Towards Secure and Robust Recommender Systems: A Data-Centric Perspective

Zongwei Wang
zongwei@cqu.edu.cn
Chongqing University
Chongqing, China

Junliang Yu
jl.yu@uq.edu.au
The University of Queensland
Brisbane, Australia

Tong Chen
tong.chen@uq.edu.au
The University of Queensland
Brisbane, Australia

Hongzhi Yin
h.yin1@uq.edu.au
The University of Queensland
Brisbane, Australia

Shazia Sadiq
shazia@eecs.uq.edu.au
The University of Queensland
Brisbane, Australia

Min Gao*
gaomin@cqu.edu.cn
Chongqing University
Chongqing, China

ABSTRACT

As recommender systems (RS) continue to evolve, the field has seen a pivotal shift from model-centric to data-centric paradigms, where the quality, integrity, and security of data are increasingly becoming the key drivers of system performance and personalization. This transformation has unlocked new avenues for more precise recommendations, yet it also introduces significant challenges. As reliance on data intensifies, RS face mounting threats that can compromise both their effectiveness and user trust. These challenges include (1) Malicious Data Manipulation, where adversaries corrupt or tamper with datasets, distorting recommendation outcomes and undermining system reliability; (2) Data Privacy Leakage, where adversarial actors exploit system outputs to infer sensitive user information, leading to serious privacy concerns; and (3) Erroneous Data Noise, where inaccuracies, inconsistencies, and redundant data obscure the true user preferences, degrading recommendation quality and user satisfaction. By focusing on these critical data-centric challenges, this tutorial aims to equip participants with the knowledge to build RS that are secure, privacy-preserving, and resilient to data-driven threats, ensuring reliable and trustworthy performance in real-world environments. In addition, attendees will gain hands-on experience with our newly released toolkit for RS-based attacks and defenses, providing them with practical, actionable insights into safeguarding RS against emerging vulnerabilities.

CCS CONCEPTS

• **Information systems** → **Recommender systems**.

KEYWORDS

Recommender System, Data-Centric, Security, Robustness

* Corresponding author

WSDM '25, March 10–14, 2025, Hannover, Germany

ACM ISBN 979-8-4007-1329-3/25/03
https://doi.org/10.1145/3701551.3703484

ACM Reference Format:
Zongwei Wang, Junliang Yu, Tong Chen, Hongzhi Yin, Shazia Sadiq, and Min Gao. 2025. Towards Secure and Robust Recommender Systems: A Data-Centric Perspective. In *Proceedings of the Eighteenth ACM International Conference on Web Search and Data Mining (WSDM '25), March 10–14, 2025, Hannover, Germany*. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3701551.3703484

COVER SHEET

Tutorial Length. The tutorial lasts for 3 hours, plus a 20-min break.

Intended Audience. This tutorial is suitable for attendees with intermediate knowledge of RS, but also accessible to those with basic familiarity in data mining. No advanced expertise is required.

Relevant Tutorials. There is only one relevant prior tutorial, which provides an introduction and future outlook on the comprehensive landscape of trustworthy RS[1]. In contrast, our tutorial specifically focuses on secure and robust RS, delivering an in-depth analysis from a data-centric perspective.

Brief Biography of Presenters:

- **Prof. Hongzhi Yin** is an ARC Future Fellow, Full Professor, and the Director of the Responsible Big Data Intelligence Lab at The University of Queensland. He has published 300+ papers with an H-index of 77, making notable contributions to RS. He has rich lecture experience and taught five relevant courses. He has also delivered 20+ keynotes and tutorials at the top-tier conferences like WWW, DASFAA, and KDD.
- **Mr. Zongwei Wang** is currently pursuing his Ph.D. at Chongqing University and is a visiting student at The University of Queensland. His research has been published on top data mining conferences such as KDD, TIST, WSDM, etc. He has presented his work at multiple top-tier conferences, such as KDD and PAKDD.
- **Dr. Junliang Yu** is an ARC DECRA Fellow at the University of Queensland, specializing in RS, data-centric AI, and graph learning. With over 30 publications in premier venues, he has presented his work at multiple top-tier conferences. He has also delivered lectures at summer schools, taught courses on RS and social media analytics, and organized two highly acclaimed tutorials on self-supervised RS at WWW'22 and DASFAA'23.
- **Dr. Tong Chen** is a Senior Lecturer and ARC DECRA Fellow at The University of Queensland. His research on lightweight,

[1] https://advanced-recommender-systems.github.io/trustworthiness-tutorial/

on-device, and trustworthy RS has been published on top-tier international venues such as KDD, SIGIR, WWW, TKDE, and TOIS. He has ample track records in lecturing, witnessed by his teaching experience in data science, as well as invited tutorials on cutting-edge RS at the WWW'22,24, and DASFAA'23.

- **Prof. Shazia Sadiq** is a Full Professor at The University of Queensland. Her research focuses on responsible data management and aims to reduce the socio-technical barriers to data-driven transformation. She is the Fellow of the Australian Academy of Technological Sciences and Engineering. Throughout her 25-year career, she has received numerous invitations to speak at prestigious conferences, academic institutions, and industry forums, delivering over 20 tutorials, talks, panels, and keynotes.
- **Prof. Min Gao** works as a Full Professor at Chongqing University, China. She has published 100+ papers, making notable contributions to RS and data mining. She also has rich lecture experience and taught three relevant courses, such as Advanced Machine learning, Computer Networks, and Advanced Databases, and has presented her work at multiple top-tier conferences.

1 MOTIVATION AND TARGET AUDIENCE

Advanced recommender systems (RS) have become essential tools for mitigating information overload in various real-world applications. Over the past few years, recommendation models have undergone substantial evolution, moving from traditional collaborative filtering techniques [10, 18, 46] to more sophisticated approaches grounded in deep learning [5, 6, 22, 33]. However, as these models expand in both size and complexity, the primary bottleneck impeding further improvements in recommendation is increasingly shifting from model architecture to the quality of the underlying recommendation data. In response, rather than exclusively concentrating on model development, an emerging trend among researchers has driven a notable shift toward data-centric methodologies in the field. This transition represents a pivotal advancement in the evolution of data-centric RS, where the refinement of data quality is prioritized as a key driver of system performance [11].

The fundamental premise of data-centric RS is that the quality of the data ultimately determines the upper limits of a model's performance, as high-quality recommendation data allows RS to better align with users' expectations and needs [7, 40, 47]. While improving data quality is essential for enhancing the effectiveness of recommendations, ensuring the security and robustness of that data is equally critical for maintaining the reliability and trustworthiness of RS [4, 19, 21, 37, 45, 51]. Vulnerabilities in data, such as malicious manipulation, privacy breaches, or noise introduction, can severely lead to unreliable or biased recommendations. Moreover, in real-world applications where users increasingly rely on RS for decision-making, even minor data issues can erode trust in the system. In this context, as researchers continue to prioritize data-centric approaches, the focus on both data security and robustness becomes paramount, shaping the future landscape of RS research.

This tutorial is designed for a broad audience, including academic and industrial researchers, graduate students, and practitioners from the recommendation field and related areas. By the end of the tutorial, participants will have a solid understanding of basic poisoning attacks and defensive strategies to enhance the security and robustness of RS. Additionally, they will gain hands-on experience using an open-source toolkit. While prior knowledge of recommendation systems is preferred, the tutorial will also cover foundational concepts to ensure better engagement and accessibility for all attendees.

2 OUTLINE OF THE TOPICS TO BE COVERED

This tutorial seeks to provide a comprehensive introduction to secure and robust recommendations by focusing on three key aspects from a data-centric perspective, while also outlining future directions for advancing this field.

(1) Securing Data Integrity - Defending Against Malicious Manipulation in RS. In data-centric RS, the integrity of recommendation data is crucial for ensuring reliable performance and trustworthy outcomes. Attackers, however, can target this data by corrupting training datasets or manipulating model gradients, ultimately distorting recommendation results and undermining system performance [14, 20, 32]. These attacks exploit weaknesses in the data pipeline, from data collection to model training, introducing biases that lead to inaccurate or skewed recommendations. From a data-centric perspective, protecting the integrity of recommendation data is essential. Attackers strategically select data points to corrupt or manipulate gradients, which highlights the importance of understanding how these malicious interventions can influence the system's decision-making process [2, 12]. By identifying and analyzing these vulnerabilities, more robust strategies can be developed to safeguard data integrity. Furthermore, defensive measures such as data validation, anomaly detection, and adversarial training are being employed to enhance the resilience of RS against data-centric attacks, ensuring system reliability and robustness in the face of adversarial manipulation [1, 8, 30].

In this tutorial, a comprehensive framework will be presented that encompasses both the understanding of potential vulnerabilities and the development of strategies to protect the integrity of recommendation data. The framework will explore the various methods attackers use to corrupt or manipulate data, along with the defensive techniques employed to counter these threats.

(2) Preserving Data Privacy – Defending Against Adversarial Inference in RS: In data-centric RS, protecting user privacy is critical, yet increasingly challenging as adversarial inference attacks become more sophisticated [3, 35, 38, 42]. These attacks exploit the rich data generated by RS to uncover sensitive information. For example, membership inference attacks allow adversaries to determine whether a particular user's data was included in the training set, while attribute inference attacks enable the extraction of private user attributes that were meant to remain undisclosed [13, 31, 36, 41]. Such breaches compromise user trust and present significant ethical and legal challenges in deploying RS.

This tutorial will provide an in-depth exploration of these privacy attacks, focusing on how adversaries exploit vulnerabilities in the data pipeline of RS to compromise user privacy. By examining membership and attribute inference attacks, participants will gain a deeper understanding of how sensitive data can be extracted from RS outputs. To counter these threats, various defense mechanisms will be discussed, including data obfuscation, limiting information

leakage, and the integration of privacy-preserving techniques during both training and inference phases.

(3) Managing Data Noise – Overcoming the Impact of Inaccurate and Redundant Data in RS: In data-centric RS, the quality of data directly influences the accuracy of predictions and overall user satisfaction. Data noise that arises from inaccurate, redundant, or irrelevant information can significantly degrade system performance by introducing inconsistencies that obscure user preferences [9, 48, 49]. This noise comes from many sources, including repeated interactions, cross-platform preference inconsistencies, or even intentionally injected malicious data [17, 28, 29]. Addressing data noise is essential for maintaining the reliability of RS in data-centric environments, where system success hinges on data quality.

This tutorial will provide a systematic investigation into the origins of noisy data in RS and introduce corresponding solutions to filter and mitigate its effects. Solutions will be explored across multiple approaches aimed at identifying, filtering, and minimizing the impact of noisy data on RS. These include techniques for selecting high-quality data, adjusting training processes to be more resilient to noise, and refining datasets to focus on the most relevant and informative data.

(4) Research Limitations and Future Opportunities: Despite recent progress, current data-centric research on secure and robust RS still faces several limitations, presenting ample opportunities for further investigation. In this tutorial, we will highlight the gaps in existing studies and propose innovative directions to advance the field of secure and robust RS. Moreover, we will explore how the integration of large language models (LLMs) can introduce new dimensions to these systems, offering a promising avenue for enhancing both their security and robustness. By identifying these key areas for future research, we aim to pave the way for the continued development of more secure and robust RS.

3 RELEVANCE TO THE COMMUNITY AND REFERENCES TO RELATED RESOURCES

Our team is recognized as a pioneer in the field of robust and secure recommender systems, consistently contributing to both academic and practical advancements in this domain. Over the years, our work on secure and reliable recommendation systems, in collaboration with co-authors, has been published in top-tier venues such as KDD, WWW, SIGIR, TKDE, WSDM, and TOIS, significantly influencing the research community. Beyond academic publications, we actively contribute to the broader RS community by developing open-source frameworks[2][3][4] for benchmarking recommender systems, which have collectively garnered over 2,000 stars on GitHub. These contributions reflect our dedication to supporting the growth and adoption of secure, privacy-preserving, and resilient recommender systems within the community.

- Securing data integrity: [15, 23, 26, 27, 34, 39, 43, 50].
- Preserving Data Privacy: [3, 35, 36, 38, 42, 45].
- Managing Data Noise [24, 44].
- Two survey papers on secure recommendation [16, 25].
- ARLib - A toolkit for secure and robust recommendation.

[2] https://github.com/Coder-Yu/QRec
[3] https://github.com/Coder-Yu/SELFRec
[4] https://github.com/CoderWZW/ARLib

4 FORMAT AND DETAILED SCHEDULE

The tutorial is delivered as a lecture-style tutorial with extra hands-on experience (3 hours in duration plus a 20-min break). The schedule and detailed organization of the topics are as follows.

I. Introduction (20 mins)

(1) Overview of Recommender Systems (5 mins)
(2) Introduction of Data-Centric Recommender Systems and its confronted Issues (15 mins)

II. Securing Data Integrity - Defending Against Malicious Manipulation in Recommender Systems (40 mins)

(1) Types of Malicious Manipulation Attacks (20 mins)
(2) Defense Against Malicious Manipulation Attacks (20 mins)

III. Preserving Data Privacy – Defending Against Adversarial Inference in Recommender Systems (40 mins)

(1) Types of Inference Attacks against Data Privacy (20 mins)
(2) Data Privacy-Preserving Methods (20 mins)

IV. Managing Data Noise – Overcoming the Impact of Inaccurate and Redundant Data in Recommender Systems (40 mins)

(1) Origins and Types of Data Noises (20 mins)
(2) Data Denoising Methods (20 mins)

V. Research Limitations and Future Opportunities (20 mins)

(1) Extension of Existing Research Questions (10 mins)
(2) Security of Large Language Models-Driven Recommender Systems (10 mins)

VI. Open-source Toolkit for Robust and Secure Recommendation (20 mins)

5 TYPE OF SUPPORT MATERIALS TO BE SUPPLIED TO ATTENDEES.

The tutorial materials, including the slides and video recordings, will be made available online in advance for attendees via the tutorial homepage[5] on GitHub. To avoid the potential occurrence of technical problems, a pre-recorded lecture will be uploaded to YouTube beforehand.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 62176028), the Australian Research Council under the streams of Discovery Early Career Research Award (Grant No. DE250100613 and Grant No. DE230101033), Future Fellowship (Grant No. FT210100624), Industrial Transformation Training Centre (Grant No. IC200100022), Discovery Project (Grant No. DP240101108 and Grant No. DP240101814), and Linkage Project (Grant No. LP230200892).

REFERENCES

[1] Hongyun Cai and Fuzhi Zhang. 2019. Detecting shilling attacks in recommender systems based on analysis of user rating behavior. *Knowledge-Based Systems* 177 (2019), 22–43.

[5] https://secure-robust-recsys.github.io/

[2] Wenqi Fan, Tyler Derr, Xiangyu Zhao, Yao Ma, Hui Liu, Jianping Wang, Jiliang Tang, and Qing Li. 2021. Attacking black-box recommendations via copying cross-domain user profiles. In *ICDE*.

[3] Jiuru Gao, Jiajie Xu, Guanfeng Liu, Wei Chen, Hongzhi Yin, and Lei Zhao. 2018. A privacy-preserving framework for subgraph pattern matching in cloud. In *Database Systems for Advanced Applications: 23rd International Conference, DASFAA 2018, Gold Coast, QLD, Australia, May 21-24, 2018, Proceedings, Part I 23*. Springer, 307–322.

[4] Yaojun Hao, Guoyan Meng, Jian Wang, and Chunmei Zong. 2023. A detection method for hybrid attacks in recommender systems. *Information Systems* 114 (2023), 102154.

[5] Xiangnan He, Kuan Deng, Xiang Wang, Yan Li, Yongdong Zhang, and Meng Wang. 2020. Lightgcn: Simplifying and powering graph convolution network for recommendation. In *SIGIR*.

[6] Xiangnan He, Lizi Liao, Hanwang Zhang, Liqiang Nie, Xia Hu, and Tat-Seng Chua. 2017. Neural collaborative filtering. In *WWW*.

[7] Zhuangzhuang He, Yifan Wang, Yonghui Yang, Peijie Sun, Le Wu, Haoyue Bai, Jinqi Gong, Richang Hong, and Min Zhang. 2024. Double Correction Framework for Denoising Recommendation. In *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 1062–1072.

[8] Shao-Ping Hsiao, Yu-Che Tsai, and Cheng-Te Li. 2022. Unsupervised Post-Time Fake Social Message Detection with Recommendation-aware Representation Learning. In *Companion Proceedings of the Web Conference 2022*. 232–235.

[9] Bahjat Kawar, Michael Elad, Stefano Ermon, and Jiaming Song. 2022. Denoising diffusion restoration models. *Advances in Neural Information Processing Systems* (2022).

[10] Yehuda Koren, Robert Bell, and Chris Volinsky. 2009. Matrix factorization techniques for recommender systems. *Computer* (2009).

[11] Riwei Lai, Li Chen, Rui Chen, and Chi Zhang. 2024. A Survey on Data-Centric Recommender Systems. *arXiv preprint arXiv:2401.17878* (2024).

[12] Chen Lin, Si Chen, Hui Li, Yanghua Xiao, Lianyun Li, and Qian Yang. 2020. Attacking recommender systems with augmented user profiles. In *CIKM*.

[13] Yuwen Liu, Xiaokang Zhou, Huaizhen Kou, Yawu Zhao, Xiaolong Xu, Xuyun Zhang, and Lianyong Qi. 2024. Privacy-preserving point-of-interest recommendation based on simplified graph convolutional network for geological traveling. *ACM Transactions on Intelligent Systems and Technology* 15, 4 (2024), 1–17.

[14] Jing Long, Tong Chen, Quoc Viet Hung Nguyen, Guandong Xu, Kai Zheng, and Hongzhi Yin. 2023. Model-agnostic decentralized collaborative learning for on-device POI recommendation. In *Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval*. 423–432.

[15] Hao Ma, Min Gao, Feng Wei, Zongwei Wang, Feng Jiang, Zehua Zhao, and Zhengyi Yang. 2024. Stealthy attack on graph recommendation system. *Expert Systems with Applications* (2024), 124476.

[16] Thanh Toan Nguyen, Nguyen Quoc Viet Hung, Thanh Tam Nguyen, Thanh Trung Huynh, Thanh Thi Nguyen, Matthias Weidlich, and Hongzhi Yin. 2024. Manipulating recommender systems: A survey of poisoning attacks and countermeasures. *Comput. Surveys* (2024).

[17] Yuhan Quan, Jingtao Ding, Chen Gao, Lingling Yi, Depeng Jin, and Yong Li. 2023. Robust preference-guided denoising for graph based social recommendation. In *Proceedings of the ACM Web Conference 2023*. 1097–1108.

[18] Steffen Rendle, Christoph Freudenthaler, Zeno Gantner, and Lars Schmidt-Thieme. 2012. BPR: Bayesian personalized ranking from implicit feedback. *arXiv preprint arXiv:1205.2618* (2012).

[19] Fatemeh Rezaimehr and Chitra Dadkhah. 2021. A survey of attack detection approaches in collaborative filtering recommender systems. *Artificial Intelligence Review* 54 (2021), 2011–2066.

[20] Qinyong Wang, Hongzhi Yin, Tong Chen, Junliang Yu, Alexander Zhou, and Xiangliang Zhang. 2022. Fast-adapting and privacy-preserving federated recommender system. *The VLDB Journal* (2022).

[21] Shilei Wang, Peng Zhang, Hui Wang, Hongtao Yu, and Fuzhi Zhang. 2022. Detecting shilling groups in online recommender systems based on graph convolutional network. *Information Processing & Management* 59, 5 (2022), 103031.

[22] Xiang Wang, Xiangnan He, Meng Wang, Fuli Feng, and Tat-Seng Chua. 2019. Neural graph collaborative filtering. In *SIGIR*.

[23] Zongwei Wang, Min Gao, Jundong Li, Junwei Zhang, and Jiang Zhong. 2022. Gray-box shilling attack: an adversarial learning approach. *ACM TIST* (2022).

[24] Zongwei Wang, Min Gao, Wentao Li, Junliang Yu, Linxin Guo, and Hongzhi Yin. 2023. Efficient Bi-Level Optimization for Recommendation Denoising. In *SIGKDD*.

[25] Zongwei Wang, Junliang Yu, Min Gao, Guanhua Ye, Shazia Sadiq, and Hongzhi Yin. 2024. Poisoning Attacks and Defenses in Recommender Systems: A Survey. *arXiv preprint arXiv:2406.01022* (2024).

[26] Zongwei Wang, Junliang Yu, Min Gao, Hongzhi Yin, Bin Cui, and Shazia Sadiq. 2024. Unveiling Vulnerabilities of Contrastive Recommender Systems to Poisoning Attacks. In *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 3311–3322.

[27] Fan Wu, Min Gao, Junliang Yu, Zongwei Wang, Kecheng Liu, and Xu Wang. 2021. Ready for emerging threats to recommender systems? A graph convolution-based generative shilling attack. *Information Sciences* (2021).

[28] Jiahao Wu, Wenqi Fan, Shengcai Liu, Qijiong Liu, Rui He, Qing Li, and Ke Tang. 2023. Dataset condensation for recommendation. *arXiv preprint arXiv:2310.01038* (2023).

[29] Jiahao Wu, Qijiong Liu, Hengchang Hu, Wenqi Fan, Shengcai Liu, Qing Li, Xiao-Ming Wu, and Ke Tang. 2023. Leveraging Large Language Models (LLMs) to Empower Training-Free Dataset Condensation for Content-Based Recommendation. *arXiv preprint arXiv:2310.09874* (2023).

[30] Yishu Xu and Fuzhi Zhang. 2019. Detecting shilling attacks in social recommender systems based on time series analysis and trust features. *Knowledge-Based Systems* 178 (2019), 25–47.

[31] Dingqi Yang, Bingqing Qu, and Philippe Cudré-Mauroux. 2018. Privacy-preserving social media data publishing for personalized ranking-based recommendation. *IEEE Transactions on Knowledge and Data Engineering* 31, 3 (2018), 507–520.

[32] Liu Yang, Ben Tan, Vincent W Zheng, Kai Chen, and Qiang Yang. 2020. Federated recommendation systems. *Federated Learning: Privacy and Incentive* (2020), 225–239.

[33] Junliang Yu, Hongzhi Yin, Xin Xia, Tong Chen, Jundong Li, and Zi Huang. 2023. Self-supervised learning for recommender systems: A survey. *TKDE* (2023).

[34] Wei Yuan, Quoc Viet Hung Nguyen, Tieke He, Liang Chen, and Hongzhi Yin. 2023. Manipulating Federated Recommender Systems: Poisoning with Synthetic Users and Its Countermeasures. *arXiv* (2023).

[35] Wei Yuan, Chaoqun Yang, Quoc Viet Hung Nguyen, Lizhen Cui, Tieke He, and Hongzhi Yin. 2023. Interaction-level membership inference attack against federated recommender systems. In *Proceedings of the ACM Web Conference 2023*. 1053–1062.

[36] Wei Yuan, Chaoqun Yang, Liang Qu, Guanhua Ye, Quoc Viet Hung Nguyen, and Hongzhi Yin. 2024. Robust federated contrastive recommender system against model poisoning attack. *arXiv preprint arXiv:2403.20107* (2024).

[37] Wei Yuan, Hongzhi Yin, Fangzhao Wu, Shijie Zhang, Tieke He, and Hao Wang. 2023. Federated unlearning for on-device recommendation. In *Proceedings of the Sixteenth ACM International Conference on Web Search and Data Mining*.

[38] Wei Yuan, Shilong Yuan, Chaoqun Yang, Nguyen Quoc Viet hung, and Hongzhi Yin. 2023. Manipulating Visually Aware Federated Recommender Systems and Its Countermeasures. *ACM Transactions on Information Systems* 42, 3 (2023), 1–26.

[39] Wei Yuan, Shilong Yuan, Chaoqun Yang, Nguyen Quoc Viet hung, and Hongzhi Yin. 2023. Manipulating Visually Aware Federated Recommender Systems and Its Countermeasures. *ACM Transactions on Information Systems* 42, 3 (2023), 1–26.

[40] An Zhang, Wenchang Ma, Jingnan Zheng, Xiang Wang, and Tat-Seng Chua. 2024. Robust collaborative filtering to popularity distribution shift. *ACM Transactions on Information Systems* 42, 3 (2024), 1–25.

[41] Honglei Zhang, Fangyuan Luo, Jun Wu, Xiangnan He, and Yidong Li. 2023. LightFR: Lightweight federated recommendation with privacy-preserving matrix factorization. *ACM Transactions on Information Systems* 41, 4 (2023), 1–28.

[42] Shijie Zhang, Hongzhi Yin, Tong Chen, Zi Huang, Lizhen Cui, and Xiangliang Zhang. 2021. Graph embedding for recommendation against attribute inference attacks. In *Proceedings of the Web Conference 2021*. 3002–3014.

[43] Shijie Zhang, Hongzhi Yin, Tong Chen, Zi Huang, Quoc Viet Hung Nguyen, and Lizhen Cui. 2022. Pipattack: Poisoning federated recommender systems for manipulating item promotion. In *WSDM*.

[44] Shijie Zhang, Hongzhi Yin, Tong Chen, Quoc Viet Nguyen Hung, Zi Huang, and Lizhen Cui. 2020. Gcn-based user representation learning for unifying robust recommendation and fraudster detection. In *SIGIR*.

[45] Shijie Zhang, Wei Yuan, and Hongzhi Yin. 2023. Comprehensive privacy analysis on federated recommender system against attribute inference attacks. *IEEE Transactions on Knowledge and Data Engineering* (2023).

[46] Yan Zhang, Defu Lian, and Guowu Yang. 2017. Discrete personalized ranking for fast collaborative filtering from implicit feedback. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 31.

[47] Jujia Zhao, Wang Wenjie, Yiyan Xu, Teng Sun, Fuli Feng, and Tat-Seng Chua. 2024. Denoising diffusion recommender model. In *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval*. 1370–1379.

[48] Weibin Zhao, Lin Shang, Yonghong Yu, Li Zhang, Can Wang, and Jiajun Chen. 2023. Personalized tag recommendation via denoising auto-encoder. *World Wide Web* 26, 1 (2023), 95–114.

[49] Jiawei Zheng, Qianli Ma, Hao Gu, and Zhenjing Zheng. 2021. Multi-view denoising graph auto-encoders on heterogeneous information networks for cold-start recommendation. In *Proceedings of the 27th ACM SIGKDD conference on knowledge discovery & data mining*. 2338–2348.

[50] Ruiqi Zheng, Liang Qu, Tong Chen, Kai Zheng, Yuhui Shi, and Hongzhi Yin. 2024. Poisoning decentralized collaborative recommender system and its countermeasures. In *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval*. 1712–1721.

[51] Zhihao Zhu, Rui Fan, Chenwang Wu, Yi Yang, Defu Lian, and Enhong Chen. 2023. Model Stealing Attack against Recommender System. *arXiv preprint arXiv:2312.11571* (2023).