

Trustworthy Recommender Systems

SHOUJIN WANG, RMIT University, Macquarie University, Australia

XIUZHEN ZHANG, RMIT University, Australia

YAN WANG, Macquarie University, Australia

HUAN LIU, Arizona State University, United States

FRANCESCO RICCI, Free University of Bozen-Bolzano, Italy

Recommender systems (RSs) aim to help users to effectively retrieve items of their interests from a large catalogue. For a quite long period of time, researchers and practitioners have been focusing on developing accurate RSs. Recent years have witnessed an increasing number of threats to RSs, coming from attacks, system and user generated noise, system bias. As a result, it has become clear that a strict focus on RS accuracy is limited and the research must consider other important factors, e.g., trustworthiness. For end users, a trustworthy RS (TRS) should not only be accurate, but also transparent, unbiased and fair as well as robust to noise or attacks. These observations actually led to a paradigm shift of the research on RSs: from accuracy-oriented RSs to TRSs. However, researchers lack a systematic overview and discussion of the literature in this novel and fast developing field of TRSs. To this end, in this paper, we provide an overview of TRSs, including a discussion of the motivation and basic concepts of TRSs, a presentation of the challenges in building TRSs, and a perspective on the future directions in this area. We also provide a novel conceptual framework to support the construction of TRSs.

CCS Concepts: • **Information systems** → **Recommender systems**;

Additional Key Words and Phrases: recommender systems, trustworthy recommendation

ACM Reference Format:

Shoujin Wang, Xiuzhen Zhang, Yan Wang, Huan Liu, and Francesco Ricci. 2022. Trustworthy Recommender Systems. *ACM Comput. Surv.* 1, 1, Article 1 (June 2022), 16 pages. <https://doi.org/0000001.0000001>

1 INTRODUCTION

1.1 Why we need trustworthy recommender systems?

We are living in the era of information explosion and digital economy, where the information overload problem has become increasingly important. As a matter of fact, today people usually make choices from massive and rapidly increasing catalogues of products and services (generally called *items*), while consuming a large amount of time and resources to discriminate relevant from not-relevant items. To make informed choices and decisions in a more effective and efficient way, *Recommender Systems (RSs)* have been introduced into almost every aspect of our daily life, work, business, study, entertainment and socialization [34, 41]. Today RSs are one of the most important and popular application areas of artificial intelligence (AI). Formally, RSs are software tools and

Authors' addresses: Shoujin Wang, RMIT University, Macquarie University, Sydney, Australia, shoujinwang@foxmail.com; Xiuzhen Zhang, RMIT University, Melbourne, Australia, xiuzhen.zhang@rmit.edu.au; Yan Wang, Macquarie University, Sydney, Australia, yan.wang@mq.edu.au; Huan Liu, Arizona State University, Tempe, United States, huan.liu@asu.edu; Francesco Ricci, Free University of Bozen-Bolzano, Bolzano, Italy, fricci@unibz.it.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2022 Association for Computing Machinery.

0360-0300/2022/6-ART1 \$15.00

<https://doi.org/0000001.0000001>

techniques which provide suggestions on items which may be of interest to end users. According to McKinsey's report¹, 35% of what customers purchase on Amazon and 75% of what users watch on Netflix come from recommendations.

Since the release of the first RS, "Tapestry" in 1992, which was then termed collaborative filtering technique [14], RSs have flourished and achieved great success in the past 30 years. A series of RS approaches and models including content-based filtering, collaborative filtering, and hybrid approaches have been developed and deployed, most of which have achieved good recommendation performance. In recent years, benefiting from the advancement of machine learning, especially deep learning, more powerful and accurate RS models have been proposed [34, 55].

Although tremendous successes have been achieved in the RS area, the majority of existing research works has focused on the improvement of the system accuracy, while only some minor part of the literature has also taken some other important properties and values of RSs into account, such as diversity and novelty [5]. In fact, existing accuracy-oriented RSs have not properly considered end users in the broader context of human-machine interaction where other important factors are commonly considered as critical for the overall user experience [22]. There are some additional aspects that requires particular attention. Firstly, the cyberspace where RSs are deployed is becoming increasingly complex and full of threats coming from various sources and of diverse nature, including cyber-attacks, noisy and fake information and system bias. This triggers the demand of trustworthy RSs (TRSs) which aim to compete in the complex and challenging cyberspace. Secondly, *stakeholders* including users, owners and regulators of RSs, have increasingly higher demand for RSs [1]. These stakeholders not only demand recommendation accuracy, but also need trustworthiness, including robustness, fairness, explainability, privacy-preservation, etc. Actually, trustworthiness is even more important than accuracy in some critical and sensitive domains, including finance and medicine, where highly reliable RSs are required. In practice, it has become a consensus both in the academia and industry that accuracy should not be the only focus of an RS, and trustworthiness must be prioritised. These analyses have triggered the urgent demand of a new RS paradigm, i.e., TRSs.

1.2 What are trustworthy recommender systems?

The term "trustworthy" describes an entity on which a subject can rely to be good, honest, sincere [8]. Specific aspects of "trustworthy" include: trustable, reliable, dependable, faithful, honourable, creditworthy, responsible [54]. In general, a **TRS** refers to an RS on which its stakeholder can rely to be good, trustable, reliable, dependable, and faithful.

A recommendation process is complex and interactive; it involves several entities, such as, users, items, the RS, and even the provider of items (e.g., sellers). All of them actually form a *recommendation ecosystem* which enables the recommendation activities [1]. In practice, these parties also correspond to the necessary elements for recommendations: data (i.e., user/item/provider related information, e.g., user-item interactions), approaches and models (i.e., RS).

TRSs are actually the result of trustworthy RS approaches and models built in a trustworthy ecosystem. Although trustworthy RS approaches and models are pivotal for enabling trustworthy recommendations, they cannot survive without a trustworthy ecosystem. Most of studies in the literature only discussed trustworthy RS approaches while ignoring the significance of trustworthy ecosystem. For instance, Ge et al. [12] provided a timely survey on the various techniques for enabling robust, fair, explainable or secure RSs while without touching trustworthy ecosystems or complex challenges in building TRSs, which greatly differentiates it from our work. To bridge this gap, we first propose a novel concept of trustworthy recommendation ecosystem, which is the

¹<https://www.mckinsey.com/industries/retail/our-insights/how-retailers-can-keep-up-with-consumers>

foundation for building trustworthy RSs. In addition, trustworthy recommendation ecosystem can well differentiate trustworthy RSs from the generally discussed trustworthy artificial intelligence (AI) since it is derived from the core characteristics and properties of the recommendation scenario. Then, we illustrate the various aspects to specify the “trustworthiness” of RSs with an emphasis on the trustworthiness of recommendation approaches and models. Finally, we describe some specific and straightforward examples of trustworthy RSs in the real world.

1.2.1 Trustworthy recommendation ecosystem. A recommendation process unfolds in a complex user-RS-item interaction scenario. Items are provided by various providers, including sellers, news source websites, and thus providers are an indispensable part of the process. As mentioned above, these four parties together form a basic ecosystem for recommendation activities and they interact with each other, possibly in a collaborative form, to complete the recommendation task. A trustworthy recommendation ecosystem includes trustworthy *users, items, providers and RSs*, which will be illustrated successively in the following paragraphs.

Trustworthy users. Users consuming recommendations can possess diverse characteristics and perform various tasks in the cyberspace. Some users may not be trustworthy, and may try to obstacle the proper functioning of RSs. For instance, it is not uncommon to identify special users (e.g., internet water army and internet hacker) who may attempt to perform fake or false interactions with items to intentionally bias the recommendation models for a given personal and even malicious purpose (e.g., biased product promotions) [56]. Therefore, in order to build a trustworthy RS, only trustworthy users should be authorised to operate. Trustworthy users can be roughly characterized by two aspects: (1) the user profile information should be true, accurate, and users’ behaviour on the recommendation platforms should reflect genuine preferences and intentions; (2) users should maintain a good reputation in their interaction behaviour [44, 45], e.g., they should write true and objective reviews or ratings for items, and pay for the purchased items on time.

Trustworthy items. Usually, there are massive quantities and diverse types of items on an online consumption platform. Items have diverse characteristics and can bring different impact to the RS stakeholders, which are individual users, the local community and even the whole society. Although most of the items can well satisfy users’ needs and can have a positive impact on the stakeholders interests in the long run, some items may produce a negative impact on either the individual users, the community or the society. For example, additive electronic games usually match young children’s preferences well. But these games often create addiction and thus can negatively affect users’ lives, work or studies, hence resulting in significant negative impact on users and their family. Another example is fake news, which may match some minority users’ stance and reading preferences. But they mislead the public, and may cause serious social problems, and should not be recommended to end users [42]. To this end, only trustworthy items should be recommended by a trustworthy RS. Trustworthy items can be characterized by two aspects: (1) the item-related information (e.g., item attributes) used for recommendations should be true and precise, so that the intrinsic characteristics of all items can be easily captured; (2) the candidate items to be recommended to end users should be trustable and responsible, namely the items must not bring potential negative impacts to the stakeholders of RSs.

Trustworthy providers. Providers are the party who provide items in online platforms. For example, a provider may be a seller in an e-Commerce platform, or a news source website which releases original news in the news domain. In the real world, some providers are not trustworthy since they may provide fake or poor-quality items, leading to negative impact to the end users and the society. For instance, some sellers may sell fake products while some news websites may release fake news. Obviously, trustworthy providers are necessary for building trustworthy RSs and they

can be characterised by two aspects: (1) the providers should be responsible for the quality and potential impact of the items they provide. For instance, the sellers should provide products or services with guaranteed quality, while the news websites should provide verified true news only while combating fake news; (2) it is important for providers to maintain a good reputation through their historical transaction or releasing behaviours [43, 53].

Trustworthy RSs. Recommendation approaches which are usually built on data mining or machine learning models should be reliable and stable. Specifically, they should not only be able to accurately capture users' preferences and items' characteristics so as to provide accurate recommendation services to end users, but also perform stably all the time, even in the most complex, dynamic and challenging context (e.g., the cyberspace facing frequent cyber-attacks). Trustworthy approaches and models are the most important part in trustworthy RSs and they can be characterised by multiple specific aspects, which will be discussed in detail in the next part.

1.2.2 Aspects of trustworthy recommender systems. In some related areas, such as, trustworthy AI, many different aspects have been proposed to specify "trustworthy" from perspectives including regulations, mechanism, and technology [54]. Several aspects related to the technology perspective have been commonly recognized, including robustness, fairness, explainability, transparency, privacy, accountability, and responsibility. Since RSs are a specific application area of AI, the aspects used to define trustworthy AI are also applicable to characterise trustworthy RSs. However, due to the very special and specific data characteristics, work mechanism and computation task of an RS, there are additional aspects, such as, human's perception and trustworthy evaluation, which are specific to the RS scenario and can well distinguish trustworthy RSs from trustworthy AI. Next, we illustrate the various aspects for characterizing trustworthy RSs.

- **Robustness** indicates an RS that has strong fault-tolerant capability to survive attacks, noisy and fake information (e.g., such as users' arbitrary behaviours and fake reviews/ratings on items) [30], which often commonly affect the input data used for recommendations.
- **Fairness** indicates that the RS is able to reduce or remove possible bias towards certain groups of stakeholders (e.g., the disparities in treating user with different demographics or items with low and high popularity) which may be present in the input data, the recommendation model or in the recommendation results [29]. Consequently, the final recommendation results can be assessed as fair from both the user side and the provider side.
- **Transparency** generally means that the functioning mechanism and the recommendation model are transparent to all the stakeholders of the RS, and it is not perceived as a "black box" [4]. Transparency can greatly reduce the potential risks of deploying ineffective RSs in real-world domains, especially in some sensitive and critical domains like finance and healthcare domains.
- **Explainability** means that the recommendation mechanism, recommendation models and the recommendation results are well-explained so that the stakeholders of the RS can properly understand how and why the recommendations are generated [57].
- **Privacy and security** means that the RS is able to effectively protect the personal privacy of relevant stakeholders [38]. This aspect is even more important in RS, compared to other web applications, since RSs are consuming a large amount of profile and behaviour, which often contains a sensible users' characteristics.
- **Responsibility.** The development and deployment of RSs should be conducted in a responsible manner (e.g., follow the regulations and law), so that the RS will not explicitly or implicitly harm anybody. Moreover, the generated recommendation results should be beneficial to the all stakeholders [11]. For instance, fake news should not be recommended to any users even if

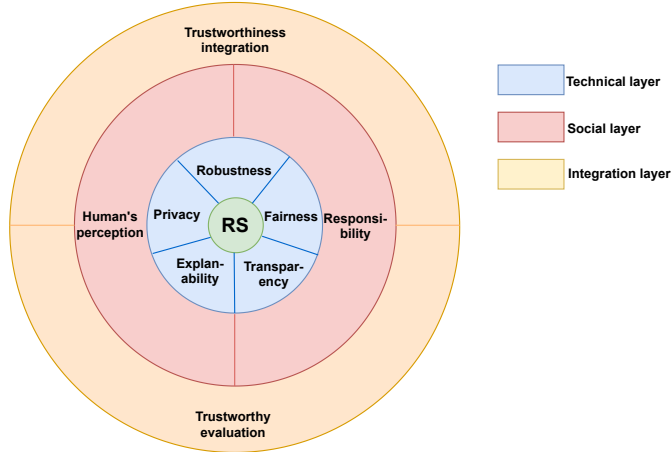


Fig. 1. The various aspects to characterise TRSs and the relations among them. According to the characterization perspective, they can be organized into three layers.

it may interest some ones, or addictive games should not be recommended to young children either.

- **Human's perception of trustworthiness**, relates to the subjective perception, which the relevant stakeholders have, of the trustworthiness of an RS. This is unique to RSs and is of great significance. In fact, an RS is actually involving a human-machine interaction [21], and whether an RS is trustworthy or not, ultimately depends on human's feeling and perception. However, almost all of the existing approaches to model trustworthy RSs have been developed by assuming a single point of view, that of the machine [48], i.e., the RS models and algorithms, while have ignored the human's factor. Moreover, existing work often mechanically computes a numerical measurement value to quantify the trustworthiness of RSs. Such lack of consideration of the human's factor triggers the urgent demand to take human's perception into account when talking about trustworthy RSs.
- **Trustworthiness integration**. Although various aspects and perspectives have been proposed to characterise trustworthy RSs, they are mostly separated from each other. In addition, most of the existing studies on trustworthy RSs have focused on one or two aspects of trustworthiness alone. For instance, fairness-aware RSs and explainable RSs only focus on the fairness and explainability aspect respectively. However, accounting for only one or two aspects can not lead to a truly trustworthy RSs. In order to build truly trustworthy RSs, all the aforementioned different aspects, including both objective and subjective aspect, should be integrated together organically and effectively towards to a unified trustworthy RS framework.
- **Trustworthy evaluations**. On one hand, both the evaluation methods and the evaluation metrics must be reliable to well and precisely reflect the performance of the RS. One example is that most offline evaluations are performed under a very ideal situation and thus they cannot actually indicate how an RS will perform in the real-world online scenarios [15]. On the other hand, new evaluation protocols and metrics are in demand to evaluate the trustworthiness of an RS so that all the aforementioned aspects can be appropriately validated.

Although these different aspects touch a variety of issues and often correspond to different elements and stages of an RS, they are closely inter-connected and must be jointly addressed to contribute to the “trustworthiness” of the RS, as illustrated in Fig. 1. For instance, fairness often relates to explainability. In fact, the fairness perspective (e.g., users' gender or item popularity) that

is considered and how fairness is assured should be explainable to the end users, so that they can clearly understand and accept the generated fair recommendation results.

1.2.3 Examples of trustworthy recommender systems in the real world. For decades, RSs have been widely exploited in nearly all information systems that we use daily for work, study or entertainment. In recent years, along with the occurrence of an increasing number of cyber threats including cyber attacks, fake or false online information, bias in the cyber space, trustworthy RSs are an evident need. There is a variety of examples of real-world trustworthy RSs across different application domains. In E-commerce domain, one typical example is the robust RS which can tame fake ratings and reviews [26] in platforms like Ebay or Amazon. This type of RSs detects fake ratings and reviews inserted in the platform and discard them when generating trustworthy recommendations. In media domain, a typical example is a recently proposed fact check technology (e.g., Google fact check tools) for the news domain, which introduces a series of techniques to check the veracity of news on the web so that only verified true news will be recommended to end users [13]. Another typical example is a veracity-aware news recommender system published at the 2022 Web Conference [42]. This system checks the veracity of each news piece before generating recommendations, so that only checked true news will be recommended to end users.

2 THE RECOMMENDATION PARADIGM SHIFT

2.1 From accuracy-oriented RSs to trustworthy RSs

RS research can date back to 1990s when the first collaborative system “Tapestry” was reported in the literature [14]. From early 1990s to the middle of 2000s, several algorithms have been developed for enabling content-based or collaborative filtering recommendations [34, 47]. From 2008 to 2016, driven by the popular Netflix challenge, matrix factorization methods have dominated the scenario for a long time. Since the middle of 2010s, benefiting from the rapid development of deep learning techniques, deep learning based RSs have become the main stream in recommendation domain [55].

Along with that technological shift and revolution of RSs, the focused research problems, challenges and evaluation mechanisms of RSs have also changed. Since the first studies on RSs to early 2010s, the accuracy of recommendation results has been the most important and often the only evaluation criteria that was used to evaluate an RS. Specifically, that means that the researchers tried to assess whether the recommended items were truly preferred (e.g., clicked, purchased, highly rated) by users. During this period, nearly all efforts were devoted to develop more accurate RS models and algorithms, such as more accurate matrix factorization algorithms to predict the unknown user-item ratings with a smaller and smaller prediction error. Then, starting from early 2010s, more and more researchers realized that the accuracy criterion is insufficient for evaluating an RS, and thus new evaluation dimensions, including diversity and novelty were proposed [2, 15]. As a result, the evaluation of an RS moved from single-criteria evaluations, based on accuracy, to multi-criteria evaluations based on a range of dimensions, such as accuracy, diversity and novelty, while accuracy still was considered as the most important criteria.

Since late 2010s, due to an increasing level of threats in the cyberspace, coming from cyber attacks, noises, and biases, the trustworthiness of RSs have attracted increasing attention from both academia and industry. As a result, a growing number of studies have focused on trustworthy RSs, from various perspectives, such as robustness, fairness, explainability or privacy. For example, some work aimed to build robust RSs which can fight against shilling attacks [16], and fairness-aware RSs to generate fair recommendations for users with different demographics [49]. Some other work have instead focused on building explainable RSs to generate user-understandable recommendation results [57], or secure and privacy-preserved RSs which puts a special concern on users’ privacy [38]. Obviously, the research focus and the ultimate goal of these studies is no

longer centered on the improvement of recommendation accuracy. Instead, they have changed the direction towards enhancing the trustworthiness of RSs. This has actually revolutionized the research focus and the evaluation perspectives, from accuracy-oriented recommendations towards trustworthiness-oriented recommendations, leading to a recommendation paradigm shift.

In practice, the trustworthiness of RSs has been attracting much attention from different sectors including academia, industry and government. A typical example is that the Chinese government released regulations on recommendation algorithms for internet information services in early 2022 [32]. A large proportion of the regulations emphasised the significance of trustworthy RSs to be deployed in the real-world business applications.

2.2 From trust-aware recommender systems to trustworthy recommender systems

Trust-aware recommender systems mainly consider and leverage the trust relationships between humans and organizations to enhance the recommendation performance. Here the trust relationships can vary, some typical examples include the trust relations between different users on online or offline social networks (e.g., friends on facebook, or colleagues in one organization), the trust relationships between users and comments, ratings on items from others, the trust relationships between customers and sellers [52, 58]. Since early 2000s, a variety of studies [3, 10, 28, 53] have been done to investigate how to well to model and leverage such diverse trust relationships to improve the performance of RSs.

Differently from trust-aware RSs, trustworthy RSs aim to build reliable RSs which can be accepted by humans, which were proposed in late 2000s for the first time [30]. However, early definitions on trustworthy RSs mainly focused on one single aspect of trustworthiness, namely robustness [30, 48]. So trustworthy RSs in the early stage mainly refers to those RSs which are robust while facing various types of attacks in the cyberspace. However, they are not fully trustworthy since there are some other important aspects contributing to trustworthiness that were initially overlooked, including the aforementioned fairness, explainability, privacy and responsibility.

Therefore, it is of great theoretical and practical significance to develop the next-generation trustworthy RSs which go beyond the existing robustness-oriented ones. To this end, in this paper, we propose novel trustworthy RSs in which all the nine aforementioned aspects contributing to trustworthy RSs are considered, leading to a significant step towards the implementation of truly trustworthy RSs.

3 TRUSTWORTHY RECOMMENDER SYSTEMS: A FOUR-STAGE PERSPECTIVE

Classical Recommendation Process. Generally speaking, a typical machine learning-based recommendation process comprises the following four successive and inter-connected stages:

- **Data preparation stage**, including data collection and preprocessing;
- **Data representation stage**, which often learns an informative representation of the raw input data as the input of the downstream recommendation model;
- **Recommendation generation stage**, which deploys some data mining or machine learning based prediction models to predict the unknown user-item interactions, e.g., ratings, clicks;
- **Performance evaluation stage**, which employs various evaluation methods, including online and offline evaluations, to evaluate the recommendation results from different perspectives such as accuracy, diversity, and fairness.

Trustworthy Recommender Systems. To be trustworthy, an RS should be trustworthy in each of the aforementioned four stages. Each stage has its unique computation task, characters and goal, so the “trustworthiness” of different stages often has different specific meanings and focuses on different aspects of the aforementioned nine aspects (cf. Section 1.2.2). For instance, data preparation stage

often focuses more on the “robustness” aspect, since the data preparation methods should be robust enough to survive to noisy and fake data, possible coming from attacks. While the recommendation generation stage should focus more on aspects like “fairness”, “transparency” and “robustness”, since fair, transparent and robust RS models and algorithms are required in this stage for generating recommendations. Next, we try to characterize a trustworthy RS from a four-stage perspective while the specific meaning of “trustworthy” in each stage will be highlighted.

- **Robust and secure data preparation**, on one hand, is necessary to combat noisy and fake information, and bias in the raw data, generated in the cyberspace, and survive to possible attacks on the data. In this way, the prepared data for recommendations can accurately reflect users’ preferences and items’ characteristics. On the other hand, the users’ data should be managed and processed in a secure way so that sensitive and privacy information will not be leaked.
- **Robust and explainable data representation**, which employs robust and explainable data representation models to precisely learn informative and interpretable latent representations of the original input data in a stable way regardless of the potential attacks. In most cases, the learned latent representations are latent vectors without an explicit semantic meaning, which then negatively impacts on explainability. In addition, it is often not very clear which information is encoded in the representations. Therefore, the “explainability” aspect should be emphasized in this stage.
- **Fair, transparent, explainable and responsible recommendation generation**, in which fair, transparent and explainable RS models should be adopted to provide fair exposure opportunities of all items to different users in a transparent, explainable and responsible way. In addition, the models should also be able to provide straightforward explanations by using texts or images corresponding to the recommendation results, to faithfully explain how the recommendations are generated and why they are appropriate for a given user. More importantly, only those items with positive impact to stakeholders can be recommended.
- **Trustworthy evaluations** comprise two-sided evaluations: (1) *technical evaluation*, and (2) *ethical evaluation*. The technical evaluation aims to evaluate the recommendation performance from some technical perspectives such as accuracy, diversity, novelty, and explainability. More trustworthy and reliable evaluation protocols and metrics are required to evaluate such technical performance. In contrast, the ethical evaluation aims to evaluate recommendations from the ethical perspective such as the responsibility and social impact. For instance, whether the recommendation activities and the recommendation results are responsible and beneficial to the relevant stakeholders. Towards trustworthy RSs, ethical evaluations are necessary and of great significance to the sustainable development of the community and the society. Some examples of unethical but maybe preferable recommendations include the recommendations of fake news [42] and the recommendation of addictive games to young children. To the best of our knowledge, this is the first time the proposal of an ethical evaluation of RSs is put forward in the literature.

4 CHALLENGES FOR BUILDING TRUSTWORTHY RECOMMENDER SYSTEMS

Although the significance and urgency of trustworthy RSs have been commonly recognised, the research in this area is still in an early stage. A variety of challenges and research problems remain to be properly addressed in each of the aforementioned four stages. We therefore analyze the particular challenges of each stage.

Challenges in data preparation stage. Before building an RS model, a necessary step is to collect and prepare data to train and test the model. Such data often contains user-item interactions

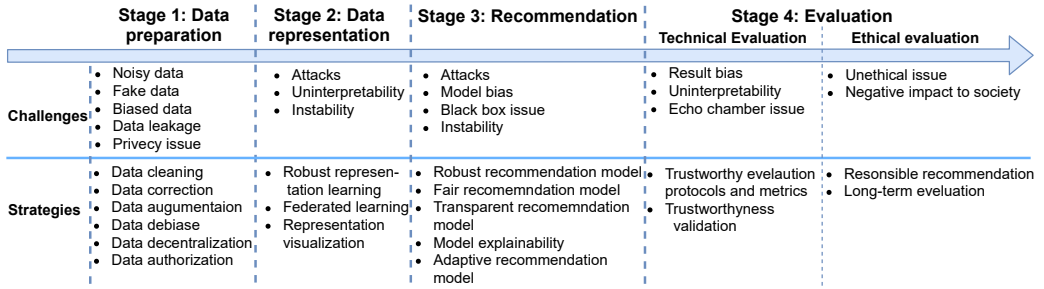


Fig. 2. The challenges and corresponding strategies for building TRSs.

such as users' clicks, purchases, ratings, or comments on items, and side information such as users' attributes, social relations, and items' features [20]. The data is often collected from online consumption platforms such as amazon.com, youtube.com, and abcnews.go.com. Due to the large amount of diverse users (e.g., 10M+ users) on each platform, it is inevitable that some users' behaviours may be noisy and unreliable (e.g., randomly click or view a set of items on amazon.com), or there may be some malicious users (e.g., internet water army) who have performed malicious behaviours, e.g., posting fake ratings or comments to some targeted items or sellers. These factors bring noise, bias, and fake information into the interactions or side information, making the data used for recommendations unclean and unreliable. As a result, the data can not accurately reveal the users' preferences and item characteristics, and thus misleads the downstream recommendation models.

Therefore, a big challenge at the data preparation stage is to effectively detect and remove critical data, e.g., noisy, fake, or biased data, and retain the genuine data. This task is quite challenging since this critical data usually accounts for a quite small proportion of the whole population, making it very difficult to discover it, especially when critical data looks quite similar to the genuine data. Possible strategies to address this challenge include a set of conventional and emerging data preprocessing techniques. For instance, some advanced data augmentation and data debias methods [36], including counterfactual data augmentation [46] and contrastive learning [39], have been extensively studied to remove the bias in raw data in recent years.

Another challenge at this stage is related to the data privacy and security issue. This is especially important in real-world RS applications since the data used for recommendations often contains a large amount of users' private information which should be protected. To be specific, on one hand, during the collection of raw data, it is important to ensure that only the really required data will be collected. On the other hand, when a large amount of data is collected, it is important to build a safe and strong infrastructure and mechanism to properly store and manage it, including secure and powerful database, and rigorous data access mechanism. Another way to address the data privacy and security issue is to introduce federated learning [51] and edge computing [37]. In this way, the data used for recommendations can be decentralized to various edge devices such as users' mobile phones where the individual users' privacy can be well protected.

Challenges in data representation learning stage. Data representation aims to learn an informative numerical vector in a latent space to well represent each data point in the original input dataset. For instance, the well-known representation learning model Word2Vec [35] learns a latent numerical low-dimensional vector to represent each word.

In advanced machine learning, especially in deep learning area, data representation learning is a prior step of all the downstream learning models and tasks. The quality of data representation directly determines the performance of the learning models. Therefore, machine learning based RS

models often consists of two main steps: data representation learning and prediction. The output of the first step is taken as input of the second for the prediction task. For instance, in matrix factorization or neural network based RS models, each user/item is represented by a K-dimensional latent vector which is learned by mapping the user/item ID into a latent space [31]. The main challenges in representation learning stage lie in the following three aspects.

First, how to learn accurate and informative representations to precisely retain the original information in the raw data? For instance, the similarities/distances between the raw data points should be accurately reflected by their corresponding representations in the latent space. Towards this challenge, some advanced representation learning techniques including contrastive representation learning [50] are able to learn more accurate and informative representations.

Second, how to learn interpretable representations? One common and critical issue with latent representations is the lack of explainability. It is often not clear what the semantic meaning of the latent vectors is, making the learned representations uninterpretable for humans. Sometimes, it is not clear what kind of information is encoded in the latent vectors either, which brings some potential risks for the real-world applications of RS models. To address this challenge, some explainable representation learning models and techniques including data visualization can be developed to disclose the patterns encoded in the latent representations.

Third, how to combat attacks on representation learning models? In general, nearly all machine learning models including representation learning models may suffer from some external attacks, especially those deployed in real-world applications. The attackers may quickly generate a large amount of fake data to intentionally mislead the models and thus downgrade the quality of the learned representations. Some possible strategies include robust representation learning techniques, such as adversarial representation learning which fights against attacks in an adversarial way [9].

Challenges in recommendation generation stage. In this stage, the data representations learned in the previous stage will be imported into the selected RS model for generating recommendations. The key challenge lies in how to build a *robust, fair, transparent, explainable* and *responsible* RS model which can work in a trustworthy way in a complex and dynamic environment.

First, similarly to what was observed for the representation learning stage, RS models also easily suffer from various attacks. So the first challenge is how to build robust RS models which can survive various attacks especially those malicious attacks and adversarial attacks in the complex cyberspace where RSs are deployed.

Second, some particular design and work mechanisms of the RS models may lead to biased RS models and thus generate biased recommendations. Therefore, another challenge in this stage lies in how to effectively remove the bias. Various model debias techniques like auto-debias which learns the debias parameter from the data [6] can address this issue to some degree.

Third, advanced machine learning based RS models, especially deep learning based ones often run in a black-box mode, and thus the computations in the model are not transparent and explainable to humans. This makes it hard to understand how an RS model is working and what potential risks and disadvantages the model may have. Hence, this may bring potential risks for the applications of RS models in real-world, especially in some social and economic domains which are critical, such as, healthcare and finance, where a small mistake may lead to a large loss (e.g., the loss of a life or a large sum of money). Hence, the third challenge in this stage lies in how to build transparent and explainable RS models whose work mechanism are well understandable to humans. In this way, how and why the recommendations are generated can be well disclosed and visible to end users, which greatly reduces the risks of the employment of RSs in real-world business.

Fourth, considering the real-world application context, some recommendation behaviours may be profit-driven while ignoring the ethical or even the legal issues (e.g., recommending additive

games to children). Some recommendation results may be accurate but not responsible, such as recommendations of fake news to particular users [42]. Hence, how to ensure responsible recommendation behaviours and recommendation results which are for social good is another big challenge in this stage.

Challenges in the evaluation stage. In this stage, the recommendation results, e.g., predicted user-item rating values, or a list of ranked items, generated by an RS model are evaluated to measure its performance. Conventionally, the evaluation metrics could be a variety of quantity metrics of concern such as accuracy, and diversity, which can directly measure the performance from the technical perspective. However, as mentioned in the Introduction, trustworthy evaluation should go beyond conventional technical performance evaluation. Instead, they should contain both *technical evaluation* and *ethical evaluation*.

For the technical evaluation, existing evaluation protocols and metrics for RSs are mostly accuracy-oriented [47]. They are not sufficient to comprehensively evaluate an RS, especially in the complex cyberspace which often contains noises, attacks, and bias [19]. In such a complex context, the stakeholders of an RS usually focus not only on accuracy, but also on trustworthiness. Hence, the effective evaluation of the trustworthiness of an RS has a great social and economic significance. However, the evaluation of the trustworthiness of an RS is quite challenging, and involves multiple aspects, such as the robustness, fairness, explainability and privacy. Some of them are hard to be quantified in a traditional online or offline experiment. In addition, different application scenarios often have different requirements on the trustworthiness of the RS and focus on different aspects. For instance, in an online e-commerce platform where attacks and noise behaviours are routinely detected, the robustness of the RS should be a primary attention point. Conversely, in an offline RS for medicine treatment, the transparency of the RS model and the explainability of the recommendation results may be more important. Therefore, it is of great importance to define novel trustworthiness evaluation schemes for RSs, including both new evaluation protocols and evaluation metrics for comprehensively and systematically measuring the trustworthiness of RSs.

Ethical evaluation aims to evaluate an RS from the ethical and social perspectives. Specifically, they measure whether the recommendation behaviours and recommendation results will have a positive impact on the various stakeholders. Here, the impact of an RS could be on the recognition or the behaviours of end users, and it could be explicit or implicit, short-term or long-term. Ethical evaluations are quite challenging since the various impact and influence of RSs on both individual level and the society level are very difficult to accurately capture and quantify [17]. New and well-designed ethical evaluation methods are in demand for RSs, which may combine both qualitative and quantitative evaluations.

5 A FRAMEWORK FOR TRUSTWORTHY RECOMMENDER SYSTEMS

To build a trustworthy RS is therefore a challenging task. Not only various aspects of trustworthiness, such as robustness, fairness and security, and the complex relations among them, should be well considered in a unified way, but also new and trustworthy evaluation protocols and metrics are in order. Each aspect often involves specific models and techniques. For instance, robustness is often achieved via adversarial learning techniques such as generative adversarial networks [7]. Due to its extreme complexity, it is challenging to design a very specific model for trustworthy RSs which can well handle all the aspects. However, a systematic methodology to build a comprehensive trustworthy RS while considering all the different aspects in different stages is in a compelling challenge and there is the need of a unified framework for trustworthy RSs. Hence, to bridge this gap, we propose a conceptual framework to support trustworthy RSs.

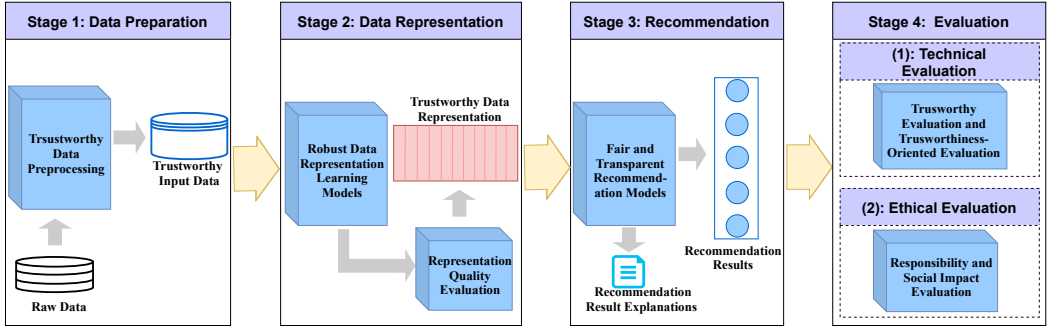


Fig. 3. A conceptual framework for building TRSs.

Consistent with the four stages of recommendation process discussed in Section 3, our proposed trustworthy RS framework consists of four stages: (1) *trustworthy data preparation*, (2) *robust and explainable data representation*, (3) *fair, transparent, explainable and responsible recommendation generation*, and (4) *trustworthy evaluation*, as is depicted in Figure 3.

Trustworthy data preparation. Trustworthy data preparation aims to first collect raw data (e.g., user-item interaction data and side information data) from online platforms in a trustworthy way (e.g., privacy-preserved) and then transfer it to trustworthy input data (e.g., clean, unbiased and reliable data) for the downstream recommendation tasks. Note that the collected raw data often contains noises, bias and false information, etc. Some conventional and advanced data preprocessing techniques can be employed to support trustworthy data preparation. For instance, some data cleaning methods including pattern-based error detection [18] and machine learning based outlier detection [33] can be utilized to detect and remove those noisy and fake data in the raw dataset. In recent years, some advanced machine learning approaches like counterfactual data augmentation [46] and contrastive learning based data augmentation [39] have been commonly utilized to reduce the bias in input data for recommendations.

Robust and explainable data representation. In principle, there are two specific steps for achieving trustworthy data representations: (1) representation learning to learn user and item representations, and (2) representation quality evaluation to evaluate the learned representations. In RS area, the evaluation step is often incorporated into the downstream recommendation task, i.e., the representation quality is measured by the quality of recommendation results.

For the representation learning step, as discussed in Section 3, trustworthy can be specified into robust and explainable. On the one hand, to support the robustness of data representation learning models so that they can perform stably when facing attacks and noises, one typical solution is adversarial representation learning models [9]. In addition, to remove the possible biased and noisy information hidden in the representations, some representative debiasing and denoising models including Denoising Autoencoder (DAE) [25] can be deployed for more accurate representation learning for recommendations. On the other hand, in order to make the learned latent representations more interpretable for humans, some data visualization techniques such as t-SNE [40] can be helpful to explicitly reveal the hidden patterns in latent data.

Fair, transparent, explainable and responsible recommendation generation. In the recommendation generation stage, the core task is to design and develop trustworthy RS models. As discussed in Section 3, trustworthy in this stage can be characterised along four dimensions: fair, transparent, explainable, and responsible. We illustrate them in the following.

First, a trustworthy RS model must be free of bias so that it can perform equally well for different users and items. In support of this, disentanglement learning based approaches [27] can be used

for removing bias in RS models. In addition to RS models, bias may also exist in recommendation results, which could be reduced by re-ranking techniques based on some particular constraints.

Second, trustworthy RS models should be transparent. To support the transparency, some set-based techniques can be employed to explicitly present the RS models to end users via natural language [4]. Building transparent RS models is quite challenging and more studies are deserved.

Third, to support the explainability of recommendation results, the output of recommendation generation stage should be two-sided: (1) the normal recommendation results, e.g., a list of selected candidate items, and (2) corresponding explanations of the recommendation results to well explain how and why the recommendations are generated. The explanations should be straightforward and well-understandable, either in textual or visual formats.

Last but not the least, to be trustworthy, the recommendation generation process must be responsible in terms of both the recommendation behaviours and the recommendation results. On one hand, some additional constraints and criteria can be employed to ensure the above aspects towards social good. For instance, some models can be developed to filter out those fake products, addictive games and fake news from recommendation lists. On the other hand, some regulations may be enforced to guide the harmonic development and deployment of RS techniques.

Trustworthy evaluation. Evaluation is an important step for ensuring the quality of recommendation results generated by RS models. As depicted in Figure 3 and discussed in Section 3, both technical evaluation and ethical evaluation are required for a trustworthy RS. Regarding technical evaluation, most of the existing evaluations are accuracy-oriented, while trustworthiness evaluations are in their early stage. Although a few metrics have been defined to measure one specific aspect of trustworthiness, such as fairness [24], there is no unified method to systematically evaluate multiple aspects as discussed in Section 1.2. New evaluation protocols and metrics are in demand for comprehensive trustworthiness evaluations.

Regarding ethical evaluation, to the best of our knowledge, there is no existing work reported in the literature. Ethical evaluation mainly evaluates the social impact of recommendation behaviours and results. For instance, whether the recommendation behaviours are legal and ethical or if the recommendation results lead to some good/bad impact (e.g., lead users to become addicted to video games). Ethical evaluation is full of complexity and dynamics, in which the users' cognition, perception and behaviours should be taken into account. To this end, some possible solutions include user studies, and the combination of qualitative and quantitative studies.

6 FUTURE DIRECTIONS

Truly trustworthy recommender systems. Although there are existing work aiming at building trustworthy RSs, nearly all of them focus on only one single aspect (e.g., fairness or explainability). For instance, some early work on trustworthy RSs only focuses on the robustness of RSs [30], aiming to build resilient RSs to combat attacks. More recently, some other work focuses on either explainability [57], security [23] or fairness [24]. However, to be truly trustworthy, usually all these various aspects (cf. 1.2) of trustworthiness should be carefully considered in a unified way. Therefore, more analyses are in demand to build truly trustworthy RSs.

Human-centered trustworthy recommender systems. Although some studies have attempted to build trustworthy RSs, almost all of them only mechanically developed the so-called trustworthy models from the machine perspective, while ignoring the human factor. However, whether an RS is trustworthy or not should be ultimately determined by the relevant stakeholders, rather than by the RS model itself. Therefore, human's perception and judgement should be well incorporated when developing and evaluating a trustworthy RS, which deserves a deeper investigation.

Trustworthy recommendation ecosystems. As discussed in Section 1.2, trustworthy RSs can not survive without a trustworthy recommendation ecosystem. However, almost all the existing work on trustworthy RSs only focus on the development of trustworthy RS models while ignoring other important elements, e.g., trustworthy items and providers, in the ecosystem. Therefore, more studies in the development of trustworthy recommendation ecosystems are in order.

Multi-granular fairness aware trustworthy recommender systems. Fairness is essentially multi-granular and exists at different levels [29], such as the high-level fairness between different groups, and low-level fairness between different individuals within each group. A really fair RS should be fair in all the different granularities rather than only a single granularity as done in most of the existing work. Hence, to comprehensively model multigranular fairness is of great significance for building truly fair RSs.

Fine-grained personalized recommender systems. Although it is a common sense that personalization is the core aspect and the basis of RSs, the recommendation results of most existing RSs are not personalized enough since they are mostly preferred by the majority users only while unsatisfied by the minority ones. Therefore, it is in highly demand for designing innovative RS models and evaluation approaches to ensure fine-grained personalization of recommendation results which can satisfy nearly each user.

Responsible recommender systems. Most of existing RSs are technique-driven, which are built on advanced machine learning techniques and are evaluated from the technical perspective only. The social impact of RSs are hardly considered during the design, development and evaluation of RSs. However, RSs are not only a technique issue, but also a social issue. More studies are deserved to explore how to well incorporate social impact and social science into the whole life-cycle of RSs.

New evaluation protocols and metrics. As discussed in Section 1.2, building trustworthy RSs triggers new challenges for RS evaluations. On one hand, new technical evaluation protocols and measures are in demand to comprehensively measure the trustworthiness of RSs. On the other hand, new ethical evaluation methods are needed to effectively measure the social impact of RSs.

7 CONCLUSIONS

Trustworthy recommender system (TRS) is an extremely challenging yet demanding topic, which is of both great theoretical and practical values. In this paper, we have provided a comprehensive overview of this topic. We comprehensively characterized trustworthy RSs by thoroughly analyzing the various aspects specifying the trustworthiness of RSs. We provided a novel four-stage framework to systematically illustrate trustworthy RSs and analyzed the corresponding challenges in each of the four stages in building trustworthy RSs. We have also described a conceptual framework to support trustworthy RSs and pointed out some future directions in this vibrant area. The research in trustworthy RS is flourishing and it is our hope that this work can provide readers with a comprehensive understanding of the key aspects, main challenges, key techniques when building trustworthy RSs and shed some light on future studies.

ACKNOWLEDGMENTS

This work was supported by Australian Research Council Discovery Project DP200101441.

REFERENCES

- [1] Himan Abdollahpouri, Gediminas Adomavicius, Robin Burke, and et al. 2020. Multistakeholder recommendation: Survey and research directions. *User Model. User Adapt. Interact.* 30, 1 (2020), 127–158.
- [2] Gediminas Adomavicius and YoungOk Kwon. 2011. Improving aggregate recommendation diversity using ranking-based techniques. *IEEE Trans Knowl Data Eng* 24, 5 (2011), 896–911.
- [3] Milad Ahmadian, Mahmood Ahmadi, and Sajad Ahmadian. 2022. A reliable deep representation learning to improve trust-aware recommendation systems. *Expert Systems with Applications* 197 (2022), 116697.

- [4] Krisztian Balog, Filip Radlinski, and Shushan Arakelyan. 2019. Transparent, scrutable and explainable user models for personalized recommendation. In *SIGIR*. 265–274.
- [5] Pablo Castells, Neil J. Hurley, and Saul Vargas. 2015. Novelty and diversity in recommender systems. In *Recommender Systems Handbook*, Francesco Ricci, Lior Rokach, and Bracha Shapira (Eds.). Springer, 881–918.
- [6] Jiawei Chen, Hande Dong, and et al. 2021. AutoDebias: learning to debias for recommendation. In *SIGIR*. 21–30.
- [7] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. 2021. A Survey on adversarial recommender systems: from attack/defense strategies to generative adversarial networks. *ACM Comput. Surv.* 54, 2 (2021), 1–38.
- [8] O. L. Dictionaries. 2022. Definition of trustworthy. <https://www.oxfordlearnersdictionaries.com/definition/americanenglish/trustworthy>.
- [9] Jeff Donahue and Karen Simonyan. 2019. Large scale adversarial representation learning. In *NIPS*. 10542–10552.
- [10] Manqing Dong, Feng Yuan, Lina Yao, Xianzhi Wang, Xiwei Xu, and Liming Zhu. 2022. A survey for trust-aware recommender systems: a deep learning perspective. *Knowledge-Based Systems* (2022), 108954.
- [11] Mehdi Elahi, Dietmar Jannach, Lars Skjærven, and et al. 2021. Towards responsible media recommendation. *AI and Ethics* (2021), 1–12.
- [12] Yingqiang Ge, Shuchang Liu, Zuohui Fu, and et al. 2022. A survey on trustworthy recommender systems. *arXiv preprint arXiv:2207.12515* (2022), 1–43.
- [13] Noah Giansiracusa. 2021. Tools for truth. In *How Algorithms Create and Prevent Fake News*. Springer, 217–229.
- [14] David Goldberg, David Nichols, Brian M Oki, and Douglas Terry. 1992. Using collaborative filtering to weave an information tapestry. *Commun. ACM* 35, 12 (1992), 61–70.
- [15] Asela Gunawardana and Guy Shani. 2015. Evaluating Recommender Systems. In *Recommender Systems Handbook*, Francesco Ricci, Lior Rokach, and Bracha Shapira (Eds.). Springer, 265–308.
- [16] Ihsan Gunes, Cihan Kaleli, Alper Bilge, and Huseyin Polat. 2014. Shilling attacks against recommender systems: a comprehensive survey. *Artificial Intelligence Review* 42, 4 (2014), 767–799.
- [17] Naieme Hazrati and Francesco Ricci. 2022. Recommender systems effect on the evolution of users’ choices distribution. *Inf. Process. Manag.* 59, 1 (2022), 102766.
- [18] Zengyou He, Xiaofei Xu, Zhexue Joshua Huang, and Shengchun Deng. 2005. FP-outlier: frequent pattern based outlier detection. *Computer Science and Information Systems* 2, 1 (2005), 103–118.
- [19] Keman Huang, Michael Siegel, and Stuart Madnick. 2018. Systematically understanding the cyber attack business: a survey. *Comput. Surveys* 51, 4 (2018), 1–36.
- [20] Dietmar Jannach, Pearl Pu, Francesco Ricci, and Markus Zanker. 2021. Recommender systems: past, present, future. *AI Mag.* 42, 3 (2021), 3–6.
- [21] Dietmar Jannach, Paul Resnick, Alexander Tuzhilin, and Markus Zanker. 2016. Recommender systems—beyond matrix completion. *Commun. ACM* 59, 11 (2016), 94–102.
- [22] Joseph A. Konstan and Loren G. Terveen. 2021. Human-Centered Recommender Systems: Origins, Advances, Challenges, and Opportunities. *AI Mag.* 42, 3 (2021), 31–42.
- [23] Shyong K Lam, Dan Frankowski, and et al. 2006. Do you trust your recommendations? An exploration of security and privacy issues in recommender systems. In *ETRICS*. 14–29.
- [24] Jurek Leonhardt and et al. 2018. User fairness in recommender systems. In *WWW Companion*. 101–102.
- [25] Xugang Lu, Yu Tsao, Shigeki Matsuda, and Chiori Hori. 2013. Speech enhancement based on deep denoising autoencoder. In *Interspeech*, Vol. 2013. 436–440.
- [26] Yanzhang Lyu, Hongzhi Yin, Jun Liu, Mengyue Liu, Huan Liu, and Shizhuo Deng. 2021. Reliable recommendation with review-level explanations. In *ICDE*. 1548–1558.
- [27] Jianxin Ma, Chang Zhou, Peng Cui, Hongxia Yang, and Wenwu Zhu. 2019. Learning disentangled representations for recommendation. In *NIPS*.
- [28] Paolo Massa and Paolo Avesani. 2007. Trust-aware recommender systems. In *RecSys*. 17–24.
- [29] Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, and et al. 2021. A survey on bias and fairness in machine learning. *Comput. Surveys* 54, 6 (2021), 1–35.
- [30] Bamshad Mobasher, Robin Burke, Runa Bhaumik, and et al. 2007. Toward trustworthy recommender systems: an analysis of attack models and algorithm robustness. *ACM Transactions on Internet Technology* 7, 4 (2007), 23–es.
- [31] Xia Ning, Christian Desrosiers, and et al. 2015. A comprehensive survey of neighborhood-based recommendation methods. In *Recommender Systems Handbook*, Francesco Ricci, Lior Rokach, and Bracha Shapira (Eds.). 37–76.
- [32] Cyberspace Administration of China. 2022. Regulation rules on the recommendation algorithm for internet information service. http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.
- [33] Guansong Pang, Chunhua Shen, Longbing Cao, and et al. 2021. Deep learning for anomaly detection: a review. *Comput. Surveys* 54, 2 (2021), 1–38.
- [34] Francesco Ricci, Lior Rokach, and Bracha Shapira (Eds.). 2022. *Recommender Systems Handbook*. Springer.
- [35] Xin Rong. 2014. Word2vec parameter learning explained. *arXiv preprint arXiv:1411.2738* (2014).

- [36] Tobias Schnabel, Adith Swaminathan, and et al. 2016. Recommendations as treatments: debiasing learning and evaluation. In *ICML*. 1670–1679.
- [37] Weisong Shi and et al. 2016. Edge computing: vision and challenges. *IEEE Internet of Things Journal* 3, 5 (2016), 637–646.
- [38] Hyejin Shin, Sungwook Kim, and et al. 2018. Privacy enhanced matrix factorization for recommendation with local differential privacy. *IEEE Trans Knowl Data Eng* 30, 9 (2018), 1770–1782.
- [39] Yonglong Tian, Chen Sun, Ben Poole, Dilip Krishnan, Cordelia Schmid, and Phillip Isola. 2020. What makes for good views for contrastive learning?. In *NIPS*. 6827–6839.
- [40] Laurens Van Maaten and et al. 2008. Visualizing data using t-SNE. *Journal of Machine Learning Research* 9, 11 (2008).
- [41] Shoujin Wang, Longbing Cao, Yan Wang, Quan Z Sheng, Mehmet A Orgun, and Defu Lian. 2021. A survey on session-based recommender systems. *Comput. Surveys* 54, 7 (2021), 1–38.
- [42] Shoujin Wang, Xiaofei Xu, Xiuzhen Zhang, Yan Wang, and et al. 2022. Veracity-aware and event-driven personalized news recommendation for fake news mitigation. In *WWW*. 3673–3684.
- [43] Yan Wang, Lei Li, and Guanfeng Liu. 2015. Social context-aware trust inference for trust enhancement in social network based recommendations on service providers. *World Wide Web* 18, 1 (2015), 159–184.
- [44] Yan Wang and Fu-ren Lin. 2006. Trust and risk evaluation of transactions with different amounts in peer-to-peer e-commerce environments. In *ICEBE*. 102–109.
- [45] Yan Wang, Duncan S Wong, and et al. 2008. Evaluating transaction trust and risk levels in peer-to-peer e-commerce environments. *Inf Syst E-Bus Manag* 6, 1 (2008), 25–48.
- [46] Zhenlei Wang and et al. 2021. Counterfactual data-augmented sequential recommendation. In *SIGIR*. 347–356.
- [47] Le Wu, Xiangnan He, and et al. 2022. A survey on accuracy-oriented neural recommendation: from collaborative filtering to information-rich recommendation. *IEEE Trans Knowl Data Eng* (2022).
- [48] Zhiang Wu and et al. 2012. HySAD: A semi-supervised hybrid shilling attack detector for trustworthy product recommendation. In *KDD*. 985–993.
- [49] Lin Xiao, Zhang Min, Zhang Yongfeng, Gu Zhaoquan, Liu Yiqun, and et al. 2017. Fairness-aware group recommendation with pareto-efficiency. In *RecSys*. 107–115.
- [50] Yuwen Xiong, Mengye Ren, and et al. 2020. Loco: local contrastive representation learning. In *NIPS*. 11142–11153.
- [51] Qiang Yang, Yang Liu, Yong Cheng, Yan Kang, Tianjian Chen, and Han Yu. 2019. Federated learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning* 13, 3 (2019), 1–207.
- [52] Haibin Zhang, Yan Wang, and Xiuzhen Zhang. 2012. A trust vector approach to transaction context-aware trust evaluation in e-commerce and e-service environments. In *ICSOc*. 1–8.
- [53] Haibin Zhang, Yan Wang, Xiuzhen Zhang, and et al. 2015. Reputationpro: the efficient approaches to contextual transaction trust computation in e-commerce environments. *ACM Transactions on the Web* 9, 1 (2015), 1–49.
- [54] He Zhang, Bang Wu, Xingliang Yuan, Shirui Pan, and et al. 2022. Trustworthy graph neural networks: aspects, methods and trends. *arXiv preprint arXiv:2205.07424* (2022).
- [55] Shuai Zhang, Lina Yao, Aixin Sun, and Yi Tay. 2019. Deep learning based recommender system: a survey and new perspectives. *Comput. Surveys* 52, 1 (2019), 1–38.
- [56] Xiuzhen Zhang, Lishan Cui, and Yan Wang. 2013. Commtrust: computing multi-dimensional trust by mining e-commerce feedback comments. *IEEE Trans Knowl Data Eng* 26, 7 (2013), 1631–1643.
- [57] Yongfeng Zhang, Xu Chen, et al. 2020. Explainable recommendation: a survey and new perspectives. *Foundations and Trends® in Information Retrieval* 14, 1 (2020), 1–101.
- [58] Xiaoming Zheng, Yan Wang, Mehmet Orgun, and et al. 2014. Trust prediction with propagation and similarity regularization. In *AAAI*. 237–243.