechanism can be combined with existing Byzantine-robust FL methods and improves their performance against many untargeted poisoning attacks, especially our *ClusterAttack*.

**3 Preliminaries**

In this section, we introduce the settings of federated recommendation systems and the threat model used in this work.

**3.1 Federated Recommendation Systems**

Let  $\mathcal{I}$  and  $\mathcal{U}$  denote the sets of  $M$  items and  $N$  users/clients in a recommender system, respectively. These clients try to train a global model collaboratively without sharing their private data. We assume that the parameter set of the recommendation model  $\Theta$  consists of three parts: an item model  $\Theta_{\text{item}}$  that converts the item ID into the item embedding, a user model  $\Theta_{\text{user}}$  that infers user interest embedding from the user profile (e.g., user ID or historical interacted items), and a predictor model  $\Theta_{\text{pred}}$  that predicts a ranking score given an item embedding and a user embedding. In each training round, the server first distributes the current global model parameters  $\{\Theta_{\text{item}}, \Theta_{\text{pred}}\}$  to  $n$  randomly selected clients. Then each selected client computes the update gradient  $g = [g_{\text{item}}, g_{\text{user}}, g_{\text{pred}}]$  with their local data. Following the previous work (Rong, He, and Chen 2022; Wu et al. 2022), we assume they use BPR (Rendle et al. 2009) with  $L_2$  regularization to train the local model, i.e., the gradient  $g$  is generated by optimizing the following loss function:

$$\mathcal{L}_{\text{rec}} = -\log(\sigma(\hat{y}_p - \hat{y}_n)) + \lambda \|\Theta\|_2^2,$$

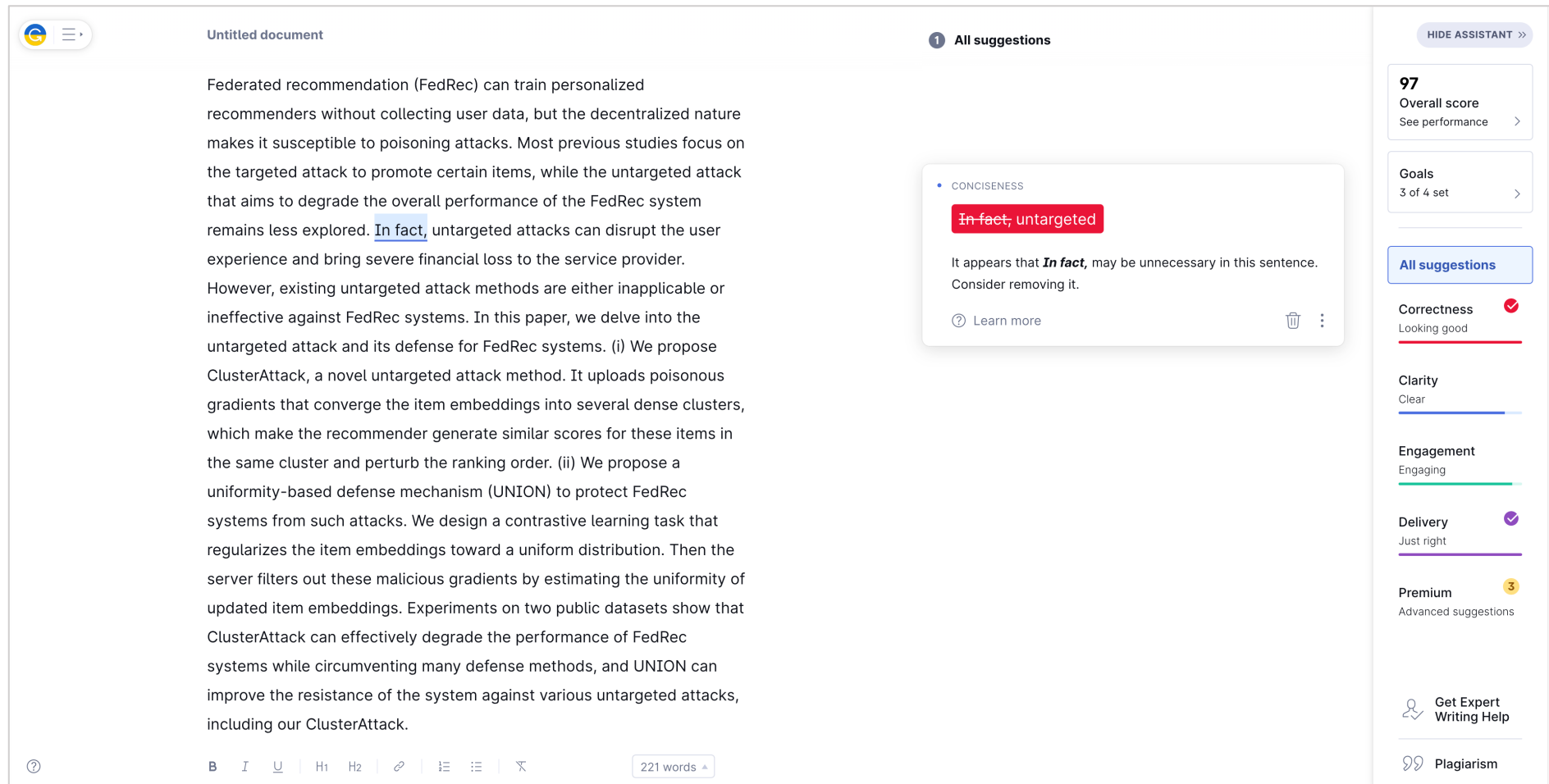
where  $\sigma$  is the sigmoid function,  $\hat{y}_p$  and  $\hat{y}_n$  are the predicted ranking scores of the positive and negative items. Next, the

# Conclusions

30

## ■ English Writing

### □ Grammarly



The screenshot displays the Grammarly interface for an "Untitled document". The main text area contains a paragraph about Federated recommendation (FedRec) systems. A suggestion box highlights the phrase "In fact, untargeted" in red, indicating a conciseness issue. The suggestion text reads: "It appears that **In fact**, may be unnecessary in this sentence. Consider removing it." Below the suggestion is a "Learn more" link and a trash icon.

The right sidebar shows the overall score of 97, with a link to "See performance". It also displays "Goals" (3 of 4 set) and a list of metrics: "Correctness" (Looking good, red checkmark), "Clarity" (Clear, blue progress bar), "Engagement" (Engaging, green progress bar), and "Delivery" (Just right, purple checkmark). At the bottom of the sidebar, there is a "Premium" badge (3) for "Advanced suggestions", a "Get Expert Writing Help" button, and a "Plagiarism" icon.

The bottom of the document editor shows a toolbar with standard text formatting options (bold, italic, underline, heading, link, list, indent, undo, redo) and a word count of 221 words.

# Conclusions



31

## ■ English Writing

### □ QuillBot

Modes: Standard Fluency Formal Simple Creative Expand Shorten Synonyms:

82 Words Rephrase 1/4 Sentences • 84 Words

● Changed Words — Structural Changes ● Longest Unchanged Words ⓘ

Federated recommendation (FedRec) can train personalized recommenders without collecting user data, but the decentralized nature makes it susceptible to poisoning attacks. Most previous studies focus on the targeted attack to promote certain items, while the untargeted attack that aims to degrade the overall performance of the FedRec system remains less explored. In fact, untargeted attacks can disrupt the user experience and bring severe financial loss to the service provider. However, existing untargeted attack methods are either inapplicable or ineffective against FedRec systems.

Without user data, Federated Recommendation (FedRec) can train individualized recommenders, but because it is decentralized, it is vulnerable to poisoning attempts. The majority of earlier research has concentrated on targeted attacks meant to promote certain products, but untargeted attacks meant to harm the FedRec system's overall performance have received less attention. Untargeted attacks can actually ruin the user experience and cost the service provider a lot of money. On the other hand, FedRec systems are inaccessible to or ineffectual against current untargeted attack techniques.

# Conclusions

## ■ English Writing



### ▣ DeepL, Academic Phrasebank, etc.



**GENERAL LANGUAGE FUNCTIONS**

- Being cautious
- Being critical
- Classifying and listing
- Compare and contrast
- Defining terms
- Describing trends
- Describing quantities
- Explaining causality
- Giving examples
- Signalling transition
- Writing about the past

An enhanced and expanded version of PHRASEBANK is available in PDF or Kindle format:

[ABOUT PHRASEBANK](#)

### Being critical

As an academic writer, you are expected to be critical of the sources that you use. This essentially means questioning what you read and not necessarily agreeing with it just because the information has been published. Being critical can also mean looking for reasons why we should not just accept something as being correct or true. This can require you to identify problems with a writer's arguments or methods, or perhaps to refer to other people's criticisms of these. Constructive criticism goes beyond this by suggesting ways in which a piece of research or writing could be improved.

*... being against is not enough. We also need to develop habits of constructive thinking.*  
Edward de Bono

---

— Highlighting inadequacies of previous studies

Previous studies of X have not dealt with ...  
 Researchers have not treated X in much detail.  
 Such expositions are unsatisfactory because they ...  
 Most studies in the field of X have only focused on ...  
 Such approaches, however, have failed to address ...  
 Previous published studies are limited to local surveys.  
 Half of the studies evaluated failed to specify whether ...  
 The research to date has tended to focus on X rather than Y.  
 Previously published studies on the effect of X are not consistent.  
 Smith's analysis does not take account of ..., nor does she examine ...  
 The existing accounts fail to resolve the contradiction between X and Y.  
 Most studies of X have only been carried out in a small number of areas.  
 However, much of the research up to now has been descriptive in nature ...  
 The generalisability of much published research on this issue is problematic.  
 Research on the subject has been mostly restricted to limited comparisons of ...  
 However, few writers have been able to draw on any systematic research into ...  
 Short-term studies such as these do not necessarily show subtle changes over time ...  
 Although extensive research has been carried out on X, no single study exists which ...  
 However, these results were based upon data from over 30 years ago and it is unclear if ...  
 The experimental data are rather controversial, and there is no general agreement about ...

---

+ Identifying a weakness in a single study or paper





**Thanks!**  
**Q&A**