Journal Pre-proof

Latest Trends of Security and Privacy in Recommender Systems: A Comprehensive Review and Future Perspectives

Yassine Himeur, Shahab Saquib Sohail, Faycal Bensaali, Abbes Amira, Mamoun Alazab

PII: S0167-4048(22)00141-9
DOI: https://doi.org/10.1016/j.cose.2022.102746
Reference: COSE 102746

To appear in: *Computers & Security*

Received date: 15 October 2021
Revised date: 18 February 2022
Accepted date: 25 April 2022

Please cite this article as: Yassine Himeur, Shahab Saquib Sohail, Faycal Bensaali, Abbes Amira, Mamoun Alazab, Latest Trends of Security and Privacy in Recommender Systems: A Comprehensive Review and Future Perspectives, *Computers & Security* (2022), doi: https://doi.org/10.1016/j.cose.2022.102746

Highlights

- A comprehensive survey on security and privacy in recommender systems
- Investigation of security aspects, e.g. trust, authentication, privacy, and malicious attacks.
- Fairness, bias and filter bubbles of recommender systems
- Blockchain, explainable AI, edge computing, and federated learning for recommender systems

Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
00 (2022) 1–38

Latest Trends of Security and Privacy in Recommender Systems: A Comprehensive Review and Future Perspectives

Yassine Himeur[a,*], Shahab Saquib Sohail[b], Faycal Bensaali[a], Abbes Amira[c,d], Mamoun Alazab[e]

[a]Department of Electrical Engineering, Qatar University, Doha, Qatar
[b]Department of Computer Science and Engineering, School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, 110062
[c]Department of Computer Science, University of Sharjah, Sharjah, UAE
[d]Institute of Artificial Intelligence, De Montfort University, Leicester, United Kingdom
[e] College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT, Australia

Abstract

With the widespread use of Internet of things (IoT), mobile phones, connected devices and artificial intelligence (AI), recommender systems (RSs) have become a booming technology because of their capability to analyze big data and shape users' habits through well-designed, contextual, and engaging recommendations. Novel generations of RSs have been developed based on the latest AI and machine learning (ML) technologies such as big data RSs, ML-based RSs, explainable RSs, fusion-based RSs, etc. However, the characteristics of modern RSs raise new security and privacy issues because of the sensitivity of users' data and its vulnerability to being illegally accessed. Moreover, there is a lack of thorough reviews that explain the current privacy and security challenges in RSs and where the actual research is heading. To overcome these issues, this paper sheds light on the existing security and privacy concerns in modern RSs. It provides a comprehensive survey of recent research efforts on security and privacy preservation in RSs. Typically, the security and privacy aspects in advanced RSs and the latest contributions are first discussed based on a well-defined taxonomy. Next, the applications of secure and privacy-preserving RSs are studied. Moving forward, a critical analysis is conducted to (i) highlight the merits and drawbacks of existing frameworks and (ii) draw the essential findings. Lastly, future directions that attract significant research and development attention are explained.

Keywords: Recommender systems, security and privacy, trust, authentication, malicious attacks, blockchain.

1. Introduction

1.1. Background

Recommender systems (RSs) represent an essential component of most knowledge-based systems, which mainly implement information processing and analysis, ensure content delivery, support decision-making regarding different user activities. RSs have been primarily proposed to (i) assist the user in making better decisions, (ii) overcome the data overload problem, and (iii) identify and promote contents that are viewed as more convenient for each user [1, 2]. In this regard, RSs gather and process massive amounts of data of different kinds, e.g. users' preferences, users' actions, the users' current contexts (including users' locations or companies, times of the days or weeks, etc.), users' neighborhood and activities in social media and online platforms, items bought, purchased or selected by users

*Corresponding author
Email addresses: yassine.himeur@qu.edu.qa (Yassine Himeur), shahabssohail@jamiahamdard.ac.in (Shahab Saquib Sohail), f.bensaali@qu.edu.qa (Faycal Bensaali), aamira@sharjah.ac.ae (Abbes Amira), alazab.m@ieee.org (Mamoun Alazab)

(products, movies, music, etc.) [3]. To that end, aiming at efficiently processing collected data, static and/or dynamic views are usually adopted, and various algorithms are implemented to extract pertinent characteristics, starting from collaborative filtering (CF), and statistical models to artificial intelligence (AI) and matrix factorization (MF) [4].

The wide deployment of the internet of things (IoT) and connected devices (smartphones, smartwatches, smart tablets, intelligent vehicles, etc.) has significantly menaced users' privacy [5]. Specifically, studies have shown that there is increasing trends for using information from smartphones and IoT devices (e.g. real-time data, GPS locations, RFID data, etc.) [6, 7]. Typically, predictions expect that more than 75 billion IoT connected devices will be in use by 2025 worldwide [8]. While RSs are crucial for promoting and investigating the advantages of IoT services, they have a point in common that aims at generating tailored recommendations. They need accurate data related to the users' attributes, actions, preferences, or demands. Accordingly, the more precise data describing the users' profiles are, the more personalized the recommendations for the users are. Therefore, RSs glean big data for ensuring accurate and engaging recommendations, which are automatically gathered or explicitly provided by users [9]. For instance, the e-commerce sector relies on using reliable and effective RSs to grow businesses, improve revenues, and increase customer satisfaction. Thus, while automatically recorded data result from users' interaction with RSs and decision-making based on generated recommendations, users can also explicitly offer other kinds of data, especially by building their profiles and describing their likes/dislikes, or including personal information (e.g. age, gender, profession, etc.) about themselves [10]. However, both types of data can be quite sensitive in some situations, and their leakage represents a severe threat for users. In this respect, RSs face serious data privacy issues since all the RS engines, personalizing content according to users' needs, handle sensitive information from users to provide personalized recommendations. Therefore, the threat level can be high if the collected personal information is too detailed [11]. Moreover, data privacy issues can be seen to be (i) personal data breaches, (ii) information leakage that can be used to track users, (iii) recommendation data revealing customers' interests and preferences, etc. [12, 13].

On another hand, with the increasing amounts of data collected from connected devices and the advance of artificial intelligence (AI) and machine learning (ML), cloud computing, and big data analytics, RSs are increasingly engaged in heavy communication under the connection of networks, by transmitting RSs' data to remote cloudlet platforms that have powerful computing resources [14, 15]. In this regard, the overall data is collected and processed by the automated process for understanding, visualizing and extracting pertinent information [16]. In doing so, new challenges arise when sending this confidential information to the cloud servers because of the existence of different potential risks and threats of hacking and stealing this data, which in turn, can result in illicitly and illegitimately utilizing a RS and/or engendering risks related to data leaks and identity theft. In addition, nowadays, hackers use emails, social media, phone calls, and any other form of communication for stealing useful data that can help them to hack RSs, which increases the risks of hacking the RSs and leaking confidential information [17].

In order to overcome the aforementioned issues, increasing efforts have been put in recent years to develop powerful security and privacy preservation mechanisms for RSs, most of them involve the use of AI-powered tools [17, 18]. In this regard, this paper aims at (i) shedding light on most recent security and privacy issues associated with RSs based on analyzing different aspects, including trust, authentication, secure communication and end user's privacy; (ii) describing recent contributions proposed in state-of the-art to overcome these issues, (iii) analyzing the importance of security and privacy preservation of RSs' data in various application scenarios, e.g. e-commerce, healthcare, energy, IoT, social media and smart city; discussing the main open questions and research challenges that are still unresolved, and (iv) deriving a set of future orientations that can be followed to address unresolved challenges.

1.2. Related Surveys and Our Contributions

The security and privacy aspects are of utmost importance when developing RSs. Several frameworks have been proposed in the literature to address them [19]. However, very few have described the main challenges and identified future directions, attracting considerable R&D in the near and far future. For example, in [20], some general insights about privacy problems in RSs are provided. Similarly, the risks to user privacy imposed by RSs are discussed briefly in [18, 21] by overviewing existing schemes and then discussing the privacy implications for the users of RSs. Moving forward, in [22], works only discussing personalized RSs with privacy protection are reviewed. While in [23, 24], the privacy concerns are only analyzed for the case of CF-based RSs. Likewise, in [10], Zhang et al. discuss the privacy question in online RSs by investigating the influence of users' control mechanisms and data inputs. In [25], privacy risks and existing privacy preservation schemes in news-based RSs are presented.

Table 1. Comparison of the contributions of the proposed survey in comparison with other related review articles.

	Security aspects	Privacy issues	Malcious attacks	Application scenarios	Othe features, e.g. bias faireness, ethics, scalability	Future directions		
						Blockchain	Explainable AI	Edge based RSs
[10]	no	yes	no	no	no	no	no	no
[18]	no	yes	no	no	no	no	no	no
[20]	no	yes	no	no	no	no	no	no
[21]	no	yes	no	no	no	no	no	no
[22]	no	yes	no	no	no	no	no	no
[23]	no	yes	no	no	no	no	no	no
[24]	no	yes	no	no	no	no	no	no
[25]	no	yes	no	no	no	no	no	no
Our	yes	yes	yes	yes	yes	yes	yes	yes

While the aforementioned contributions have mainly focused on discussing briefly the privacy concerns in RSs, they completely ignore the security issues. Moreover, open research challenges regarding both security and privacy are also not addressed. To that end, this framework differs from existing reviews in many aspects. Therefore, it (i) lays a solid foundation to understand both security and privacy issues in all kinds of RSs, (ii) identifies current challenges related to trust, authentication, secure communication and user's privacy, and (iii) derives an ensemble of future directions attracting great interest in the near and far future. Table 1 summarizes the main contributions of this paper in comparison with other related reviews in terms of the discussed challenges, including privacy, security, malicious attacks, other features (e.g. bias, faireness, ethics and scalability) and future directions (e.g. the use of blockchain, expalianable AI and edge-based RSs). Therefore, the main contributions of this study are summarized as follows:

- Providing a comprehensive survey on security and privacy by analyzing recent frameworks and investigating different security aspects, such as trust, authentication, privacy, malicious attacks (i.e. shilling attacks, adversarial attacks, poisoning attacks, profile pollution attacks, and co-visitation injection attacks), fairness of RSs, bias of RSs, and filter bubbles of RSs.
- Describing the strengths and weaknesses of existing contributions and discussing the importance of privacy preservation and security in RSs from the application perspective, including the e-commerce, healthcare, energy, e-learning, IoT and smart city, and social networks..
- Conducting a critical discussion and extracting the important findings.
- Identifying future directions that help improve the security and privacy protection in RSs and attract significant research in the near future by adopting blockchain, explainable RSs (XRSs), explainable security (XSec), and edge/fog-based RSs.

The rest of this paper is organized as follows. Sec. 2 describes security and privacy challenges in RSs. Next, Sec. 3 discusses the principal applications of RSs and highlights the importance of security and privacy preservation in each application scenario. While Sec. 4 discusses the limitations and drawbacks of existing RS frameworks and presents the important findings. Moving on, future directions to overcome the limitations identified in this study are derived in Sec. 5. Finally, Sec. 6 presents the main conclusions drawn from this survey.

2. Security and privacy in RSs

The security and privacy issues have extensively been discussed in the literature with respect to different branches of computer science, including computer network, data security, health privacy over e-health care systems, communication security, users' privacy over social network sites (SNS) and privacy and security aspects in RSs, etc. The proliferation of the RS research has raised many related issues, and a few researches have been reported, which cover

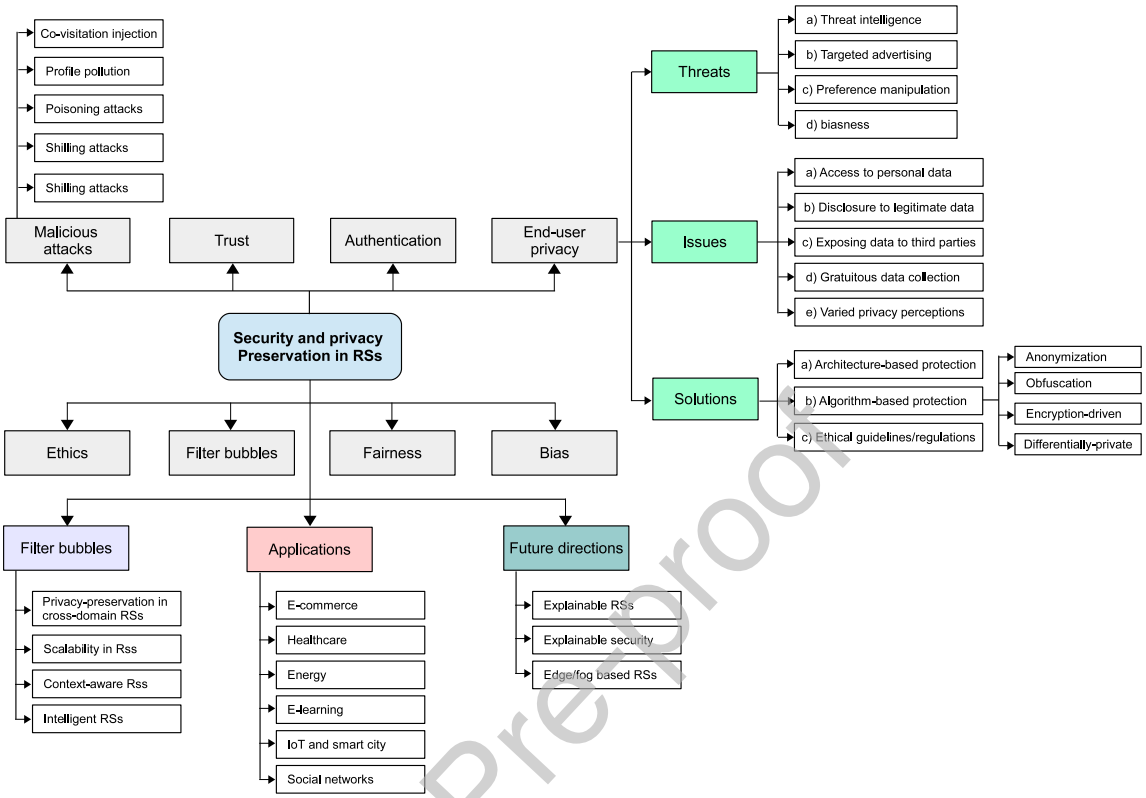

Figure 1. A generic taxonomy adopted in this paper to analyze existing frameworks of security and privacy preservation in Rss.

some aspects of user's privacy and security. However, to the best of our knowledge, a descriptive work that have comprehensively included state of the art privacy aspects as well as security concerns, is missing. Accordingly, an extensive survey that covers various privacy and security challenges is presented in this framework, such as trust, authentication, end-user's privacy, malicious attacks, fairness of RSs, bias of RSs, filter bubbles of RSs and ethics of RSs. I this regard, a generic taxonomy is adopted as portrayed in Fig. 1 to facilitate the comprehension of the main security and privacy challenges in RSs, and also provide the reader with the overall picture of the organization of the presented work.

2.1. Trust

Trust refers to the trustworthiness of both users and items. A user can be trusted if his/her reliability in making recommendation in the past is verified. The user can be a) reliable in general, i.e. the user is considered to be reliable inclusively, or b) reliable in some specific situations [26]. In addition to this, following are the noteworthy points about trust in recommendations [27, 28]: (i) trust is subjective; (ii) trust is conditionally transitive, i.e. the transitivity of trust does not always hold but it holds true sometimes, as its transitivity depends upon the context in which the users are having trust over each other; (iii) trust is not always commutative, i.e if user 1 trusts user 2, it does not imply the reverse is also true, e.g. if user 1 is an expert of a particular domain, eventually, everyone in the community would prefer to trust him/her however, the reverse may not be true. Fig. 2 illustrates the conditional transitivity and commutativity of trust in a recommender environment, and (iv) trust is not absolute, Cortesi [29] argues that trust must not only be computed by dyadic behavior rather it is greatly affected by social behavior in a community, hence, the trust is not absolute and its dynamics are updated with increased social interactions. In addition, the trust is strengthened by having trust itself, arguably, it is a self-reinforcing mechanism. Further, he has tried to fill the gap between theoretical

dyadic interaction and experimental social implications. However, the authors in [30] have discussed in detail through their experiments that CF is futile for new users in a community environment due to the cold start problems, as CF does not evaluate the neighbor of a user effectively, in turn, the global trust, which is computed by weighing similarity of neighbors found to be less productive with comparison to local trust metrics.

Thus, it remains an open question for researchers to explore whether dyadic relations are more effective in reducing the impact of cold start or traversing the complete trust network to identify the trustee and truster for each user in the network. However, in [31], authors incorporate ratings and trust both, and design a unified model by bridging these two together. They argue that there is a sparsity in the trust information itself, if rating information is added to it, they can have a greater impact. Thus, it has been shown experimentally, by providing implicit and explicit ratings and trust information, that the recommendation accuracy has improved and the influence of sparsity and cold start has decreased. Furthermore, learning the trust propagation in a trust network is one task and aggregating these knowledge for a trust enhanced RS is another one. Different approaches have been reported for designing trust aware RSs, e.g. using trust network [32], graph based [33], deep learning (DL) based [34], and CF based [35], etc. The relevant reported research on trust and related privacy issues are summarized in section 4, while a typical trust-based RS is illustrated in Fig. 3, in which the process of learning trust relationship in a usersâĂŹ trust network by the RSs for making trustworthy recommendation, is simplified. Further, it is shown that how RSs make use of trustee' preferences (right most block of the diagram) for making final recommendation.

2.2. Authentication

Although user authentication represents a critical element in most of privacy preservation RSs, it has not been widely used in most existing RSs. It is also considered as the the first layer of security in the recommendation engine. Only a limited number of works have described the importance of this stage and develop secure RSs. Among them, knowledge based authentication (KBA) [36], which has been proposed to verify the credibility of claimed identities by matching various user-related data. For instance, in [36], the manner for authenticating users with abundant rating data in RSs is studied. Typically, a quantifiable user authentication approach for RSs with secure personalized information using a Naive Bayes process is introduced.

2.3. End-user's privacy

Privacy refers to assuring information or parts of information of any individual is not accessible gratuitously to anyone, and must not be used for any unintended scope. A detailed guidelines consisting of several principles for fair information practices has been issued by the organization for economic cooperation and development (OECD) [37]. Violating any of these principles is considered a privacy breaching. We have presented a taxonomy of end user's privacy; the issues, threats and solutions in Fig. 4, which illustrates the three different aspects of end users privacy (i) the issues in the design of the RS related to user's privacy. These issues include accessing user's personal information to leaking it to third parties; (ii) the threats these issues may lead to. Typically, these different issues raise several threats to users like misuse of their data for changing their preferences (preference manipulation), e.g., voters' preferences in presidential elections; and (iii) the solutions to these problems. The solutions to the concerned issues and consequently threats can be solved in three different ways.

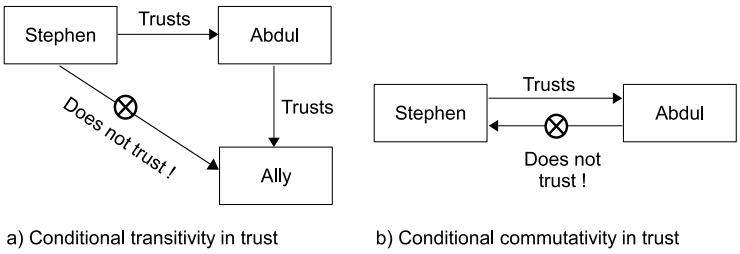

Figure 2. Conditional transitivity and commutativity in trust for RS.

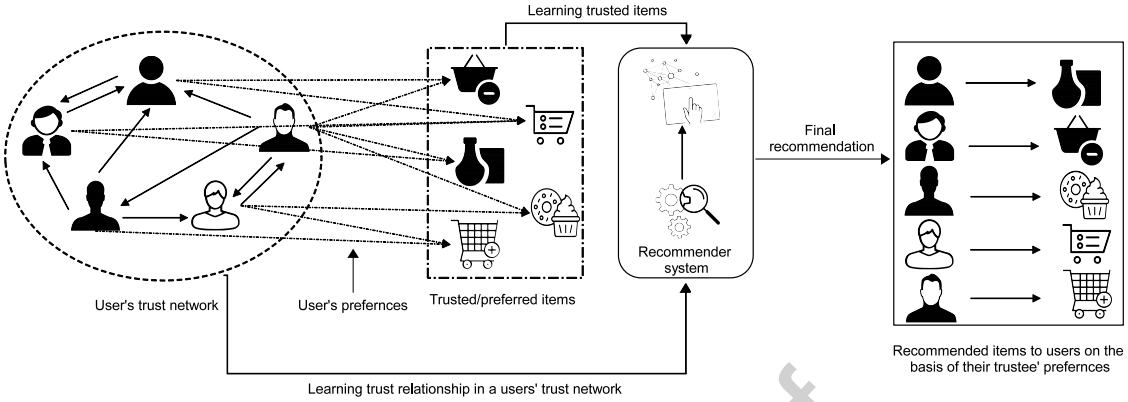

Figure 3. A typical trust-based RS.

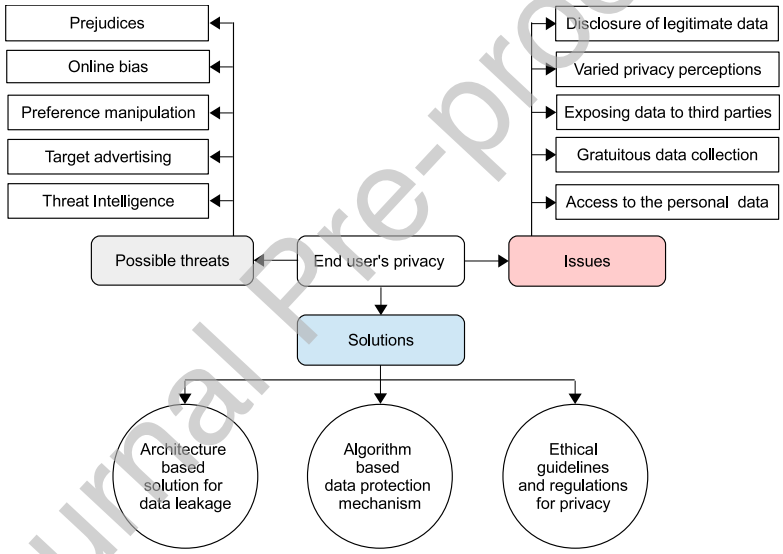

Figure 4. A taxonomy of issues, threats and solutions for end users' privacy.

2.3.1. Issues

As it is stated in the above section that violation of any principle defined by the OECD can be referred to as privacy breaching. These guidelines are related to collection and use limitations, security guards, integrity of data, purpose specification, exposure, independent involvement, and accountability, etc. Different issues that may arise while dealing with users' privacy, are discussed below.

a) Access to personal data: direct access to users' personal data is a delicate and sensitive issue, and can lead to various threats. The users personal data, also termed as personally identifiable information (PII) [38], can reveal the users demographic details, their behavior [39] and preferences [40] over online activities, their social relationship and network structure [20], their online transactions and trends [41], etc. Thus , it has remain a challenge for the researchers and service providers to design a RS in which direct access to users' data can be avoided. However, it has not been possible and one of the main reason for this is the nature of RSs, i.e., there exist a trade off between recommendation quality and users' privacy. A comprehensive information about users helps in providing a better and

accurate recommendation. However, it is the fact that threat to users' privacy is directly proportional to the detail information of users a system has.

b) Disclosure to legitimate data: users' privacy has been put on stake not only by data theft or providing an access to it to other sources illegally but also through legal data disclosure. Considering a situation in which a court orders and allows surveillance by law enforcement agencies although data access in this scenario is lawful, however, it is often conducted without any consent from users. In addition to this, there is the possibilities that this data can be gathered even without information to the service providers [21]. One more aspect worth to mention is that privacy law and data protection law are two different entities and compliance with one does not necessarily imply compliance with the other [42]. Consider anonymization of data in which data is altered or modified in such a way that it seems, it assures users' privacy, however, the research has indicated that these hidden data can be traced back through deanonymization or reidentification [43].

c) Exposing data to third parties: the users' privacy is much concerned when their data is exposed to the third parties. The nature of these third parties depends upon different platforms and scenarios. In some cases, the data is given to third parties with a good intention through anonymization, e.g., patient data can be shared among health researchers [44], and in other cases, service providers may sell the data for lucrative offers, like, web log information of the users are sold to third parties (advertisers) [45]. Some researchers have relied partially on third parties to avoid the misuse of users personal data and preserve privacy. For example, authors in [46] have split the customer data between semi trusted third party and service providers to retain the privacy as no authority will have a complete information about users. However, in this case, the third parties among themselves can share the data and they do not have any architecture to indicate if there is any collusion between merchants and still makers. There are several other threats a third party accessible data can lead to, which are discussed in the coming sections.

d) Gratuitous data collection: the users' personal data which might be collected gratuitously and unsolicited, can be sold to third parties for monetary benefits [47] or it can be of significant use in future because of the RS's ability of inferring preferences from the users' personal data. Moreover, the data storage does not bother online service providers from cost point of view as it has become cheaper, this is why the large data collection has wooed these service providers. However, it is never mandatory that the collection of data will always be threat to privacy, as in recent survey of USA school students, users have shown exemplary trust over online platforms [48] and authors have shown that the users are not always concerned for their data if they are getting a good recommendation from a trusted source. However, users are reluctant particularly in leakage of their contextual data and concerned for its tracking, probably, one of the reason for this is the ability of RS to infer, which, user might be wary for [49].

e) Varied privacy perceptions: we have stated above that the privacy has been defined delicately different and the main reason for this is the difference in perception and behavior of users towards privacy [50]. The users perceive privacy from their own context, for some particular case, the personal information revealing to which user is not interested in, he/she might be necessarily acknowledging the same to some other [51]. For example, no one would like to leak the location of spouse where she may be heading to, but at the same time, for security concerns, he must be interested in knowing her location. In fact, the privacy breaching invites the security concerns, and vice versa. Here, it is important to understand the degree of trade off between negative and positive aspects of privacy and maintain a balance in between. Some users are more concerned about their privacy, which in turn affects the personalization. On the other side, some users do not care enough for their privacy and would prefer to get accurate and appealing recommendations [52, 53]. The user behavior for different context in which their privacy may be compromised and the situation in which recommendation quality is affected, have been studied deeply in [19, 54]. The authors in [55, 50] discuss the types of users from the perspective of their privacy concerns, such as sincere, casual and over-concerned, and three privacy categories have been classified by the authors in [56], namely, collection, control and consent. However, the study suggests inference of collected data and purpose of its use may also serve as the criteria for privacy concerns [21].

2.3.2. Threats

The issues related to users' privacy discussed above may lead to potential threats to the users. These threats include fraudulent transaction, medical data theft and black mailing, misbehaving, biases, social engineering, and even put end users' lives at risk. The different threats have been discussed in the following sub-sections.

a) Threat intelligence: the study regarding threats due to the issues raised by end users' privacy risk suggests that the

expected cost for security breaches in 2020 would be 1.2 trillion US dollar which was reported 491 billion dollar in 2014 [57]. The issue of identifying actionable threat intelligence and there different parameters are yet to be deeply studied [58], however, threat intelligence refers to a situation when information about several aspects of users, by any means of intelligence, including computational, logical, analytical, etc., are exposed and can create any menace to their privacy, security or personal interests [59]. The threat intelligence, interchangeably used with cyber threat intelligence (CTI) [60], helps in boosting preventive capabilities to better understand the threat information. On the one hand it makes user aware of what security threat they may have, on the other hand actionable threat intelligence indicates an agent who may breach the security and can create menace to the users.

b) Targeted advertising: the access of the users' PII can malignly trap them in targeted advertising [38]. With the help of targeted advertising, the users' data can be exploited for the interest of the agent who is intentionally targeting the users [61]. In an infamous and one of the largest data breaching case in the history of modern technological era, executed by Cambridge Analytica, one of their employees, C. Wylie, says, "We exploited Facebook to harvest millions of people profiles. And built models to exploit what we know about them and target their inner domain that was the basis the entire company was built on." The Cambridge Analytica firm took the users personal information without prior permission and started profiling USA voters with the help of the system they built for targeting the individual voters with political advertisements [62]. These advertisements are personalized and designed for each user that best matches to their personalities so that it sounds attractive to them. Most importantly user perceives it as useful recommendation and never knew that these are targeted ads which were meant to influence their voting [63]. Further, the targeted advertising can reveal secrets which may be harmful or embarrassing [64]. For examples, ads related to personal behavior revealing teenagers private activities to their parents, confidential assignment (say a research project) may be revealed to colleagues if the related ads started popping up to your system, etc.

c) Preference manipulation: as a consequence of targeted advertising, the users can be victim of preferences manipulation without being aware of it. The preference manipulation includes targeting voters to predict and influence their preferences for the possible candidates, hence the result through ballot boxes. For example, the program can be designed in a way either to identify the individuals may be enticed to vote for their client or may be discouraged to vote for their opponents even it can play a crucial role in tipping the final result, hence, it can be understood how severe it could be. Further, this manipulation has been observed in 2016 US election. However, if not the main reason for the outcome, it has enough significance. This degree of significance has been confirmed with the help of research conducted in Stanford on 3500000 users [47]. Further, the users are menaced with a key approach of being impelled in such a way that they tend to change their behavior and preferences in the way the concealed targeting agents are guiding to. The preference manipulation mechanism can lead to grave threat to users including misguiding to opt an item which you never intended for, leaving the most suitable item to least one, and opting for a harmful option without being aware of the fact that the user has been targeted and has become a victim of targeted advertising.

d) biasness: the evidence of biasness in online purchasing through price discrimination has been reported by authors in [65, 66]. With the help of users personal data, which might be leaked or accessed through any fair or unfair means, the online merchandisers alters the price for customer accordingly. This discrimination is an obvious violation of data collection principle as stated in the OECD guidelines for fair information practices [37]. Moreover, Hanak et al. [67] has experimentally shown not only price discrimination but price steering (appearance of different products or products in different order for same search to different users for emphasizing specific products) also exist and practiced by several leading e-commerce sites.

2.3.3. Solutions

The key for the solution of the above issues and consequently, threats to the users, is keeping the balance between recommender quality and users' privacy. Since the more information about a user is provided, the better recommendation is achieved. Thus, the main challenge is to fulfill the recommendation expectations of the users without their data being compromised. Researches in the field of privacy suggest we may have (i) an architecture based solution which can assure that no data theft is possible with the suggested mechanism, (ii) an algorithmic solution for data protection. Data needs to be protected from any security attack, in addition, it must assure that the protected data is not traced back for revealing users identity and information, and (iii) ethical guidelines and regulations for privacy, which the recommendation-providing agencies must adhere to. These solution strategies have been discussed below.

a) Architecture-based protection: it is mainly used to deal with data stealing. The RS model assembles the user's

information from multiple sources to provide them with the better personalized recommendations. These data may be available with them even after the recommendation model have concluded. To assure the users regarding privacy of their personal data, the system should have earned trust from the users, for this, user must understand that (i) personal data is not disclosed without prior consent, (ii) the data storage has been designed in such a way that it has neither linked to session of any users, (iii) nor partially linked to any users profile, and (iv) the storage has temporal limitations, i.e., the data will not be kept forever, and would be removed once its (temporal) limit has reached. If users trust has not been taken into consideration, the recommender facilities may not receive a positive feedback which shall affect the product's selling [68]. For this, the authors have suggested a certification which can guarantee a honest technical audit regarding the pre-requisite aspects of a robust software capable enough to preserve the privacy [69]. Moving forward, the authors in [70] have suggested a privacy-preserving recommendation technique in which their architecture allows profile data from multiple sources to be cross-linked only from trusted parties, moreover, they can deploy entities in the multi agent system environment that permits entities to perform a well-defined task. The researchers in [46, 71] have also suggested distributed data storage as a solution to the privacy breaching, as RS maintains a centralized model to store and process data which are more prone to attacks and threats. For example, the authors in [46] suggest a theoretical approach for splitting data between operator and customer, whereas Jiang et al. [71] propose a secure distributed CF technique. They have also incorporated randomized algorithms and MF for assuring the model to be privacy preserving. Similarly, Lathia et al. [72] try to reduce the role of centralized platform for recommendation. The authors compare the similarity in rating sets of the two users, meaning thereby, the users profiles are not explored rather their rating sets are taken into consideration and they evaluate their performance by comparing two rating sets with the third one. However, the computational complexity is also a major concern while designing distributed architecture, therefore, the two stage recommendation process, i.e. modeling and recommending has emerged in which typically data is required for former stage, and recommendation is generated at the later stage.

b) Algorithm-based protection: it has been categorized in the literature into four major categories, which are based on (i) anonymization (also refer to as pseudonyms) [41], (ii) obfuscation (approaches that incorporate data modification) [73, 74, 75], (iii) encryption-driven (cryptography techniques) [76, 77] and (iv) differential privacy [78]. Each technique having their own merits and limitations.

- Anonymization is basically hiding or restricting users details. For example, if a user is active at multiple platforms, the activities and behavior of the user must not be accessible to cross-platform and keep away from the online services. Sometimes, user attributes like name, gender, age, etc. are removed so that the PII is not revealed. K-anonymity is one of the most used anonymization technique, however, it has earlier been found that anonymization has some severe issues and limitations, like there is uncertainty in guaranteed privacy [79], in addition to this, for data mining algorithms, these cannot be applied to high dimensional data as they can cause irrecoverable loss [80]. Moreover, for a less diverse attributes, an attacker can easily identify the values of these attributes which may be very delicate and vulnerable. Furthermore, k-anonymity fails in providing guaranteed privacy for attackers with some background knowledge of the subject concerned. To overcome this issue, authors in [81] propose l-diversity where they claim that an attacker is unlikely to identify the values of the attributes with such a rich diversity. However, the pre-requisite for l-diversity is that each sensitive attribute should have a corresponding value in each equivalence class. Furthermore, in l-diversity, attribute disclosure must be prevented, which is not always possible. In [82], "t-closeness" is proposed, where t is a threshold value. The central idea of their method is that the distance between the two distributions should be no more than t. By reducing the distance to t, the method restricts the attackers to gain a limited information about an individual. Rajendran et al. [83] present a comparative study of anonymization techniques namely, k-anonymity, l-diversity and t-closeness and discuss their pros and cons in details. Precisely, l-diversity lacks in preventing the exposure of sensitive attributes as there exists a semantic relationship between them, whereas, t-closeness prevents from attribute disclosures, which helps in protecting data, also it identifies the semantic closeness of attributes where l-diversity fails.

- Obfuscation (or perturbation) refers to modifying data, say, by adding some noise so that an adversaries cannot identify who the user is. Polat and Du [74] have coined the term very first time in 2003 (see Table 2), in which they hide ratings with the help of data perturbation. Interestingly, aggregation of ratings are taken into consideration for recommendations, and hence, the effect of data perturbation in recommending items to

Table 2. The first reported "algorithm-based data protection mechanisms" for RSs.

Technique	Application Area	Inconvenient
Anonymization or pseudonyms [84]	RSs, web content personalization	Uncertainty in guaranteed privacy cannot be applied to high dimensional data
Obfuscation [73, 74]	RSs, secure data modeling through data mining	Inapplicability to binary data
Encryption-driven (homomorphic encryption) [76]	RSs	Require high computational resources
Differential privacy [78]	RSs	Too much noise ultimately reduces the data utility Low performance with complex queries
Hybrid (combination of the above techniques) [85]	RSs	Increase the complexity of the RS

users are trivial. However, one of the major problems with the perturbation while noise is added to it, is its inapplicability to binary data, which is extensive in RSs, as the binary behavior logs (log of online activities like purchase data, watching video, etc.) serve as base for recommendation. Consequently, it makes noise to be easily identified. Whether demographic information like gender, can be inferred from the details revealed to RSs or not, is investigated by Weinsberg et al. [75]. They have obfuscated gender details and concluded that gender can be inferred from the information disclosed to RSs, even, they predicted the gender of a person watching movie without there rating being considered.

- Encryption-driven approaches (or cryptography techniques) diminish the users' privacy risk when data is exposed to third parties or personal information is being inferred. In addition to this, cryptography-based solutions also reduce the chance of unintentional misuse of data, e.g. they try to protect when a hacker attacks to steal the data. In [76], Canny proposes a protocol, to the best of our investigation, it is probably the first of its kind. Table 2 summarizes the first reported algorithmic approaches for privacy preserving RSs. Most of the cryptography influenced techniques use homomorphic encryption, such as [77, 86, 87, 88, 89]. However, apart from homomorphic encryption, there are the reported works that exploit privacy-preserving MF algorithm. Nikolaenko et al. [90] propose such an algorithm in which cryptoservice provider assists the recommender engine. The RS does not learn the users' rating, despite, is capable of profiling the items. They claim that the algorithm may fit for large-scale datasets. Another utilisation of homomorphic encryption is done by Jeckmans et al. [20]. They explore to recommend accurately by a merchandiser while keeping customer privacy intact without involving third parties, i.e., they would consider data from their customer and their own internal resources. They have incorporated additive homomorphic encryption in addition to division protocols. Their proposed protocol, which involves only two parties, run peer to peer between servers, it makes it convenient in providing recommendations on the basis of user-to-user similarity.

- Differentially-private algorithms [78] do not cryptographically secure the computation of RSs, rather they coerce a computation in such a way that it prevents the inference of user data from the recommendation result. It incorporates uncertainty through noise. The reason behind the guaranteed privacy by differentially private algorithms is that the preclude the ability to infer from any output even if the input is different [91]. Laplace mechanism is used by many researchers to achieve differential privacy [92, 93], in which delicately adjusted noises are added to computation. These noises are sampled from the Laplace distribution. The works in [94] and [78] both exploit differentially-private k-nearest neighbor (KNN), however they have adopted different procedures. The former have incorporated randomness in selecting KNN samples, interestingly with high similarity, whereas the later have explored differentially-private adaptation of item-item covariance matrix.

Also, one of the promising methods to address the privacy issues with the help of algorithms may be the combination of different solution approaches discussed above, for example, cryptography techniques incorporated with some architectural solutions [85, 95], MF with differential privacy [96], [97], or MF with homomorphic encryption [98, 21]. In fact, differentially private RSs are more easily integrated with other algorithm based solutions as Berlioz

et al. [97] argue that differential privacy is not a specific way to solve the privacy issue, rather, it is a concept that can be integrated to design various approaches for getting different magnitudes of success. They have shown that same differential computation for adding noise in different stages of MF is quite possible. Further, they have evaluated the added noise at different stages and suggested that input perturbation has a better performance. Similarly Kim et al. [98] incorporate MF with fully homomorphic encryption. They have performed MF over data which is encrypted and hence the output obtained is also encrypted. In doing so, the RS could not learn about both user rating and item profiles. Thus, they have achieved obfuscation without affecting the RS accuracy. More interestingly, they have reduced the time of computation which lowers the cost of using homomorphic encryption.

c) Ethical guidelines/regulations for privacy: the role of the government and law regulatory agencies are much important in preserving the users' privacy. Several governments, including USA [99] and other regulatory agencies, e.g. OECD [37] have issued the protocol for online activity to maintain the users' privacy and keep the fair information practices.

A detail discussion on how EU directives on online privacy and information disclosure by app developers, can collaborate to preserve users' privacy, is discussed by the authors in [42]. In this article, they outline the personal data disclosure problem to third parties and emphasize on the role of app developers, which they argued, can boost the data protection in the app environment. They have considered four EU data protection principles, (i) data minimisation, (ii) data security, (iii) purpose limitation, and (iv) data transparency in the context of mobile app development. In the light of the above discussion, the authors suggest few technical guidelines. However, in [100], it is argued differently and debated that the privacy is not an absolute term and differs from user to user, and hence, must be designed with this consideration. For some instance, the same user has his privacy preferences changed depending upon his interest, thus it is all about users for whom the RS is designed [43]. However, it is not easy that all users start behaving rationally, and the law regulatory agencies need to take these consideration into their account also for a safe and helpful online environment.

2.4. Malicious attacks

A RS is designed in such a way that it allows users to give their input for identifying their preferences and mapping these attributes to their neighborhood for an accurate prediction and robust recommendation [101]. This facilitates the malicious entities; an unsolicited user, an attacker or an online vendor, to attack the system for their advantage [102]. An attack on a RS is perceived as - "An external interference by means of either an automated algorithm or by maliciously intruding a noise in the database which in turn can affect the system prediction, hence resulting in an inaccurate, biased or untrustworthy recommendation."

Various studies for exploring the way an attacker can invade, detection of these attacks and possible ways to combat these malicious evasions, have been reported and a few works have also surveyed these contributions. However, the previous reviews lack in (i) coverage of diverse attack types, (ii) explaining attacks beyond CF, and (iii) discussing statistically robust detection mechanisms [103]. In what follows, we present a holistic view of security attacks and subsequently the contribution of the individuals and groups in the concerned field, types of attacks and possible solutions. Table 3 overviews the principal security attacks on RSs with respect to their features, detection techniques and cited contributions.

2.4.1. Shilling attacks (profile injection attacks)

The first to introduce the attacks in RSs were O'Mahony et al. [112]. They have discussed the different scenarios in which an attack on a RS is possible and have introduced *robustness* as an important evaluation measure in addition to accuracy. Moving on, the work in [105] has coined the term *shilling attacks* for these malicious activity, because the users behave like shills who infiltrate the recommender environment to inject bogus profiles. Since, the similarities between users' preferences which are obtained through user profiling serve as a base for RSs in a collaborative environment. Thus, these RSs are vulnerable to attacks by means of inserting bogus profiles.

The fake users' profiles can be misused by manipulating users' similarities prediction, and consequently, recommendation results. For example, a publisher may lower the ratings of the books published by other publishers, or may higher the ratings of the books published by them. Therefore, shilling attacks can lead to bias recommendations of any targeted item for selected individuals or groups. In [106], a more vivid terminology has been raised, "profile injection attack" for shilling attacks. It has been reported that the shilling behavior (promotion of some specific product) is one

Table 3. An overview of security attacks on RS with respect to their features, detection techniques and cited contributions.

Types of attacks	First reported work (Ref/Year)	Targeted recommenders	Features/Characteristics	Detection techniques	Related contributions
Shilling attacks	Concept introduced in [104]/(2002), term âĂŸshilling attacks' is coined in [105]/(2004) and term âĂŸprofile injection attack' is given by [106]/(2005)	CF based RS	Inserting bogus ratings and fake profile	statistical anomaly detection (SAD), clustering, aggregation, multi-aspect ensemble method, probability distribution (PD), convolutional neural network (CNN)	[104, 105, 106, 107] [108, 109, 110, 111] [112, 113, 114, 115] [116, 117, 118, 119] [120, 121, 122, 123]
Adversarial attacks	The effect of adversarial examples to ML was first introduced by [124] /(2013) and Generative Adversarial Networks (GAN) was introduced to CF based RS in [125]/(2017)	RS built on ML	Adversarial examples in adversarial ML	adversarial regularization, GAN, adversarial training	[126, 127, 128, 129] [130, 131, 132, 133]
Poisoning attack	Data poisoning attacks on factorization-based CF [134]/(2016)	CF and Social RS	Injecting fake ratings in social recommendations	DL and graph based approaches	[134, 135, 136, 137] [138, 139, 140, 141] [135, 142, 143, 144]
Profile pollution attacks	pollution attacks against targeted advertising [145]/(2014)	CF based RS	Polluting the users' profile by adding perturbation to their stored history		[145, 146, 138]
Co-visitation injection attacks	Fake co-visitation injection attacks to RSs [147]/ (2017)	Co-visitation RS	Inserting fake co-visitation	unified framework	[147, 148, 149, 150]

of the aspects of the attacks. However, the authors have perceived the attacks as injecting fake profiles to influence the recommendation results, and hence suggested the name.

Early works in [104, 116, 117, 118, 119] tried to investigate whether the shilling attacks or profile injection attacks is possible or not, and identified the scenario in which it can be mounted over CF based RSs. Few works, such as [114, 151, 152, 153] explore the detection mechanisms for these attacks. Usually the attacks are categorized on the basis of intent, knowledge requirement, attack dimensions, etc. Push (favoring some target item to be recommended) and nuke (lowering the rating of specified items so that it can not be listed in recommendations) are the most discussed shilling attacks' types categorised on the basis of intent of the attack. However, a general assumption about shilling attack is that it is primarily mounted for either of the above two reasons, i.e. either to push an item or to nuke the item [154].

In addition to the intent of the attack, an attack can be categorised on the strategies which are being used to attack, such as the dimension of the attack, i.e. whether the attack can be made on larger set of users or items, or it can be applied to specific targets [105, 118]. In [123], Mobasher et al. address these aspects and categorise push attacks in several categories, including (i) random attack, (ii) average attack, (iii) bandwagon attack, and (iv) segment attack. From another hand, (i) love/hate attack, and (ii) reverse bandwagon attacks are categorised as specialised nuke attack types. The prime objective in the random attack (pushing an item to favor prediction or nuking to demote an item) is attained by creating fake profiles and giving the rating to a maximum, say 5 star out of 5 or minimum, say 1 out of 5 star, depending upon the intent (push or nuke, respectively). Whereas in average attacks, the attack profile is created in such a way that it considers an average (individual mean) rating of each item for all the users and assigns the rating to filler items. Accordingly, filler items refer to the item groups, which are selected at random to which ratings are assigned inside the attack profile.

In some cases, the attackers create profiles where they use to rate only popular items, e.g. bestsellers books in the case of books or blockbuster movies in the case of movie recommendations, etc. Generally, the rating to these popular items are similar by all the users, hence it becomes easy to match the attack profiles with any target profiles. The

attacker try to associate the targeted items and rate it high (for push purpose) with the highly rated items. The above attack is an example of bandwagon attacks. In the same way, for the purpose of nuke, users can generate profiles by poorly rated items with target items. This variation is termed as reverse bandwagon attacks. However, user centric recommendation algorithms are more prone to these attacks than item centric. Therefore, item based recommendation algorithms are considered to be more robust [123]. One more point worth mentioning here is that the popularity bias (see Sec. 2.6) can be susceptible for these types of attacks.

Moving on, the segment attack refers to a situation where attackers have the knowledge of predicted preferences of target users or groups, and push the target items to them. For example, recommending a fantasy novel written for children to a ML researcher would result in a poor output, whereas its recommendation to a teenager or whose history has similar preferences, say, have purchased a fantasy drama (The lord of the rings), would be appealing. This attack is meant for item based CF and thus the item centric algorithm in this case is more vulnerable to attacks unlike the bandwagon attacks. Further, the generated profile of the users would rate high to targeted items with the preferred items and would rate to filler items to maximize the variation and boost the attack.

For the nuke purpose, the love/hate attack is found to be very influential [155, 156, 123] in which no additional knowledge is required and target items are assigned the lowest ratings, whereas all other (filler) items are assigned higher ratings. However to degrade the overall performance of the RS, no studies have suggested the false positive or negative aspects in attacks. We perceive the attack phenomena in a way is somewhat distinct from others. We suggest to create user profile in an item based CF environment where low ratings can be assigned to the expected preferred items (false positive), additionally, high ratings can be assigned to least preferred items (false negative [157]), which can be known with little efforts and knowledge, this will eventually upset the target users.

Furthermore, some researchers have categorised the attacks from the perspective of the knowledge required, i.e., whether attacker needs to have a high-level knowledge to attack or attack is possible with limited knowledge? For many attacks, users need to know rating distribution, standard deviation, etc. [123, 158]. The knowledge exploration for these attacks put a heavy cost as in the case of average attack, unlike for bandwagon attacks, attackers do not need to have diverse knowledge and can mount these attacks with limited knowledge [118, 159]. One of the serious threats that has been raised by the shills is the users' time and money. By recommending bad items, it can cost dearly to users [117, 160]. A knowledge-graph based attack to enhance the effects of several shilling attacks has been proposed in [161], however, authors have not performed the cost benefit analysis, and have not analysed the defense mechanism for their proposed model of attacks.

To achieve the accuracy in prediction and robustness in recommendation, several works have been reported suggesting various detection mechanism for shilling attacks [114, 115, 120, 121, 122]. The basic philosophy is to identify and detect the fake profiles which have been injected in the database, remove them to prevent further profile injection attacks, and consequently avoid any influence over the recommendation results. Initially, O' Mahony et al. [113] calculate the probability distribution of user profile on the basis of normalised mean absolute error. They define a threshold, for which a noise is represented by any value exceeding the threshold. To detect zero knowledge shilling attacks, Chirita et al. [162] exploit rating patterns to identify a general attacker, as the rating patterns by a genuine user and a bogus profile would differ significantly. However, researchers also consider the attack size and filler size to identify the attack profile. For instance, Burke et al. [117] take profile average deviation as a measure into consideration for exploring the difference in the number of rating by an attack profile and others.

In addition to classification mechanisms, authors have also used statistical approaches, for example, in [109], authors employ statistical anomaly detection (SAD) for detecting shilling attacks. Unlike classification techniques, Rani et al. [107] incorporate an unsupervised ML-based clustering method on different filler size and attack size over the Netflix dataset. Similarly, an unsupervised ML method has also been suggested by Cai and Zhang [108]. They have used aggregated behavior of suspicious users in identifying target items, and have claimed an improvement in accuracy in correctly identifying target items.

For collaborative RSs, the above approaches usually rely on one aspect of the user or item attributes resulting in a low precision. Hence, Hao et al. [110, 163] exploit a multi-aspects ensemble method for the detection of shilling attacks. They extract multi features and come up with a multi-aspects ensemble framework.They have experimentally shown that their results are performing better over the Netflix dataset. Although the researchers have used artificially designed features but they lack in robustness, hence, to extract deep-level features from the rating profile of a user, a CNN-based method is suggested in [111]. Authors argue that users' ratings can be precisely explained with the help of deep-level features and therefore can serve as a better option in detecting shilling attacks.

2.4.2. Adversarial attacks

Several ML techniques have been incorporated in solving the multi dimensional aspects of the recommendation technology. The growing ML research in the concerned field has also raised many challenges and issues, among them is the adversarial behavior of the ML applications [164] which puts it at risk to adversarial examples. Adversarial examples (aka adversarial samples) are intended subtle perturbations meant for compelling ML model to predict inaccurately (e.g., failing to classify an object correctly in object identification task).

Szegedy et al. [124] in an early indication to the adversarial examples have shown that even with a very low proportion, adversarial perturbations can make a neural network classifier to wrongly classify an object, e.g. misinterpreting a stop sign to a parking prohibition sign by an autonomous-driving vehicle. Adversarial attacks in RSs are the algorithms that focus on exploring such adversarial perturbations to force erroneous recommendation for influencing the recommendation results or more precisely, degrading its overall performance. For enhancing the stability and boosting the robustness of recommendations, and to tackle the above issues, Deldjoo et al. [126] come up with an idea of incorporating adversarial ML in RSs and call it as "AML-RecSys". They exploit adversarial regularization for tackling adversarial perturbations existing in the input data. Time and intent (goal) of the adversarial attacks for an ML model are important factors in dealing with it. As far as time is concerned, an adversary can attack either in training time or testing time. The attack in the first case is termed as poisoning attack (or training time attack) and for latter case, it is known as evasion attack or inference-time attack (aka pollution attack) [164]. Furthermore, the adversary can attack with two main intentions - (i) attack when target is defined (in the case of RSs, promotion or demotion of an item), and (ii) an untargeted attack (simply degrading the RS performance or maligning the image of the recommendations in the eyes of customers).

In [127], Cao et al. discuss how powerful an attack driven by adversarial examples on RS can be? and also assess the frequency of the attack with the help of a DL-based classifier. They have concluded that adversarial attacks performance is affected by the attack strength and frequency. Most of the attacks in RSs are crafted by the attackers by creating fake user profiles. Automated learning to attack RSs remains an open challenge. To answer this, in [128], authors suggest an ML technique, which makes an adversary capable to attack beyond crafted approaches advocating ML learned attacks. However, Lin et al. [129] perceive shilling attacks as a special case of adversarial attacks and have suggested a DL-based augmented shilling attack framework combining it with the idea of generative adversarial network (GAN). They have shown experimentally that their attacks can not be detected with most detection techniques.

The adversarial attacks can also influence the output of visual based RSs or multimedia RSs (MRSs) [130]. The impact of adversarial attacks on MRSs has been investigated in [131]. The authors modify the images of highly recommended items with perturbed images of low recommended items. Surprisingly, the recommendation results of the visual based recommendations have significant alterations, which confirms the impact of adversarial attacks on MRSs. The perturbation strategies, e.g. projected gradient descent (PGD), single-step fast gradient sign method (FGSM) and basic iterative method (BIM) have been well researched in some specific domain, such as computer vision. To explore these strategies further in RSs, the authors in [132] explore multi-step (iterative) perturbation strategies under minimal adversarial perturbations. They try to analyse the shortcomings of different recommender models and conclude that denser datasets can boost the robustness of a RS if it is trained over those datasets. Further, the aspect which makes the model more vulnerable is the increase in shape or the size of the model [133]. The various studies have reported the effect of adversarial attacks over reinforcement learning and contextual bandit algorithms.

2.4.3. Poisoning attacks

many researchers have used poisoning attacks and shilling attacks interchangeably [134, 135], because of the similar nature of these attacks. Both the attacks try to create fake users and generate fake ratings for a target item in consideration. However, these attacks differ in intents and approaches. A poisoning attack aims at exploiting the RS behavior for achieving the recommendation as desired by the attackers. For example, an external entity can administer malicious users for recommending the items in consideration to maximum possible users with adequately designed pseudo rating scores [137]. Additionally, the conventional shilling attacks (interchangeably termed as profile injection attacks) are meant for collaborative RSs whereas poisoning attacks can be mounted on MF-based RSs [134], graph-based RSs [135], DL based RSs [138], social RSs [136], etc.

The data poison attack is formally perceived as an optimization problem, where the intent is to maximize the attack objective (recommending the target item to maximum possible users). Bo Li et al. [134] were the first to introduce

poisoning attacks in CF based RS. They introduced an attack strategy based on an optimization technique [139] in which, on one hand, they generate fake users with malicious activities, and on the other hand, the malicious user mimic normal behavior for avoiding detection. Since the poisoning attack can be assumed as a non-convex problem, it is tough to solve the optimization issue. Therefore, authors use multiple approaches to solve it, for instance, Huang et al. [138] utilize multiple techniques for data poison attacks in a DL based RS and Zhang et al. [140] implement a poisoning neural CF based RS. In the later work, the authors also employ the approach to reduce the cost of attacks. Similarly, how poisoning attacks can influence neural CF is discussed in [141].

For designing defense mechanisms to poison attacks, several approaches have been suggested. For example, in [142], authors examine the effectiveness of these attacks over differential privacy. The many attacks which have been suggested can easily be detected by analysing rating scores, however, not many of them are optimized for graph based attacks. Hence, a defense mechanism for attacks designed for graph based RSs is crucial [135]. Moreover, many attacks are effective for RSs under the gray-box and black-box settings. Where gray box refers to settings in which parameters of the recommendation algorithm are not known but recommendation algorithms are, and black-box refers to settings where the recommendation algorithm is unknown. Moreover, in some attacks, service provider found to be intelligent enough in detecting fake users but at the same time falsely predict a few general users to be fake. Song et al. [143] propose a poison attack and name it as "PoisonRec", which requires a little knowledge for automatically learning attack strategies. PoisonRec utilizes reward signals for improving its attack strategies under the strict black-box setting. The impact of targeted poisoning attacks in indirect collaborative learning settings on DL systems is experimentally shown in [144]. It has been reported that if limited fraction of training data is poisoned by the attackers subject to the training of the final model using masked features, the targeted poisoning attacks can have a significant impact. Additionally, a statistical defense technique is designed, which exploits the fact that if malicious users do not have knowledge of data of other users, they can poison their data themselves.

2.4.4. Profile pollution attacks

The first pollution attack which authors refer to as fraud mechanism is proposed in [145] for target advertising. The authors design the attack for target advertising and generating profit to the merchandisers and other service providers over online platforms wishing to earn profit through fraudulent means. However, they face many challenges, among them is for polluting users profiles via pollution attacks. As proclaimed by the authors, this is to carefully craft pollution contents that can lead to a profitable approach for behavioral targeting and re-marketing of both types of target advertising.

Moving on, in [146], authors have explored that a profile pollution attack (PPA) aims at polluting the user's profile by exploiting cross-site request forgery (XSRF), where the users' profile refers to log information or browsing history of the users. Moreover, an attack is possible which can inject information into users' profiles for several services like, Google for web search, Amazon for online buying and YouTube for online video recommendation, etc. to influence the results of these services. A key feature of the profile pollution attack is its ability to anchorage the personalization mechanisms of these services themselves for crafting the user's experiences, rather posing any threat to user's web browser.

A primary difference between a poison attack and a pollution attack is that the former manipulates RSs at âĂIJ-training timeâĂİ, while the latter alters RSs at "testing time" [135]. The main limitation of the PPA is that it relies on XSRF, which limits its impact to smaller scale. In addition to this, PPA can pollute the users' profiles and not the items, hence, it is not useful for item-to-item RSs [138, 147].

2.4.5. Co-visitation injection attacks

The flaw of the profile pollution attack that it can not be applied to item-to-item recommendations motivated Yang et al. [147] to propose an attack which can overcome these shortcomings. They come up with an attack strategy, "fake co-visitation attack" that do not rely on XSRF. Consequently, enables it to be carried out at a large scale. Moreover, their proposed co-visitation RSs are felicitous to user-to-item as well as item-to-item recommendations. Earlier, the recommendation based on co-visitation graphs which works similar to association rules is implemented at Youtube [150]. The principle for the recommendation is based upon the assumption that if a user visits a video after watching a given video (termed as co-visitation) in a browsing session (usually twenty four hours), the two videos are related, and in future if the user watches the same video, shall visit the other also. Keeping in view the philosophy of the co-visitation, authors in [147] try to inject fake co-visitations between items.

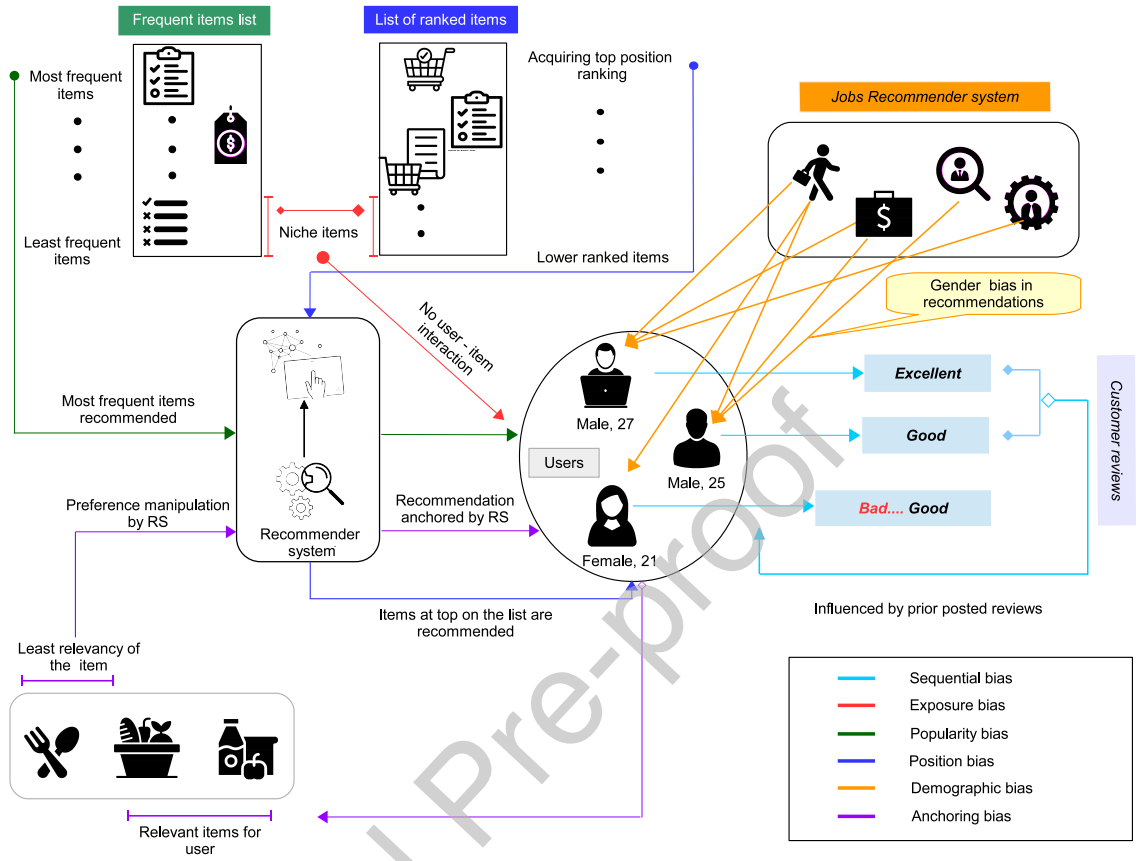

Figure 5. A block diagram for the illustration of different bias of RS

Yang et al. [149] have recently suggested a framework to identify both co-visitation attacks and profile injection attacks. Furthermore, in another work, the authors [148] suggest a similar approach and claim that their model can be integrated to detect several security attacks e.g. profile injection attacks through a unified detection framework. They argue that attackers can design a lucrative script for target items that can attract to as many users as possible for simultaneously visiting it after watching an anchor item. Anchor items refer to the list of items in which target items are not included. The point to be noted here is the restriction of the number of injectable fake co-visitations in a particular scenario. Moving forward, these fake co-visitations can be injected with different levels of knowledge that an attacker may require, from low knowledge requirement to high level knowledge. However, the selection of the anchor items and number of fake co-visitations to be injected for these items are a few important challenges in fake co-visitation injection attacks.

2.5. *Fairness of RSs*

The decision-making algorithms are widely based on the user behavior and implicit feedback for generating recommendations. The evolution of ML algorithms for these types of tasks is paramount. In this scenario, fair RSs (FRSs) can be defined as, "*the RSs which are built by the fair ML algorithms*". According to a definition suggested by Davies and Goyal [165], a fair ML algorithm neither uses protected attributes (age, gender, ethnicity, religion or its surrogate) explicitly in decision-making, nor the decision is dependant on these protected attributes. In addition to this, the predictive evaluation measures must not differ significantly over the varieties of these attributes. Considering job applicants in a company, for example, to abide by the above definitions, the system while predicting the defaulters

in making applications must exhibit similar false negative or false positive rates for white men and black women. Additionally, while predicting the success applicants, if the probability of getting success is 65% by default, the system must show equal chances for both men and women, black and white applicants. Put differently, fair recommendations can be defined as, "*the recommendation process that recommends equitably without any discrimination*". These discriminations include automated algorithmic bias or intentional discriminatory programs, which might be designed by considering protected attributes in decision-making [166]. Thus, bias recommendations lead to unfair recommendations, alternatively, unbiased RSs can be treated as FRSs. The different biases of RSs is discussed in Sec. 2.6 and illustrated in Fig. 5, where we have shown how biases of RSs can occur and consequently affect the outcome of the recommendation. In Fig. 5, sequential bias is represented with the help of arrows in sky blue color. The users have posted their reviews/opinions regarding an item and a new user who comes to share her opinion, is influenced by prior reviews and changed her mind at the last moment before putting it before the portal. This bias is called sequential bias. In continuation, in green and blue color, popularity bias and position bias have been manifested, respectively. These biases cause users to interact with the top few items which are frequent and come top in search, respectively. These biases introduce another bias in recommendations, termed as exposure bias, where niche items could not get enough exposure to users and face biasness, it is represented in red. Sometimes, RSs deliberately manipulate users' preferences to alter the outcome of a recommendation as rendered through purple arrows. The gender bias as discussed above is represented via orange color arrows where job RSs behave inequitably.

Moving on, to design a fairness-aware RS, Burke et al. [167] introduce a regularization-based approach which enables a control mechanism in establishing neighborhood for the recommendation purpose. With the help of their approach, they could handle the biases caused by statistical measures and estimates. However, authors in [168] present a method to overcome the fairness issues caused by purchase history or previous data of the users. They report that a random-influenced pattern in missing data (missing at random) and observed data (users' rating) could avoid unfairness in recommendations, because a predictable pattern can lead to a biased recommendation. For example, recommending graduate course to women would need the historical data of students enrolled in this course. According to a report of USA undergraduate studies, [169], women share only 18% bachelor degrees in computer science, hence, the model which is to be learned for the prediction may gets influenced and an equitable recommendation for men and women may not exist. Thus, recommendations can be biased. In [170], the authors introduce a causal modeling-based approach which is capable of learning anti-discrimination in recommendations. They categorize the discrimination into two different aspects, i.e. (i) whether discrimination is made direct/indirect over the protected attributes, and (ii) discrimination over protected subjects, e.g. the system, group and individual, etc. It is worth to mention that fair and safe are two different aspects, it is possible to be fair without being safe and vice versa.

2.6. Bias of RSs

Bias of RSs has been studied recently by a few researchers, however, a clear definition is missing in the literature. We define biases in RSs as, "*any intentional, logical or computational approach that influences the user preferences or alters the system's recommendation*". We say intentional because some e-commerce sites use personalization to user's disadvantage by price steering (manipulation in the display of the products or changing the order of the items shown) [67] or by price discrimination (non-uniform prices of the products across the users) [65, 66, 171, 172]. Additionally, recommendation algorithms used by YouTube is one of the best suited example of intentional approach to influence the users' preferences, as it attracts users by promoting biased content and "fake news", as a reason, the traffic remain engaged for their platform [173].

Before explaining the different biases that can occur in RSs, it would be appropriate to discuss why bias of RSs exist. Since the RS is designed to ease the information overload of the users and recommend them the best possible items [174]. To achieve this, the recommendation algorithm works on the input it receives, any biasness in data (input) can lead to biased recommendations. Furthermore, the recommender model relies mostly upon behavioral data of the user which is implicitly taken, i.e. these data are observational and not experimental, This again allows occurrence of biases in data. The presence of one kind of bias can lead the way for other biases. We simplify our statement with an example; when recommendations are generated for a user, s/he gets inclined for the few items that appear in the top of the recommendation list. However, this list does not need to be the most relevant items for the user but still its appearance in the top attracts user most. This bias is termed as position bias in RSs as users could not interact with the many items that might be relevant for them. Now, since users are more likely to go for top listed items, hence the lower ranked items in the list has gained less exposure, for the niche users, appropriate items are not shown. This leads

to another kind of bias termed as “exposure bias”. Long tail phenomena is applicable here as well, i.e. a little part of popular entities make it to interact with majority of the users. To verify the long tail phenomena in online activities, the authors in [175] have experimentally shown that from 40000 Facebook users, only 7% contribute to 50% of the contents. Similarly, the popular items are more circulated and frequently recommended than any other relevant items and it gives less chance to users to interact with other items, this bias is known as popularity bias [176], again leading to the exposure bias [177].

To identify whether a position bias exists in a RS, it has been shown in [178] that on reversing the list or random shuffling the list, users tend to click the items that appear irrespective of the relevancy of the items. More interestingly, on random shuffling, when relevant recommendation have been ranked top, it receives a higher average clickthrough rate (CTR) of 29.07% than the average CTR for that position. To solve the position bias, authors in [178] suggest click models. Sometimes, ratings that serve as the base for user feedback are missing not at random (MNAR) (See [179, 180] for a detailed discussion on MNAR) and hence it pushes the RS for another bias termed as the selection bias [181]. It implies there are the items which have not been displayed to users and missing, by virtue of which these items usually could not receive any rating, consequently, recommendation is influenced with the selection bias [182].

Following, sequential bias is encountered in a situation when users would like to give their opinion through reviews after purchasing an item. Typically, a user would get a chance to go through reviews of other customers before writing one. These reviews cause the change of mindset of the user writing a review, hence, to be written reviews are influenced [183]. Authors in [184] investigate the demographic bias RSs, i.e. bias decision on the basis of gender, age, region, cast and race. They take two online freelance marketplaces, namely Fiverr and TaskRabbit. From 13,500 profiles of the employees, they explore the demographic details of these employees and unfortunately they find the evidence of bias.

Sometimes it happen that the preferred zone of items are concealed by the RSs. To study this, the authors in [185] conduct an experiment to reveal whether a RS can manipulate user preferences or not. They conclude that the user’s preferences are highly correlated with ratings presented by a RS. Conclusively, the RS can behave as an anchor for the users’ established preferences, i.e., users’ preference ratings are flexible enough to be exigently altered by the RS. In the same direction, khenissi et al. [186] demonstrate that a RS can exhibit bias behavior as the prior exposure of the user is core in generating recommendations. One of the major set back for a bias recommendation is that it decreases diversity in recommendation and hence can loose user satisfaction and may get a low evaluation on coverage. However, diversity and exploration can significantly enhance the long term revenue for recommender providers. Above all, unbias RSs will boost fair and healthy recommendations for better online information practices [187] and all the associated beneficiaries. Furthermore, the sample size and bias have an inverse relationship, i.e. bias is found to be relatively large when the sample size is meagre [188].

2.7. Filter bubbles of RSs

In [189] the term “filter bubble” has been coined to primarily look for the existence of the filter bubble in search engines, where the objective was to exploit the biases in personalized search results. This personalized search gives different results for the same input to different users, which can trap the user in pseudo motivation and encouragement for continuing with their own belief and thoughts. This loop in which users are deceived and reinforced for their own tenets, ideology and practices, has caused misuse of users’ emotions in many ways including voting opinion manipulation (Trump), major diplomatic decisions (Brexit), etc. [190].With the growing researches in the concerned field, the existence of filter bubble over social network platforms and RSs have found by the researchers. The increasing filter bubble factor is driving the Internet users (social network platforms, ecommerce sites, web search, etc.) from the information-universe to information-village. As a consequence, the algorithm designed for recommendation or suggestion over these online platforms could lead to narrowing users choices and might drive them for some specific decisions [191]. Fig. 6 illustrates how a user can be confined in a closed loop of some specific domain and kept away from the universe diversity. The users’ history for their online activity is analysed by the recommendation engine which studies that the user is keen for news rather than any other events over Internet, hence, the news content is displayed to them on priority basis in such a way that the user involves and interacts with the similar recommendation only.

The authors in [192] investigate algorithm fairness by assessing filter bubble existence. They consider network modularity measures to propose a fairness criteria at dyadic-level. The authors successfully try to produce more heterogeneous and diverse links for combating filter bubble problems. They point out that the heterogeneous link

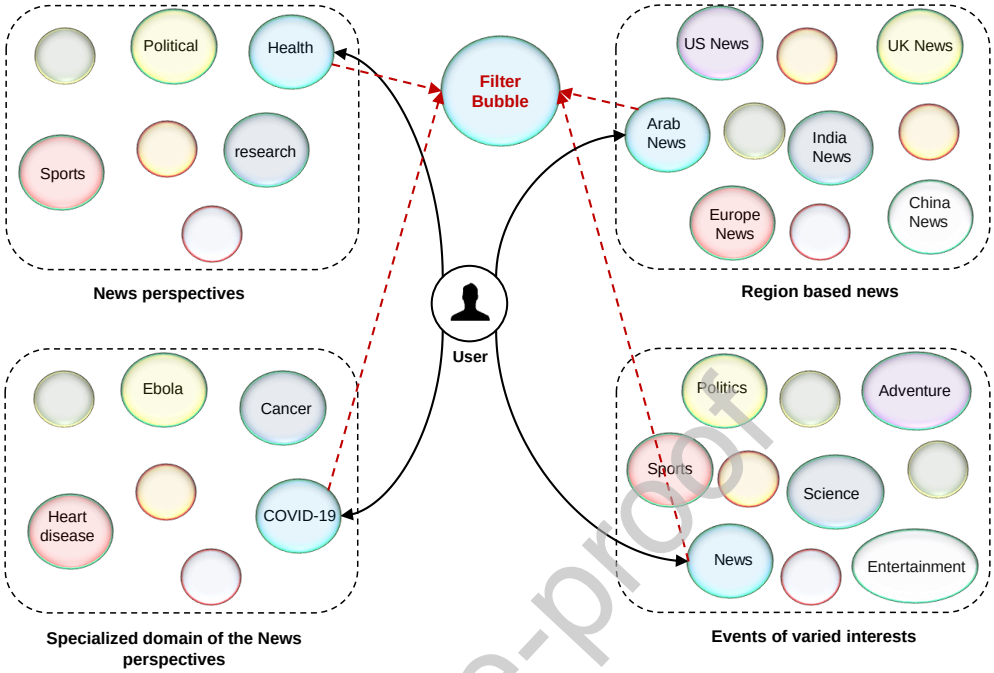

Figure 6. An illustration of the filter bubble in RSs

could dilute the filter bubble problems. However, authors in [193] explore the influence of implicit and explicit personalization on Google news. for this, they conduct an investigation related to diversity in the source and content of Google news. Surprisingly, they find no evidence of the existence of filter bubbles except a minor bias in implicit personalization. Although, they examine the filter bubble existence in specifically Google news, whereas other works confirm its existence over RSs [190, 192], online news [194] and social networking sites [191]. Thus, it is an open challenge for researchers to come forward and address the issue, and an emergent need is to design a framework for (i) investigating the issues more diversely, and (ii) proposing an acceptable solution for this to avoid any related events to happen in future, such as the Trump and Brexit issues, etc.

2.8. Ethics of RSs

The proliferation of the RS research has raised several concerns in various dimensions which have been discussed in the previous sections 2.3, 2.6 and 2.7. ML are bound to be adversarial in nature because of some of its features (see Sec. II.D.2). The adversarial nature of ML based research can cause filter bubble, bias, unfairness and polarization in recommendations [186]. For instance, one of the recently reported issues is filter bubble (see Sec. 2.7) that also put users in a loop and avoid fairness in recommendations [195].

Therefore ethical guidelines that adhere to policies and laws defined under cyber and economical transactions, and satisfies both users and vendors, is an immediate need to be regularized by the policy makers at the global as well as local level [173]. Moreover, ethics in the RS research should also assure that apart from providing satisfaction to its beneficiaries there must not be any violation to the end users' privacy which includes leakage of personal identity or exposing users to any risk that may lead to harm them in any means. Additionally, assuring that their rights are not violated is also important, i.e. users are getting fair, unbias, transparent and non-obscure recommendation. All in all, the major privacy and security aspects in RSs are outlined in Table 4 by diagrammatically explaining respective issues, major concerns and possible solutions.

Table 4. Summary of existing DL-based FMD techniques and their characteristics.

Work	Treated aspect	Dataset	Technique	Description	Advantage	Limitation
[11]	Privacy	Movielens, Flixster	Obfuscation	• First reported study to consider rating for demographic inference. Also, obfuscation was used to preserve gender privacy.	• User privacy is preserved in a scenario where recommendation needs communicating data over multiple platforms, i.e., for distributed data.	• Only one attribute "gender" is taken into consideration.
[29]	Trust	Private data with 80 agents	Mathematical modeling	• Propose a social model to identify trust dynamics and explored its relation with preferences and beliefs.	• The "belief" and "preferences" were introduced to explore the degree of trust an agent can have.	• Time-varying preferences and cheating by agents in communication are not discussed.
[31]	Trust	Ciao, Epinions, FilmTrust and Flixster	TrustSVD (MF)	• Design a unified model by bridging rating and trust, extending SVD++ with implicit and explicit influence of trust, and addressing sparsity and cold start problems.	• The first study that explores the effect of rating and trust information on recommendations, which lays a platform to identify explicit and implicit influence these both parameters on recommendations.	• The model does not fit well for top-N recommendations.
[32]	Trust	CiaoDVDs (40,133 trust relationships of 4658 users)	Hybrid CF	• Incorporate context in trust aware RSs and experimentally show enhanced performance vs. traditional RSs.	• The cold start was addressed with the help of the developed approach incorporating both trust and semantic-based social recommendation.	• Only a trust network has been considered, if a non-trustworthy comes into the picture, their work will not be productive.
[46]	Privacy	-	Theoretical approach	• Present ALAMBIC-a theoretical effort for splitting users' data between a semi-trusted third party and the service providers.	• Privacy is considered while accurately providing recommendation to users by exploiting hybrid recommendation approach.	• Heavily dependent on semi-trusted third party which may share the customer data to other third party that can lead to several threats.
[75]	Privacy	WS-DREAM	Amplified locality sensitive hashing	• Infer and obfuscate users' gender based on RS ratings.	• The method to infer the gender of users with the help of their rating has been achieved.	• Privacy-preservation effects of LSH are not evaluated.
[90]	Privacy	Movielens	MF through garbled circuits	• First reported work incorporating MF over encrypted data, and addressing scalablity issues.	• Users' profiling has been done without revealing the users' ratings. Moreover, the method can be run over very low configuration.	• Garbled circuits are vulnerable to attacks by crypto-service provider (CSP).
[97]	Privacy	Movielens	Differentially private MF	• Study the different differentially private MF and found input obfuscation as the best approach.	• Different methods incorporating MF and differential privacy were studied and input perturbation was identified as the best method to minimize privacy-accuracy tradeoff.	• There is a tradeoff between input perturbation and accuracy, hence, this approach can influence output accuracy.
[192]	Filter bubble	Fb ego network, Google +	Adversarial network and supervised link prediction	• Propose FLIP to handle the filter bubble issue, also explore the effect of protected attributes over network.	• Filter bubble issue has been alleviated through link prediction.	• This study does not explain filter bubble for CF based RS.

Table 4. (Continued)

Work	Treated aspect	Dataset	Technique	Description	Advantage	Limitation
[196]	Trust	FilmTrust	MF	• Identify top k semantic friends and address the cold start issues by capturing data implicitly.	• Context and trust were incorporated to address cold start issue, in addition, a "confidence" concept was introduced to identify trust among users.	• Distrust issues were not addressed, fake ratings could influence the outcome of their experiments, and no ways to handle profile injection is discussed.
[197]	Trust	epinions.com	CF	• Effectiveness of trust propagation for cold start issue is explored.	• Propose a solution to the malicious attacks in the bases system, where the threat of the attacks is alleviated.	• The accuracy of their approach is not evaluated.
[198]	Trust	epinions.com	CF	• Introduce a solution to cold start problems by propagating Trust aware RS	• The coverage of recommendation is increased without reducing accuracy especially for the sparse data.	• Empirical evaluation with respect to existing benchmark techniques has not been performed.
[199]	Trust	-	Axiomatic approach	• Determine the system which can alter the preferences of users in a trust network using axioms.	• Five Axioms are suggested, which can not be simultaneously satisfied by any RSs. The system which cannot be manipulated by any malicious agent is identified.	• No solution to the basic issues of RSs, e.g. cold start and sparsity, has been discussed
[200]	Trust	-	Simulation	• Identify the relation between trust aware RSs and social networks.	• The trust-based recommendations were evaluated on new evaluation measures, e.g. knowledge sparseness and network density. Their impacts on recommendations were explored.	• Identify the relation between trust aware RS and social networks.
[201]	Trust	Douban, Epinions and Flixste	Model-based with MF	• Resolve the cold start problem for trust based social CF. Distrust aspect is also taken to an extent.	• Address the cold start and data sparsity with the help of trust-based network.	• Sparsity and fake profiling is not addressed, in addition, the distrust relationship is slightly discussed without its implication on dataset.
[202]	Privacy	Jester and MovieLens Million (ML1M)	Private similarity computation protocol.	• Collaborate and conduct Top-N Recommendation.	• Top-N recommendation with privacy-preservation using the joint data while introducing reasonable overhead costs.	• Only binary categories are considered and the work is not meant for multiparty, i.e. no multi data are taken into consideration for experiments.
[203]	Fairness	Movielens	Probabilistic soft logic (PSL)	• The impact of fairness on RS accuracy and beyond accuracy is studied.	• Help in designing fair recommendation and address the observation bias as well as bias due to imbalanced data recommendation by utilizing probabilistic soft logic.	• The approach lacks exploring robustness for sparse data.

3. Applications of secure-based RSs

3.1. E-commerce

RSs have become a crucial component in most of the e-commerce applications on the web over the past decades. They allow browsers (or users) to promptly discover various products according to their preferences and tastes, and

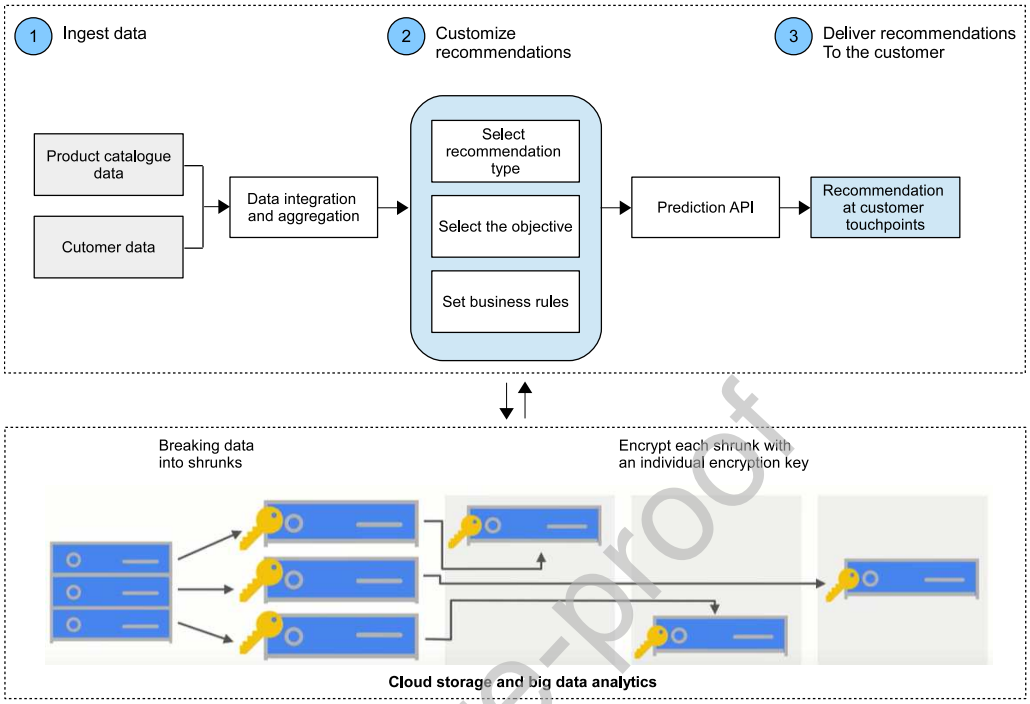

Figure 7. Flowchart of the "Recommendations AI" proposed by Google for online shopping.

simultaneously increase business value by enhancing the sales and transforming browsers into buyers [204]. As a result of the current advances, RSs in e-commerce have been modeled using different ML models to process growing amounts of data [205]. On the flip side, there are several challenges including attacks on RSs, which can be either push attacks or nuke attacks. They can negatively impact consumers satisfaction by generating fake recommendations [206]. In this regard, classifying fake profiles from genuine profiles can help improving the efficacy of e-commerce RSs and avoiding the manipulation of recommendations in e-commerce websites. Moving on, another security problem in e-commerce RSs is due to web injection, where attackers surreptitiously manipulate any unprotected in-transit HTTP web-page content and oblige victims to visiting particular items in some web recommendation services, such as, YouTube, Amazon, etc. [207].

Besides, privacy in e-commerce based RSs is another constraint as most of them are still suffering from various privacy preservation vulnerabilities. Certainly, users should have the ability to protect their sensitive information, among them their buying preferences, and they need to be safeguarded against the track of their will. Moreover, the interests of e-commerce companies need to be protected as well, and hence enabling them to produce personalized recommendations without exposing legitimately collected valuable data to third parties. To that end, immense effort is conducted nowadays to cope with these issues, through the use of blockchain [206, 208], cryptography [209], etc. A significant example in the e-commerce area could be the AI RS developed by Google, called "Recommendations AI" for delivering highly tailored product recommendations at scale for online shopping. It uses a retail application programming interface (Retail API), which in turn utilizes users' events and the product catalog for training ML based recommender algorithms and then provides recommendations based on this data. To protect sensitive data, efficient encryption mechanisms are implemented on the cloud where data is stored and complex analytics are performed to predict personalized recommendations, as it is illustrated in Fig. 7.

3.2. Healthcare

The massive amounts of data collected on the online medical platforms deter users to find useful and accurate information on time for their well-being improvement [210]. Moreover, various challenges and issues have been arisen due to the the overcharge of healthcare data (such as medical records, medical tests, and treatment suggestions), which results in huge difficulties for making patient-oriented decisions [211]. To address these challenges, RSs have been recently investigated to assist both users and medical professionals in making more effective and precise health-related decisions [212, 213].

As privacy is a main benefit for users of personalized RSs, when the latter are applied to the area of digital health, privacy protection challenges are amplified because of the nature of data used to produce recommendations and the large possible utilities of such services [214]. Typically, various studies have demonstrated that users mostly disagree with sharing data for commercial purposes but showed little concern when data is used for scientific purposes [215, 17]. In this respect, existing works have proposed different technologies to deal with the privacy concerns, including differential privacy [216], k-anonymity [217, 218], privacy-aware [219] recommendation, homomorphic encryption [17], personalized privacy trade-offs [214] and ontology-based security [220].

3.3. Energy

The use of RSs in the energy sector was mainly dedicated to (i) analyzing consumers' energy behavior via smart metering and analytics techniques, (ii) integrating social science-based consumer behavior knowledge into analysis and feedback to consumers, (iii) developing innovative service models (e.g. energy on demand services with varying price depending on request and offer).

Inspired by the methodology efficiently proposing individualized recommendations for their users, namely by exploiting micro-moments to display ads, the authors in [221] propose the $(EM)^3$ based RS framework. The innovation of the latter is to use RSs to introduce and develop breakthrough solutions for building energy-efficiency features. In addition to this, a methodology that (i) takes into account available information from the operating environment, such as the consumers' energy consumption patterns and periodic activities, (ii) proceeds with the estimation of the amount of energy needed and the typical capabilities of the operators in terms of capacity and offered costs, and (iii) recommends to consumers when it is more profitable to perform a desired activity (e.g. turn on a device, get better prices with respect to time, etc.). In this regard, in [222], a RS that adapts to the daily activities of citizens (micro-moments and habits) is proposed, which is based on long term monitoring and analysis of end-users' activities. This was possible by using a goal-based context-aware RS that helps in suggesting action recommendations at the right moment and promoting energy-saving. Moving forward, in [223], because the main objective of an energy RS is to provide end-users with personalized, accurate and engaging energy saving recommendations while ensuring a high recommendation acceptance rate, an enhancement has been conducted on the $(EM)^3$ RS by assisting the end-users with explanations to support their decision-making, increase their trust and improve the acceptance of recommendations. Therefore, the explanations have been provided in the form of ***persuasive facts*** to end-users, that include the following type of facts, (i) "the Eco type" of persuasive facts that build on the ecological impact of the energy consumption, and (ii) "the Econ type" of persuasive facts which promotes the economic impact of the energy consumption to the user. Fig. 8 illustrates the architecture of the energy saving based RS proposed in $(EM)^3$ [1].

The main limitation of the aforementioned energy saving based RSs is that they miss to address the security and privacy issues. Indeed, energy consumption data and related information (e.g. occupancy patterns and ambient conditions) are very sensitive and if a potential intruder gains access to the RS engine, it would be possible to mine and steal them. In addition, the recommendations could be biased if the identities of the authenticated users are leaked.

3.4. E-learning

Using RSs has significantly contributed to transforming and enhancing the manner in which students learn and remember course materials. for instance, the global Corona pandemic has resulted in a growing demand for e-learning platforms where it was very challenging to effectively select course contents from among various online education resources because of the differences in users' knowledge structures. Thus, the role of course RSs was significant to

[1] http://em3.qu.edu.qa/

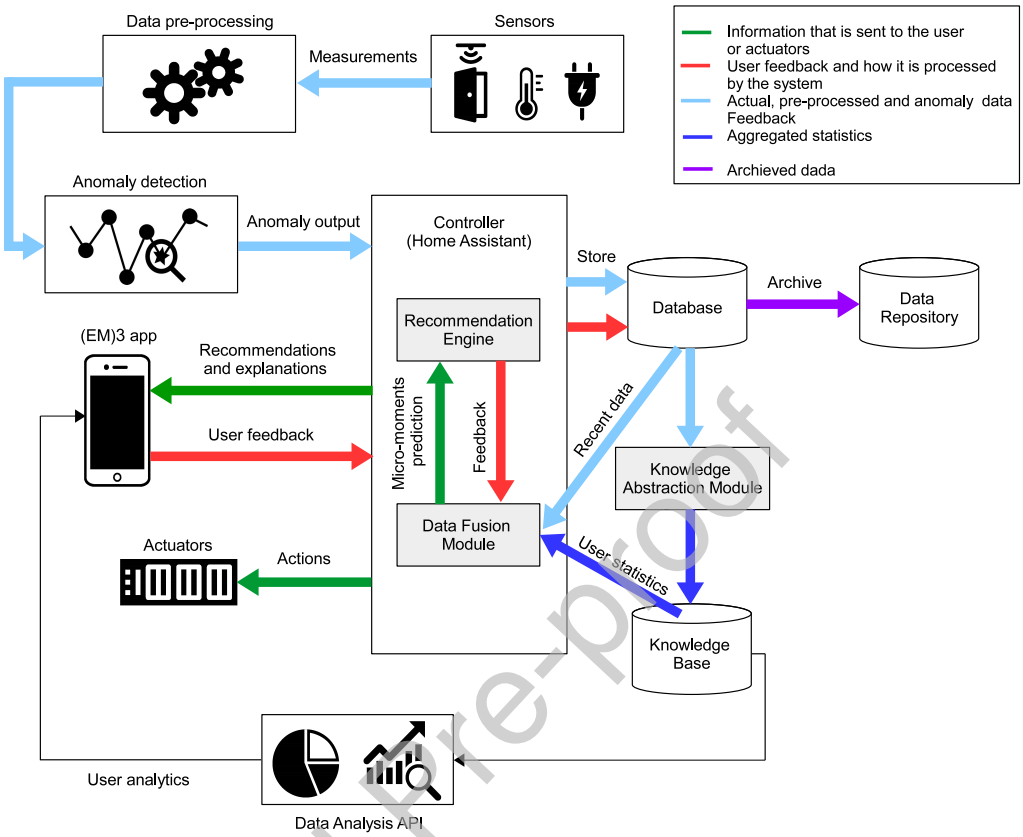

Figure 8. Overall architecture of the energy saving RS proposed in (EM)^3.

improve users' learning performance [224]. Also, students can access a large number of materials or videos to learn various topics but keep track of its relevance for them is a difficult task. To that end, RSs play an essential role in recommending education works and resources to students based on the what have previously been done [225]. A significant effort has been put in the last years to develop efficient and accurate RSs for e-learning purposes [226]. However, although the advance made, the needs for security and privacy preservation have to-date been neglected in most e-learning RSs.

3.5. IoT and smart city

With the widespread deployment of IoT devices everywhere, the use of RSs in IoT frameworks plays a major role for providing users with better services and helping them to get accurate information anytime and anywhere and make their life more convenient [227, 228]. However, because of the dynamic-heterogeneous characteristic of interconnected IoT devices, conventional RSs can not meet (i) trustworthy and user's privacy/security needs, authentication and authorization of connected things, (ii) fast and accurate recommended requirements in the current IoT environments, and (iii) information representation issues due to the heterogeneous and multimodal nature of IoT data [229]. This is in addition to the challenge of an increasing data volume which makes data processing and analysis very difficult and time consuming [230].

To address the previous issues, different studies have been proposed which present some practical solutions [231]. In [232], a location-aware service based RS with privacy-preservation in IoTs is proposed. Typically, the concepts of user/service location information and locality sensitive hashing (LSH) have been introduced. Moving on, in [233], a data-driven technique is presented for developing a privacy-setting RS for IoT devices. Specifically, by applying

ML approaches specific dataset of users, an ensemble of "intelligent profiles" has been generated. Following, the end-users are provided with privacy-preservation settings using these smart profiles. In [231], various trust based IoT RS frameworks are discussed based on a comprehensive taxonomy with regard to extracted parameters.

On the other side, because the IoT items' information description is mostly heterogeneous and multimodal, some challenges can be posed to items' representation learning of RSs. Thus, for addressing these issues and improving the recommendation effectiveness, a multimodal representation learning-based approach is investigated in [234]. Going further, aiming at solving the challenges of network discovery, navigability, and service composition is IoT, a social IoT based service RS is proposed in [235], where social relationships between devices' owners have been considered to improve the efficacy of the recommendations and increase the trust of the users on them. In a similar manner, in [236], as it is impractical to utilize users' ratings or feedback in social IoT because of the difficulty to collect this kind of data, a time-aware smart object RS is introduced by combining smart object's social similarity and users' preferences over time. This has helped in guaranteeing better recommendation effectiveness and privacy preservation.

3.6. Social networks

They are becoming the principal mediums for promoting networking, communications, and content sharing. Social networks enable users to share different types of data, e.g. news, personal information (digital photos and videos, posts, etc.), which results in generating massive amounts of data every second [237]. To that end, the use of RSs to facilitate the analysis, processing and extraction of pertinent feature from the huge amount of data is a growing field of research. Due to the nature of data shared on social networks, users pay much attention to the privacy-preservation and sensitive data protection aspects [238].

4. Discussion and important findings

4.1. Privacy-preservation in cross-domain RSs

Although user privacy protection in RSs is receiving increasing attention, most of existing research works are targeting privacy preservation in single-domain RSss, without paying attention the case of cross-domain RSs. Besides, in addition to their ability of encouraging collaboration of data between various domains for solving the data sparsity issue, the privacy-preserving cross-domain RSs are also able to ensuring end-users' sensitive data and securing the transmission of auxiliary information between domains [239]. Accordingly, there are a few studies on on this regard, among them the privacy-preserving cross-domain RS described in [240], which is mainly used for generating location-based recommendations; and the non-location-based cross-domain RS introduced in [239], which helps in (i) ensuring secure knowledge transfer between the domains, and (ii) generating secure predictions for end-users.

4.2. Scalability in RSs

The quantity of data fed into RSs is increasing significantly as more users and items/actions are added. For instance, if we take the case of an online RS, the amount of user's behavior data could rapidly attain TBs per day. Taking into consideration the massive quantity of input data in RSs, they should respond promptly in less than one second for keeping users engaged. Therefore, besides the security and privacy preservation issue, another important challenge refers to developing and integrating effective learning models into RSs for handling large volumes of data [241]. This because most of existing RSs algorithms, such as CF, can not work on users independently. By contrast, they should perform cooperative learning that helps to learn from the experience of all users, which is time-consuming as the number of users is increased.

To overcome the aforementioned problem, various works have introduced. For example, in [242], a web-based RS is built upon the use of scalable ML architecture (based on K-means clustering), which was able to analyze massive amounts of data and generate web recommendations in real-time. Accordingly, it has been implemented over a Hadoop cluster for providing scalability for an increasing number of users and URLs. Similarly, various frameworks exploit the ability of ML algorithms for extracting pertinent features for large-scale datasets to design scalalble RSs for e-learning [243, 244], social media [245], e-commerce [246], IoT [247], movie industry [248], energy efficiency [1] While in [249], the authors use online stream based approaches to deal with high throughput observations of big data RSs. Moving on, aiming at reducing the training time of review-aware RSs, Hyun et al. [250] have incorporated the

sentiments of reviews when modeling the users and items instead of concatenating the whole reviews before feeding them into a CNN model.

Moreover, to cope with the booming demand of big data analytics in RSs, other works have called in a group of agents for collaborating and then learning users' preferences and tastes, which refers to the distributed RS. However, making tailored recommendations for every user is a challenge because of the large number of candidates. Furthermore, privacy concerns raise when the information is shared among the agents. To address these challenges, Zhou et al. [251] propose a federated learning approach for training a high quality privacy-preserving centralized model and handling a big number of distributed agents. On another hand, other works has concentrated on improving the MF approaches to design scalable and large-scale RSs, such as [252, 253, 254, 255].

4.3. Context-aware RSs

In addition to the security and privacy issues that raise in RSs, the majority of works in this field focus on proposing novel schemes to increase the recommendation accuracy while ignoring other design features, such as a users' an items' context. Accordingly, another challenge for a RS is to generate engaging and on-time recommendations using contextual user-item rating information. Specifically, a context refers to a vast definition that considers several aspects; including users' location, preferences, social circle, time, weather, language, company, mood, day type, etc. In this regard, the recommendation produced should vary under different context as the rating behavior of users varies with reference the context as well.

4.4. Intelligent RSs

Because of the widespread use of connected devices in modern societies, huge amounts of data are collected every second to shape the behavior of consumers for different applications. The information overload is even more overwhelming when the multi-modality of data is considered, which the case in most of the RSs, like IoT data, financial trading or news agencies, among others. Besides, the incorporation of social networks in daily lives of the individuals has opened a new runway to generate multi-source data because social network users are great consumers of constantly changing new contents. To this end, it was of paramount importance to develop intelligent RSs for managing the increasing amounts of data using AI based cutting-edge technologies. Neural Networks, DL, model explainability or fair prediction, among others, have recently made their way in the realm of RSs, importing schemes from other AI areas for providing RSs with enhanced characteristics to process big data. In this regard, the surging of DL solutions has opened much opportunities and new challenges to deal with big data and also security and privacy issues. Several DL-based RSs, which are based on neural collaborative filtering, e.g. Wide and Deep [256], DeepFM [257], xDeepFM [258], are thus raised.

5. Future directions

5.1. Blockchain based RS

Generally, RSs are based on a central authority acting as a trusted party, which has the overall control over the recommendation framework. On the other hand, decentralized RSs can be a better alternative since they can distribute the control and responsibility tasks well in hands of the users. In this direction, as the blockchain technology is a decentralized and distributed public ledger is the best choice to develop decentralized RSs while ensuring a high level of security and privacy preservation [259, 260]. Specifically, blockchain has been recently introduced as the skeleton for creating a effective distributed infrastructures that are able to provide various features and heterogeneous services, such as secure transactions, cryptocurrencies, identity management, supply chain management, etc.

In this line, by employing blockchain in RSs, its distributed nature and efficiency can act as the required backbone to design distributed frameworks that have promising efficiency and efficacy. In addition, blockchain helps in improving the security and privacy preservation aspects and enabling other useful characteristics, among them availability, timeliness, immutability, auditability and fault tolerance. Therefore, the use of blockchain and AI can promote the development of secure RSs. For example, private blockchains help in minimizing the risks of fake profiles (identity theft), and hence combat sybil attacks in addition to shilling attacks, with regard to some participation rules. Overall, the principal advantages and differences between blockchain-based RSs and conventional decentralized RSs are outlined in Fig. 9.

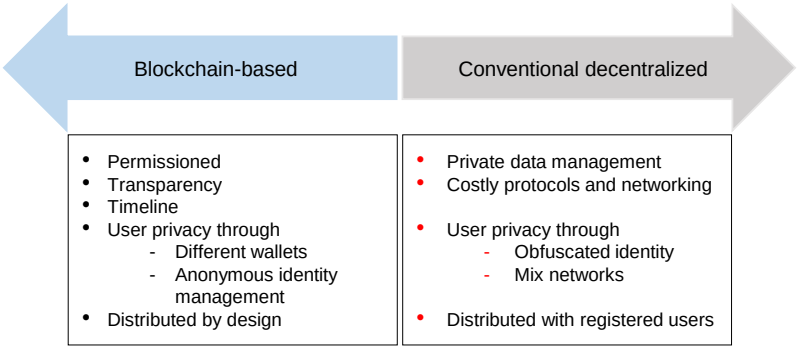

Figure 9. Principal advantages and differences between blockchain-based RSs and conventional decentralized RSs.

Therefore, the cybersecurity community is putting a great attention to integrate blockchain in RSs. This is the case of [261], in which Casino et al. utilize the blockchain as the skeleton of a decentralized RS and a decentralized locality sensitive hashing classification is adopted. This is along with an ensemble of recommender engines that have been adopted with reference to the manner data are handled by users. Thus, using private permissioned blockchain as the backbone of the RS involves that the derived RS can be high efficient and distributed by design. By consequence, this scheme relies on a two-stage process. Initially, the bucketization is performed, which helps in considerable enhancing the efficiency this approach once combined with blockchain. Next, the recommendation computation is conducted. Fig. 10 illustrates an overall architecture of a secure online RS built based on blockchain and AI.

5.2. Explainable RSs (XRSs)

RSs have a crucial role to play in different applications as explained in Sec. 3 in order to filter huge quantities of data and match users interests. While most of the RS community efforts have been committed to develop more powerful models and improve the privacy preservation of RSs, the investigation of explainability in RSs has been left behind. Indeed, providing users with intuitive explanations can help improving their experience and discovering system defects since XRSs attempt to answer the question of "why" by delivering useful recommendations to users or system designers followed by explanations about them [262]. Explanations represent the reasons behind generating the recommendations or explain the benefits from choosing the recommended items/actions. Therefore, explanations help in improving persuasiveness of the RSs, the user understanding and satisfaction and provide an immediate reward to the user.

Following the trend of explainable AI which is receiving an increasing momentum in its application in various research topics for addressing the challenges of augmented complexity, scalability and automation [263], a rapid surge in developing explainable RSs is noticed most recently. Specifically, explanations are becoming essential to ensure that users can understand and consequently trust explainable RSs. Without explanations behind the generated recommendations of a RS, there is a risk that the recommendation engine may not be considered trustworthy or legitimate [264]. There are, however, considerable issues to be overcome in order to develop explainable RS frameworks. Among them, the trade-off between reaching the simplicity of RS transparency and affecting the high-performing nature of complex but opaque RSs, i.e. if the transparency is increased, the security and privacy preservation aspects of are called into question [265, 266]. On another side, as most of the XRSs aim to explain reasons behind producing the recommenations, which can be agnostic to the context of their applications, providing unrealistic explanations. Thus, it is of utmost importance to incorporate knowledge-based models to make the explanations relevant to their application contexts.

5.3. Explainable security (XSec)

Inspired by the explainable artificial intelligence (XAI) paradigms proposed in literature [267, 268], a new concept called explainable security (XSec) has been recently appeared in [269]. The latter discusses "Six Ws" of XSec (Who?

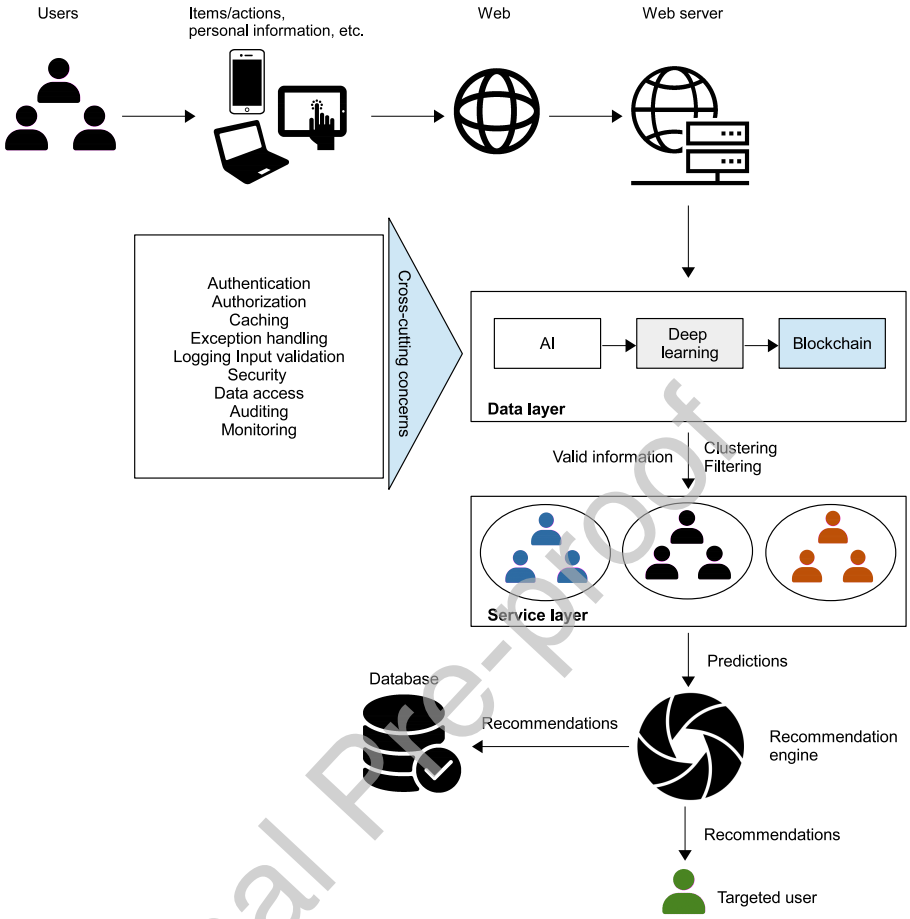

Figure 10. An example of secure RS architecture based on blockchain and AI

What? Where? When? Why? and How?) and it deserves to be further investigated for the case of RSs. Typically, XSec engages different stakeholders, such as the RS's developers, users, analysts, and attackers, and is basically multi-faceted since there are various reasoning aspects to be targeted, including those related to the RS model, threat mode and properties of security, privacy and trust along with specific attacks, vulnerabilities and countermeasures [270].

Put differently, XSec in RSs will be a new research direction that is able to bring together various cutting-edge technologies in order to develop more secure, trustworthy and engaging RSs to guide users in making appropriate decision in real-time [271]. In this context, it is expected that deploying together the competence of XAI and the innovative research on XSec, privacy and trust as a stepping stone, will help in providing some objective responses to the security and privacy issues in RSs in the near future [272]. Furthermore, it is suitable to thoroughly exploring the links and synergies between XSec and formal methods, argumentation and planning for security, as we well as with usable security, security awareness and security economics. Overall, this will be the commencement of a new friendship between explainability and security.

5.4. Edge/fog based RSs

Even though a significant effort has been paid to overcome the security and privacy issues in RSs through proposing a plethora of techniques, none of them was proficient to ensure cryptographic security and protection of users' private information. One approach to alleviate this issue is by implementing RSs on edge devices, which refers to

processing RS engines locally on the devices close to the users [273, 274]. Therefore, because it is not required to transmit data to remote cloud servers for processing, the risks of information leakage and/or hacking are much less [275]. Put differently, edge-based RSs (i) overcomes some of the security and privacy problems corresponding to the transmission and storage of sensitive personal data on the cloud, (ii) alleviates the bandwidth and latency issues that limit data transmission capacity and impede developing real-time RSs, and (iii) helps in significantly reducing the communication costs due to the use of cloudlet platforms [276, 277].

Therefore, using the edge computing is essential not only for the RSs but also for almost all the R&D fields that rely on AI, such as autonomous cars, robotics, surveillance systems, healthcare monitoring and diagnosis, etc. [276]. Additionally, by implementing the RSs on edge devices less effort is required to ensure ad-hoc maintenance usually made by data scientists or AI developers. Typically, gathered information is directly processed and analyzed before producing recommendations to be sent to the users, hence, RSs become more autonomous [278]. In this regard, research on implementing RSs on edge devices is becoming a cutting-edge challenge. For instance, the authors in [279], present an interesting tentative of developing a user-centered RS on a mobile edge device, which enable the recommendation of cultural items (e.g. Smart Search Museum). This RS is implemented using semantic searches and ML-based inference to produce accurate and intelligent recommendations.

On the other hand, fog computing has also received a great attention in the last years to meet the requirements of RSs in terms of location awareness and real-time services. The main difference of fog computing compared to edge computing is due to the fact that that the computing and intelligence tasks are brought to the local area network level of network architecture, and data are processed in fog nodes or IoT gateways [280]. For example, in [281], a fog-based hybrid RS is introduced for addressing data overload problem. In a similar manner, in [282], Ibrahim et al. develop a fog-based RS that has been employed to promote the performance of the e-learning environment. While in [283], a privacy preserving aggregation approach to overcome the privacy issues in fog-based RSs is proposed as the privacy of this kind of RSs is not straightforward.

6. Conclusion

Security and privacy preservation challenges have been well-studied in RSs, however, with the advance of AI, IoT and big data analytics as well as other related aspects such as explanability, edge and fog computing, many new security and privacy threats arise, which were not present in traditional RSs. Moreover, as far as we are aware, there is not any comprehensive review article that deeply discusses both security and privacy issues in RSs and covers the challenges that remain unresolved. To fill that gap, we present an extensive survey of security and privacy questions and frameworks in modern RSs.

In doing so, a taxonomy of existing frameworks is carried out, in which the related works have been classified into different classes that concern numerous challenges, including trust, authentication, secure communication, malicious attacks, fairness and bias along with filter bubbles and ethics in RSs. Moving forward, different applications in which the security and privacy tasks are overwhelming have been described and their main concerns have been highlighted. Next, important findings are derived via conducting a deep discussion before outlining future research directions to solve different challenges in privacy and security in RSs and also improve them with regard to other aspects. In this line, a great attention has been put to emphasize the importance of blockchain, explainablity and edge/fog computing in modern and future RSs.

The blockchain, explainable AI, edge computing, and federated learning technologies have recently opened new research perspectives for RSs. From one hand, the decentralized nature of blockchain and federated learning environments helps alleviate the security and privacy problems and process RS engines locally on the edge devices to reduce communication latency. On the other hand, intuitive explanations produced by explainable RSs enable improve users' experience and discover system defects. To that end, our future work will focus on profoundly investigating the contributions of these technologies in developing secure and privacy-preserving RSs for different applications, such as building energy efficiency, smart buildings, and e-healthcare.

Acknowledgements

This paper was made possible by National Priorities Research Program (NPRP) grant No. 10-0130-170288 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the

responsibility of the authors.

References

[1] P. Wei, S. Xia, R. Chen, J. Qian, C. Li, X. Jiang, A deep-reinforcement-learning-based recommender system for occupant-driven energy optimization in commercial buildings, IEEE Internet of Things Journal 7 (7) (2020) 6402–6413.

[2] Y. Himeur, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, G. Bravos, C. Sardianos, G. Dimitrakopoulos, Techno-economic assessment of building energy efficiency systems using behavioral change: A case study of an edge-based micro-moments solution, Journal of Cleaner Production 331 (2022) 129786.

[3] Y. Yang, J. Xu, Z. Xu, P. Zhou, T. Qiu, Quantile context-aware social iot service big data recommendation with d2d communication, IEEE Internet of Things Journal 7 (6) (2020) 5533–5548.

[4] W. Wang, J. Chen, J. Wang, J. Chen, Z. Gong, Geography-aware inductive matrix completion for personalized point-of-interest recommendation in smart cities, IEEE Internet of Things Journal 7 (5) (2019) 4361–4370.

[5] L. Strous, S. von Solms, A. Zúquete, Security and privacy of the internet of things, Computers & Security 102 (2021) 102148.

[6] M. A. S. Bubukayr, M. A. Almaiah, Cybersecurity concerns in smart-phones and applications: A survey, in: 2021 International Conference on Information Technology (ICIT), IEEE, 2021, pp. 725–731.

[7] A. Gadi, Factors influencing privacy control practices of users of mobile devices and smartphones, Social software (2021).

[8] Iot platforms: enabling the internet of things. whitepaper, ihs technology., Available online: `https://cdn.ihs.com/www/pdf/enabling-IOT.pdf`, accessed: 2021-02-01.

[9] I. Portugal, P. Alencar, D. Cowan, The use of machine learning algorithms in recommender systems: A systematic review, Expert Systems with Applications 97 (2018) 205–227.

[10] B. Zhang, N. Wang, H. Jin, Privacy concerns in online recommender systems: influences of control and user data input, in: 10th Symposium On Usable Privacy and Security ({SOUPS} 2014), 2014, pp. 159–173.

[11] X. Chi, C. Yan, H. Wang, W. Rafique, L. Qi, Amplified locality-sensitive hashing-based recommender systems with privacy protection, Concurrency and Computation: Practice and Experience (2020) e5681.

[12] Y. W. Song, H. S. Lim, J. Oh, "we think you may like this": An investigation of electronic commerce personalization for privacy-conscious consumers, Psychology & Marketing 38 (10) (2021) 1723–1740.

[13] N. Chawla, B. Kumar, E-commerce and consumer protection in india: The emerging trend, Journal of Business Ethics (2021) 1–24.

[14] A. Alsalemi, Y. Himeur, F. Bensaali, A. Amira, An innovative edge-based internet of energy solution for promoting energy saving in buildings, Sustainable Cities and Society 78 (2022) 103571.

[15] M. Rahhali, L. Oughdir, Y. Jedidi, Y. Lahmadi, M. Z. El Khattabi, E-learning recommendation system based on cloud computing, in: WITS 2020, Springer, 2022, pp. 89–99.

[16] X. Ren, H. Yin, T. Chen, H. Wang, N. Q. V. Hung, Z. Huang, X. Zhang, Crsal: Conversational recommender systems with adversarial learning, ACM Transactions on Information Systems (TOIS) 38 (4) (2020) 1–40.

[17] A. C. Valdez, M. Ziefle, The usersÃćâĆňâĎć perspective on the privacy-utility trade-offs in health recommender systems, International Journal of Human-Computer Studies 121 (2019) 108–121.

[18] B. P. Knijnenburg, S. Berkovsky, Privacy for recommender systems: tutorial abstract, in: Proceedings of the Eleventh ACM Conference on Recommender Systems, 2017, pp. 394–395.

[19] B. P. Knijnenburg, A. Kobsa, Making decisions about privacy: information disclosure in context-aware recommender systems, ACM Transactions on Interactive Intelligent Systems (TiiS) 3 (3) (2013) 1–23.

[20] A. J. Jeckmans, M. Beye, Z. Erkin, P. Hartel, R. L. Lagendijk, Q. Tang, Privacy in recommender systems, in: Social media retrieval, Springer, 2013, pp. 263–281.

[21] A. Friedman, B. P. Knijnenburg, K. Vanhecke, L. Martens, S. Berkovsky, Privacy aspects of recommender systems, in: Recommender systems handbook, Springer, 2015, pp. 649–688.

[22] C. Wang, Y. Zheng, J. Jiang, K. Ren, Toward privacy-preserving personalized recommendation services, Engineering 4 (1) (2018) 21–28.

[23] A. Bilge, C. Kaleli, I. Yakut, I. Gunes, H. Polat, A survey of privacy-preserving collaborative filtering schemes, International Journal of Software Engineering and Knowledge Engineering 23 (08) (2013) 1085–1108.

[24] I. Elnabarawy, W. Jiang, D. C. Wunsch II, Survey of privacy-preserving collaborative filtering, arXiv preprint arXiv:2003.08343 (2020).

[25] I. Mohallick, Ö. Özgöbek, Exploring privacy concerns in news recommender systems, in: Proceedings of the International Conference on Web Intelligence, 2017, pp. 1054–1061.

[26] J. O'Donovan, B. Smyth, Trust in recommender systems, in: Proceedings of the 10th international conference on Intelligent user interfaces, 2005, pp. 167–174.

[27] A. Abdul-Rahman, S. Hailes, A distributed trust model, in: Proceedings of the 1997 workshop on New security paradigms, 1998, pp. 48–60.

[28] R. Falcone, C. Castelfranchi, Trust and transitivity: a complex deceptive relationship, TRUST@ AAMAS 10 (2010) 43–53.

[29] M. Cortesi, The social dynamics of learning and trust, in: Paper presented at the DIME Final Conference, Vol. 6, Citeseer, 2011, p. 8.

[30] P. Massa, P. Avesani, Trust-aware recommender systems, in: Proceedings of the 2007 ACM conference on Recommender systems, 2007, pp. 17–24.

[31] G. Guo, J. Zhang, N. Yorke-Smith, A novel recommendation model regularized with user trust and item ratings, ieee transactions on knowledge and data engineering 28 (7) (2016) 1607–1620.

[32] Z. El Yebdri, S. M. Benslimane, F. Lahfa, M. Barhamgi, D. Benslimane, Context-aware recommender system using trust network, Computing (2021) 1–19.

[33] C.-W. Hang, M. P. Singh, Trust-based recommendation based on graph similarity, in: Proceedings of the 13th International Workshop on Trust in Agent Societies (TRUST). Toronto, Canada, Vol. 82, 2010.

[34] M. Dong, F. Yuan, L. Yao, X. Wang, X. Xu, L. Zhu, Trust in recommender systems: A deep learning perspective, arXiv preprint arXiv:2004.03774 (2020).
[35] P. Victor, M. De Cock, C. Cornelis, Trust and recommendations, in: Recommender systems handbook, Springer, 2011, pp. 645–675.
[36] Z. Wu, L. Yu, H. Sun, Z. Guan, Z. Chen, Authenticating users of recommender systems using naive bayes, in: International Conference on Web Information Systems Engineering, Springer, 2013, pp. 199–208.
[37] H. Regard, Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013).
[38] B. Krishnamurthy, C. E. Wills, On the leakage of personally identifiable information via online social networks, in: Proceedings of the 2nd ACM workshop on Online social networks, 2009, pp. 7–12.
[39] O. Enaizan, A. Zaidan, N. M. Alwi, B. Zaidan, M. Alsalem, O. Albahri, A. Albahri, Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis, Health and Technology 10 (3) (2020) 795–822.
[40] G. Iachello, J. Hong, End-user privacy in human-computer interaction, Vol. 1, Now Publishers Inc, 2007.
[41] N. Polatidis, C. K. Georgiadis, E. Pimenidis, E. Stiakakis, Privacy-preserving recommendations in context-aware mobile environments, Information & Computer Security (2017).
[42] Y. S. Van Der Sype, W. Maalej, On lawful disclosure of personal user data: What should app developers do?, in: 2014 IEEE 7th International Workshop on Requirements Engineering and Law (RELAW), IEEE, 2014, pp. 25–34.
[43] P. Ohm, Broken promises of privacy: Responding to the surprising failure of anonymization, UCLA l. Rev. 57 (2009) 1701.
[44] G. J. Annas, et al., Hipaa regulations-a new era of medical-record privacy?, New England Journal of Medicine 348 (15) (2003) 1486–1490.
[45] L. Bunnell, K.-M. Osei-Bryson, V. Y. Yoon, Recsys issues ontology: a knowledge classification of issues for recommender systems researchers, Information Systems Frontiers 22 (6) (2020) 1377–1418.
[46] E. Aïmeur, G. Brassard, J. M. Fernandez, F. S. M. Onana, A lambic: a privacy-preserving recommender system for electronic commerce, International Journal of Information Security 7 (5) (2008) 307–334.
[47] J. Isaak, M. J. Hanna, User data privacy: Facebook, cambridge analytica, and privacy protection, Computer 51 (8) (2018) 56–59.
[48] M. S. Crocco, A. Segall, A.-L. Halvorsen, A. Stamm, R. Jacobsen, "it's not like they're selling your data to dangerous people": Internet privacy, teens, and (non-) controversial public issues, The Journal of Social Studies Research 44 (1) (2020) 21–33.
[49] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, J. Zhang, Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing, in: Proceedings of the 2012 ACM conference on ubiquitous computing, 2012, pp. 501–510.
[50] N. K. Malhotra, S. S. Kim, J. Agarwal, Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model, Information systems research 15 (4) (2004) 336–355.
[51] O. R. Sanchez, I. Torre, Y. He, B. P. Knijnenburg, A recommendation approach for user privacy preferences in the fitness domain, User Modeling and User-Adapted Interaction (2019) 1–53.
[52] N. F. Awad, M. S. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS quarterly (2006) 13–28.
[53] J. Whitaker, M. S. Krishnan, C. Fornell, F. Morgeson, How does customer service offshoring impact customer satisfaction?, Journal of Computer Information Systems (2019).
[54] T. Kroll, S. Stieglitz, Digital nudging and privacy: improving decisions about self-disclosure in social networks, Behaviour & Information Technology (2019) 1–19.
[55] J. S. Daniel, Privacy self-management and the consent dilemma, Harvard Law Review 126 (2013) 1880.
[56] H. J. Smith, S. J. Milberg, S. J. Burke, Information privacy: Measuring individuals' concerns about organizational practices, MIS quarterly (1996) 167–196.
[57] T. D. Wagner, K. Mahbub, E. Palomar, A. E. Abdallah, Cyber threat intelligence sharing: Survey and research directions, Computers & Security 87 (2019) 101589.
[58] Y. Gao, L. Xiaoyong, P. Hao, B. Fang, P. Yu, Hincti: A cyber threat intelligence modeling and identification system based on heterogeneous information network, IEEE Transactions on Knowledge and Data Engineering (2020).
[59] M. Al-Hawawreh, N. Moustafa, S. Garg, M. S. Hossain, Deep learning-enabled threat intelligence scheme in the internet of things networks, IEEE Transactions on Network Science and Engineering (2020).
[60] M. F. Haque, R. Krishnan, Toward automated cyber defense with secure sharing of structured cyber threat intelligence, Information Systems Frontiers (2021) 1–14.
[61] S. A. Osia, A. S. Shamsabadi, S. Sajadmanesh, A. Taheri, K. Katevas, H. R. Rabiee, N. D. Lane, H. Haddadi, A hybrid deep learning architecture for privacy-preserving mobile analytics, IEEE Internet of Things Journal 7 (5) (2020) 4505–4518.
[62] C. Cadwalladr, E. Graham-Harrison, Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach, The guardian 17 (2018) 22.
[63] C. Cadwalladr, I made steve bannonÃćâĆňâĎćs psychological warfare toolÃćâĆňâĎć: meet the data war whistleblower.[online] the guardian (2018).
[64] S. C. Boerman, S. Kruikemeier, F. J. Zuiderveen Borgesius, Online behavioral advertising: A literature review and research agenda, Journal of advertising 46 (3) (2017) 363–376.
[65] J. Mikians, L. Gyarmati, V. Erramilli, N. Laoutaris, Detecting price and search discrimination on the internet, in: Proceedings of the 11th ACM workshop on hot topics in networks, 2012, pp. 79–84.
[66] J. Mikians, L. Gyarmati, V. Erramilli, N. Laoutaris, Crowd-assisted search for price discrimination in e-commerce: First results, in: Proceedings of the ninth ACM conference on Emerging networking experiments and technologies, 2013, pp. 1–6.
[67] A. Hannak, G. Soeller, D. Lazer, A. Mislove, C. Wilson, Measuring price discrimination and steering on e-commerce web sites, in: Proceedings of the 2014 conference on internet measurement conference, 2014, pp. 305–318.
[68] I. Palomares, C. Porcel, L. Pizzato, I. Guy, E. Herrera-Viedma, Reciprocal recommender systems: Analysis of state-of-art literature, challenges and opportunities towards social recommendation, Information Fusion 69 (2021) 103–127.

[69] J. Stafford, K. Wallnau, Is third party certification necessary?, in: Proceedings of the 4th ICSE Workshop on Component-based Software Engineering: Component Certification and System Prediction, 2001, pp. 13–17.
[70] R. Cissée, S. Albayrak, An agent-based approach for privacy-preserving recommender systems, in: Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems, 2007, pp. 1–8.
[71] J.-Y. Jiang, C.-T. Li, S.-D. Lin, Towards a more reliable privacy-preserving recommender system, Information Sciences 482 (2019) 248–265.
[72] N. Lathia, S. Hailes, L. Capra, Private distributed collaborative filtering using estimated concordance measures, in: Proceedings of the 2007 ACM conference on Recommender systems, 2007, pp. 1–8.
[73] R. Agrawal, R. Srikant, Privacy-preserving data mining, in: Proceedings of the 2000 ACM SIGMOD international conference on Management of data, 2000, pp. 439–450.
[74] H. Polat, W. Du, Privacy-preserving collaborative filtering using randomized perturbation techniques, in: Third IEEE International conference on data mining, IEEE, 2003, pp. 625–628.
[75] U. Weinsberg, S. Bhagat, S. Ioannidis, N. Taft, Blurme: Inferring and obfuscating user gender based on ratings, in: Proceedings of the sixth ACM conference on Recommender systems, 2012, pp. 195–202.
[76] J. Canny, Collaborative filtering with privacy, in: Proceedings 2002 IEEE Symposium on Security and Privacy, IEEE, 2002, pp. 45–57.
[77] Z. Erkin, T. Veugen, T. Toft, R. L. Lagendijk, Generating private recommendations efficiently using homomorphic encryption and data packing, IEEE transactions on information forensics and security 7 (3) (2012) 1053–1066.
[78] F. McSherry, I. Mironov, Differentially private recommender systems: Building privacy into the netflix prize contenders, in: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, 2009, pp. 627–636.
[79] S. R. Ganta, S. P. Kasiviswanathan, A. Smith, Composition attacks and auxiliary information in data privacy, in: Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining, 2008, pp. 265–273.
[80] J. Brickell, V. Shmatikov, The cost of privacy: destruction of data-mining utility in anonymized data publishing, in: Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining, 2008, pp. 70–78.
[81] A. Machanavajjhala, D. Kifer, J. Gehrke, M. Venkitasubramaniam, l-diversity: Privacy beyond k-anonymity, ACM Transactions on Knowledge Discovery from Data (TKDD) 1 (1) (2007) 3–es.
[82] N. Li, T. Li, S. Venkatasubramanian, t-closeness: Privacy beyond k-anonymity and l-diversity, in: 2007 IEEE 23rd International Conference on Data Engineering, IEEE, 2007, pp. 106–115.
[83] K. Rajendran, M. Jayabalan, M. E. Rana, A study on k-anonymity, l-diversity, and t-closeness techniques, IJCSNS 17 (12) (2017) 172.
[84] R. M. Arlein, B. Jai, M. Jakobsson, F. Monrose, M. K. Reiter, Privacy-preserving global customization, in: Proceedings of the 2nd ACM conference on Electronic commerce, 2000, pp. 176–184.
[85] M. Pettai, P. Laud, Combining differential privacy and secure multiparty computation, in: Proceedings of the 31st Annual Computer Security Applications Conference, 2015, pp. 421–430.
[86] S. S. Ahila, K. Shunmuganathan, Role of agent technology in web usage mining: homomorphic encryption based recommendation for e-commerce applications, Wireless Personal Communications 87 (2) (2016) 499–512.
[87] J. Wang, J. Chao, Q. Tang, Z. Liu, A. M. M. Khin, Cryptorec: Novel collaborative filtering recommender made privacy-preserving easy, IEEE Transactions on Dependable and Secure Computing (01) (2021) 1–1.
[88] M. Zhang, Y. Chen, J. Lin, A privacy-preserving optimization of neighbourhood-based recommendation for medical-aided diagnosis and treatment, IEEE Internet of Things Journal (2021).
[89] J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, V. Shmatikov, " you might also like:" privacy risks of collaborative filtering, in: 2011 IEEE symposium on security and privacy, IEEE, 2011, pp. 231–246.
[90] V. Nikolaenko, S. Ioannidis, U. Weinsberg, M. Joye, N. Taft, D. Boneh, Privacy-preserving matrix factorization, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 801–812.
[91] J. Bobadilla, F. Ortega, A. Hernando, A. Gutiérrez, Recommender systems survey, Knowledge-based systems 46 (2013) 109–132.
[92] H. Hu, G. Dobbie, Z. Salcic, M. Liu, J. Zhang, L. Lyu, X. Zhang, Differentially private locality sensitive hashing based federated recommender system, Concurrency and Computation: Practice and Experience (2021) e6233.
[93] Z. Chen, Y. Wang, S. Zhang, H. Zhong, L. Chen, Differentially private user-based collaborative filtering recommendation based on k-means clustering, Expert Systems with Applications 168 (2021) 114366.
[94] T. Zhu, Y. Ren, W. Zhou, J. Rong, P. Xiong, An effective privacy preserving algorithm for neighborhood-based collaborative filtering, Future Generation Computer Systems 36 (2014) 142–155.
[95] S. Badsha, X. Yi, I. Khalil, A practical privacy-preserving recommender system, Data Science and Engineering 1 (3) (2016) 161–177.
[96] H. Shin, S. Kim, J. Shin, X. Xiao, Privacy enhanced matrix factorization for recommendation with local differential privacy, IEEE Transactions on Knowledge and Data Engineering 30 (9) (2018) 1770–1782.
[97] A. Berlioz, A. Friedman, M. A. Kaafar, R. Boreli, S. Berkovsky, Applying differential privacy to matrix factorization, in: Proceedings of the 9th ACM Conference on Recommender Systems, 2015, pp. 107–114.
[98] S. Kim, J. Kim, D. Koo, Y. Kim, H. Yoon, J. Shin, Efficient privacy-preserving matrix factorization via fully homomorphic encryption, in: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, 2016, pp. 617–628.
[99] W. House, Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy, White House, Washington, DC (2012) 1–62.
[100] N. Helberger, K. Karppinen, L. DÃćâĆňâĎćacunto, Exposure diversity as a design principle for recommender systems, Information, Communication & Society 21 (2) (2018) 191–207.
[101] M. P. O'Mahony, N. J. Hurley, G. C. Silvestre, Recommender systems: Attack types and strategies, in: AAAI, 2005, pp. 334–339.
[102] I. Gunes, C. Kaleli, A. Bilge, H. Polat, Shilling attacks against recommender systems: a comprehensive survey, Artificial Intelligence Review 42 (4) (2014) 767–799.
[103] N. Hurley, Z. Cheng, M. Zhang, Statistical attack detection, in: Proceedings of the third ACM conference on Recommender systems, 2009, pp. 149–156.
[104] M. P. OÃćâĆňâĎćMahony, N. J. Hurley, G. C. Silvestre, Towards robust collaborative filtering, in: Irish Conference on Artificial Intelligence

and Cognitive Science, Springer, 2002, pp. 87–94.
[105] S. K. Lam, J. Riedl, Shilling recommender systems for fun and profit, in: Proceedings of the 13th international conference on World Wide Web, 2004, pp. 393–402.
[106] R. Burke, B. Mobasher, R. Bhaumik, C. Williams, Segment-based injection attacks against collaborative filtering recommender systems, in: Fifth IEEE International Conference on Data Mining (ICDM'05), IEEE, 2005, pp. 4–pp.
[107] S. Rani, M. Kaur, M. Kumar, V. Ravi, U. Ghosh, J. R. Mohanty, Detection of shilling attack in recommender system for youtube video statistics using machine learning techniques, Soft Computing (2021) 1–13.
[108] H. Cai, F. Zhang, An unsupervised method for detecting shilling attacks in recommender systems by mining item relationship and identifying target items, The Computer Journal 62 (4) (2019) 579–597.
[109] R. Bhaumik, C. Williams, B. Mobasher, R. Burke, Securing collaborative filtering against malicious attacks through anomaly detection, in: Proceedings of the 4th workshop on intelligent techniques for web personalization (ITWPĂćâĆňâĎć06), Boston, Vol. 6, 2006, p. 10.
[110] Y. Hao, P. Zhang, F. Zhang, Multiview ensemble method for detecting shilling attacks in collaborative recommender systems, Security and Communication Networks 2018 (2018).
[111] C. Tong, X. Yin, J. Li, T. Zhu, R. Lv, L. Sun, J. J. Rodrigues, A shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network, The Computer Journal 61 (7) (2018) 949–958.
[112] M. P. OĂćâĆňâĎćMahony, N. J. Hurley, G. C. Silvestre, Promoting recommendations: An attack on collaborative filtering, in: International Conference on Database and Expert Systems Applications, Springer, 2002, pp. 494–503.
[113] M. P. O'Mahony, N. J. Hurley, G. C. Silvestre, Detecting noise in recommender system databases, in: Proceedings of the 11th international conference on Intelligent user interfaces, 2006, pp. 109–115.
[114] J. Cao, Z. Wu, B. Mao, Y. Zhang, Shilling attack detection utilizing semi-supervised learning method for collaborative recommender system, World Wide Web 16 (5-6) (2013) 729–748.
[115] M. Si, Q. Li, Shilling attacks against collaborative recommender systems: a review, Artificial Intelligence Review 53 (1) (2020) 291–319.
[116] M. O'Mahony, N. Hurley, N. Kushmerick, G. Silvestre, Collaborative recommendation: A robustness analysis, ACM Transactions on Internet Technology (TOIT) 4 (4) (2004) 344–377.
[117] R. Burke, B. Mobasher, C. Williams, R. Bhaumik, Classification features for attack detection in collaborative recommender systems, in: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, 2006, pp. 542–547.
[118] R. Burke, B. Mobasher, R. Bhaumik, Limited knowledge shilling attacks in collaborative filtering systems, in: Proceedings of 3rd international workshop on intelligent techniques for web personalization (ITWP 2005), 19th international joint conference on artificial intelligence (IJCAI 2005), 2005, pp. 17–24.
[119] R. Burke, B. Mobasher, R. Zabicki, R. Bhaumik, Identifying attack models for secure recommendation, Beyond Personalization 2005 (2005).
[120] C. Li, Z. Luo, Detection of shilling attacks in collaborative filtering recommender systems, in: 2011 International Conference of Soft Computing and Pattern Recognition (SoCPaR), IEEE, 2011, pp. 190–193.
[121] Z. Zhang, S. R. Kulkarni, Detection of shilling attacks in recommender systems via spectral clustering, in: 17th International Conference on Information Fusion (FUSION), IEEE, 2014, pp. 1–8.
[122] I. Gunes, A. Bilge, H. Polat, Shilling attacks against memory-based privacy-preserving recommendation algorithms, KSII Transactions on Internet and Information Systems (TIIS) 7 (5) (2013) 1272–1290.
[123] B. Mobasher, R. Burke, R. Bhaumik, C. Williams, Toward trustworthy recommender systems: An analysis of attack models and algorithm robustness, ACM Transactions on Internet Technology (TOIT) 7 (4) (2007) 23–es.
[124] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus, Intriguing properties of neural networks, arXiv preprint arXiv:1312.6199 (2013).
[125] J. Wang, L. Yu, W. Zhang, Y. Gong, Y. Xu, B. Wang, P. Zhang, D. Zhang, Irgan: A minimax game for unifying generative and discriminative information retrieval models, in: Proceedings of the 40th International ACM SIGIR conference on Research and Development in Information Retrieval, 2017, pp. 515–524.
[126] Y. Deldjoo, T. Di Noia, F. A. Merra, Adversarial machine learning in recommender systems (aml-recsys), in: Proceedings of the 13th International Conference on Web Search and Data Mining, 2020, pp. 869–872.
[127] Y. Cao, X. Chen, L. Yao, X. Wang, W. E. Zhang, Adversarial attacks and detection on reinforcement learning-based interactive recommender systems, in: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 2020, pp. 1669–1672.
[128] K. Christakopoulou, A. Banerjee, Adversarial attacks on an oblivious recommender, in: Proceedings of the 13th ACM Conference on Recommender Systems, 2019, pp. 322–330.
[129] C. Lin, S. Chen, H. Li, Y. Xiao, L. Li, Q. Yang, Attacking recommender systems with augmented user profiles, in: Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 2020, pp. 855–864.
[130] R. He, J. McAuley, Vbpr: visual bayesian personalized ranking from implicit feedback, in: Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 30, 2016.
[131] T. Di Noia, D. Malitesta, F. A. Merra, Taamr: Targeted adversarial attack against multimedia recommender systems, in: 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), IEEE, 2020, pp. 1–8.
[132] V. W. Anelli, A. Bellogín, Y. Deldjoo, T. Di Noia, F. A. Merra, Multi-step adversarial perturbations on recommender systems embeddings, arXiv preprint arXiv:2010.01329 (2020).
[133] J. Tang, H. Wen, K. Wang, Revisiting adversarially learned injection attacks against recommender systems, in: Fourteenth ACM Conference on Recommender Systems, 2020, pp. 318–327.
[134] B. Li, Y. Wang, A. Singh, Y. Vorobeychik, Data poisoning attacks on factorization-based collaborative filtering, arXiv preprint arXiv:1608.08182 (2016).
[135] M. Fang, G. Yang, N. Z. Gong, J. Liu, Poisoning attacks to graph-based recommender systems, in: Proceedings of the 34th Annual Computer Security Applications Conference, 2018, pp. 381–392.

[136] R. Hu, Y. Guo, M. Pan, Y. Gong, Targeted poisoning attacks on social recommender systems, in: 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, 2019, pp. 1–6.
[137] M. Fang, N. Z. Gong, J. Liu, Influence function based data poisoning attacks to top-n recommender systems, in: Proceedings of The Web Conference 2020, 2020, pp. 3019–3025.
[138] H. Huang, J. Mu, N. Z. Gong, Q. Li, B. Liu, M. Xu, Data poisoning attacks to deep learning based recommender systems, arXiv preprint arXiv:2101.02644 (2021).
[139] M. Welling, Y. W. Teh, Bayesian learning via stochastic gradient langevin dynamics, in: Proceedings of the 28th international conference on machine learning (ICML-11), Citeseer, 2011, pp. 681–688.
[140] Y. Zhang, J. Lou, L. Chen, X. Yuan, J. Li, T. Johnsten, N.-F. Tzeng, Towards poisoning the neural collaborative filtering-based recommender systems, in: European Symposium on Research in Computer Security, Springer, 2020, pp. 461–479.
[141] L. Chen, Y. Xu, F. Xie, M. Huang, Z. Zheng, Data poisoning attacks on neighborhood-based recommender systems, Transactions on Emerging Telecommunications Technologies (2020) e3872.
[142] S. Wadhwa, S. Agrawal, H. Chaudhari, D. Sharma, K. Achan, Data poisoning attacks against differentially private recommender systems, in: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 2020, pp. 1617–1620.
[143] J. Song, Z. Li, Z. Hu, Y. Wu, Z. Li, J. Li, J. Gao, Poisonrec: an adaptive data poisoning framework for attacking black-box recommender systems, in: 2020 IEEE 36th International Conference on Data Engineering (ICDE), IEEE, 2020, pp. 157–168.
[144] S. Shen, S. Tople, P. Saxena, Auror: Defending against poisoning attacks in collaborative deep learning systems, in: Proceedings of the 32nd Annual Conference on Computer Security Applications, 2016, pp. 508–519.
[145] W. Meng, X. Xing, A. Sheth, U. Weinsberg, W. Lee, Your online interests: Pwned! a pollution attack against targeted advertising, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 129–140.
[146] X. Xing, W. Meng, D. Doozan, A. C. Snoeren, N. Feamster, W. Lee, Take this personally: Pollution attacks on personalized services, in: 22nd {USENIX} Security Symposium ({USENIX} Security 13), 2013, pp. 671–686.
[147] G. Yang, N. Z. Gong, Y. Cai, Fake co-visitation injection attacks to recommender systems., in: NDSS, 2017.
[148] Z. Yang, Q. Sun, Y. Zhang, W. Wang, Identification of malicious injection attacks in dense rating and co-visitation behaviors, IEEE Transactions on Information Forensics and Security 16 (2020) 537–552.
[149] Z. Yang, Q. Sun, Y. Zhang, L. Zhu, W. Ji, Inference of suspicious co-visitation and co-rating behaviors and abnormality forensics for recommender systems, IEEE Transactions on Information Forensics and Security 15 (2020) 2766–2781.
[150] J. Davidson, B. Liebald, J. Liu, P. Nandy, T. Van Vleet, U. Gargi, S. Gupta, Y. He, M. Lambert, B. Livingston, et al., The youtube video recommendation system, in: Proceedings of the fourth ACM conference on Recommender systems, 2010, pp. 293–296.
[151] B. Mehta, W. Nejdl, Unsupervised strategies for shilling detection and robust collaborative filtering, User Modeling and User-Adapted Interaction 19 (1-2) (2009) 65–97.
[152] R. Burke, B. Mobasher, C. Williams, R. Bhaumik, Detecting profile injection attacks in collaborative recommender systems, in: The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), IEEE, 2006, pp. 23–23.
[153] C. A. Williams, B. Mobasher, R. Burke, Defending recommender systems: detection of profile injection attacks, Service Oriented Computing and Applications 1 (3) (2007) 157–170.
[154] F. Rezaimehr, C. Dadkhah, A survey of attack detection approaches in collaborative filtering recommender systems, Artificial Intelligence Review 54 (3) (2021) 2011–2066.
[155] F. Zhang, Reverse bandwagon profile inject attack against recommender systems, in: 2009 second international symposium on Computational Intelligence and Design, Vol. 1, IEEE, 2009, pp. 15–18.
[156] F. Zhang, Analysis of love-hate shilling attack against e-commerce recommender system, in: 2010 International Conference of Information Science and Management Engineering, Vol. 1, IEEE, 2010, pp. 318–321.
[157] S. S. Sohail, J. Siddiqui, R. Ali, Feature-based opinion mining approach (foma) for improved book recommendation, Arabian Journal for Science and Engineering 43 (12) (2018) 8029–8048.
[158] R. A. Zayed, L. F. Ibrahim, H. A. Hefny, H. A. Salman, Shilling attacks detection in collaborative recommender system: Challenges and promise, in: Workshops of the International Conference on Advanced Information Networking and Applications, Springer, 2020, pp. 429–439.
[159] K. Bryan, M. O'Mahony, P. Cunningham, Unsupervised retrieval of attack profiles in collaborative recommender systems, in: Proceedings of the 2008 ACM conference on Recommender systems, 2008, pp. 155–162.
[160] H. Cai, F. Zhang, Detecting shilling attacks in recommender systems based on analysis of user rating behavior, Knowledge-Based Systems 177 (2019) 22–43.
[161] V. W. Anelli, Y. Deldjoo, T. Di Noia, E. Di Sciascio, F. A. Merra, Sasha: Semantic-aware shilling attacks on recommender systems exploiting knowledge graphs, in: European Semantic Web Conference, Springer, 2020, pp. 307–323.
[162] P.-A. Chirita, W. Nejdl, C. Zamfir, Preventing shilling attacks in online recommender systems, in: Proceedings of the 7th annual ACM international workshop on Web information and data management, 2005, pp. 67–74.
[163] Y. Hao, F. Zhang, J. Wang, Q. Zhao, J. Cao, Detecting shilling attacks with automatic features from multiple views, Security and Communication Networks 2019 (2019).
[164] Y. Deldjoo, T. DI NOIA, F. A. MERRA, A survey on adversarial recommender systems: from attack/defense strategies to generative adversarial networks, ACM Comput. Surv. (2020).
[165] S. Corbett-Davies, S. Goel, The measure and mismeasure of fairness: A critical review of fair machine learning, arXiv preprint arXiv:1808.00023 (2018).
[166] M. D. Ekstrand, R. Joshaghani, H. Mehrpouyan, Privacy for all: Ensuring fair and equitable privacy protections, in: Conference on Fairness, Accountability and Transparency, PMLR, 2018, pp. 35–47.
[167] R. Burke, N. Sonboli, M. Mansoury, A. Ordoñez-Gauger, Balanced neighborhoods for fairness-aware collaborative recommendation (2017).

[168] S. Yao, B. Huang, Beyond parity: Fairness objectives for collaborative filtering, arXiv preprint arXiv:1705.08804 (2017).
[169] S. Broad, M. McGee, Recruiting women into computer science and information systems., Association Supporting Computer Users in Education (2014).
[170] L. Zhang, X. Wu, Anti-discrimination learning: a causal modeling-based framework, International Journal of Data Science and Analytics 4 (1) (2017) 1–16.
[171] F. Z. Borgesius, J. Poort, Online price discrimination and eu data privacy law, Journal of consumer policy 40 (3) (2017) 347–366.
[172] J. Miklos-Thal, G. Shaffer, Pass-through as an economic tool: On exogenous competition, social incidence, and price discrimination, Journal of Political Economy 129 (1) (2021) 000–000.
[173] S. Milano, M. Taddeo, L. Floridi, Recommender systems and their ethical challenges, AI & SOCIETY 35 (4) (2020) 957–967.
[174] S. S. Sohail, J. Siddiqui, R. Ali, Book recommendation system using opinion mining technique, in: 2013 international conference on advances in computing, communications and informatics (ICACCI), IEEE, 2013, pp. 1609–1614.
[175] R. Baeza-Yates, Bias on the web, Communications of the ACM 61 (6) (2018) 54–61.
[176] H. Abdollahpouri, Popularity bias in ranking and recommendation, in: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, 2019, pp. 529–530.
[177] H. Abdollahpouri, M. Mansoury, R. Burke, B. Mobasher, The unfairness of popularity bias in recommendation, arXiv preprint arXiv:1907.13286 (2019).
[178] A. Collins, D. Tkaczyk, A. Aizawa, J. Beel, Position bias in recommender systems for digital libraries, in: International Conference on Information, Springer, 2018, pp. 335–344.
[179] H. Steck, Training and testing of recommender systems on data missing not at random, in: Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining, 2010, pp. 713–722.
[180] K. Mohan, J. Pearl, Graphical models for processing missing data, Journal of the American Statistical Association (2021) 1–42.
[181] C. Dellarocas, C. A. Wood, The sound of silence in online feedback: Estimating trading risks in the presence of reporting bias, Management science 54 (3) (2008) 460–476.
[182] B. Marlin, R. S. Zemel, S. Roweis, M. Slaney, Collaborative filtering and the missing at random assumption, arXiv preprint arXiv:1206.5267 (2012).
[183] S. Piramuthu, G. Kapoor, W. Zhou, S. Mauw, Input online review data and related bias in recommender systems, Decision Support Systems 53 (3) (2012) 418–424.
[184] M. D. Ekstrand, M. Tian, I. M. Azpiazu, J. D. Ekstrand, O. Anuyah, D. McNeill, M. S. Pera, All the cool kids, how do they fit in?: Popularity and demographic biases in recommender evaluation and effectiveness, in: Conference on Fairness, Accountability and Transparency, PMLR, 2018, pp. 172–186.
[185] G. Adomavicius, J. C. Bockstedt, S. P. Curley, J. Zhang, Do recommender systems manipulate consumer preferences? a study of anchoring effects, Information Systems Research 24 (4) (2013) 956–975.
[186] S. Khenissi, O. Nasraoui, Modeling and counteracting exposure bias in recommender systems, arXiv preprint arXiv:2001.04832 (2020).
[187] R. Baeza-Yates, Bias in search and recommender systems, in: Fourteenth ACM Conference on Recommender Systems, 2020, pp. 2–2.
[188] J. Lu, D. Li, Bias correction in a small sample from big data, IEEE Transactions on Knowledge and Data Engineering 25 (11) (2012) 2658–2663.
[189] E. Pariser, The filter bubble: What the Internet is hiding from you, Penguin UK, 2011.
[190] A. Bruns, Filter bubble, Internet Policy Review 8 (4) (2019).
[191] F. Zuiderveen Borgesius, D. Trilling, J. Möller, B. Bodó, C. H. De Vreese, N. Helberger, Should we worry about filter bubbles?, Internet Policy Review. Journal on Internet Regulation 5 (1) (2016).
[192] F. Masrour, T. Wilson, H. Yan, P.-N. Tan, A. Esfahanian, Bursting the filter bubble: Fairness-aware network link prediction, in: Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 34, 2020, pp. 841–848.
[193] M. Haim, A. Graefe, H.-B. Brosius, Burst of the filter bubble? effects of personalization on the diversity of google news, Digital journalism 6 (3) (2018) 330–343.
[194] S. Flaxman, S. Goel, J. M. Rao, Filter bubbles, echo chambers, and online news consumption, Public opinion quarterly 80 (S1) (2016) 298–320.
[195] A. Polonioli, The ethics of scientific recommender systems, Scientometrics 126 (2) (2021) 1841–1848.
[196] J. Shokeen, C. Rana, A trust and semantic based approach for social recommendation, Journal of Ambient Intelligence and Humanized Computing (2021) 1–15.
[197] P. Massa, B. Bhattacharjee, Using trust in recommender systems: an experimental analysis, in: International conference on trust management, Springer, 2004, pp. 221–235.
[198] P. Massa, P. Avesani, Trust-aware collaborative filtering for recommender systems, in: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", Springer, 2004, pp. 492–508.
[199] R. Andersen, C. Borgs, J. Chayes, U. Feige, A. Flaxman, A. Kalai, V. Mirrokni, M. Tennenholtz, Trust-based recommendation systems: an axiomatic approach, in: Proceedings of the 17th international conference on World Wide Web, 2008, pp. 199–208.
[200] F. E. Walter, S. Battiston, F. Schweitzer, A model of a trust-based recommendation system on a social network, Autonomous Agents and Multi-Agent Systems 16 (1) (2008) 57–74.
[201] B. Yang, Y. Lei, J. Liu, W. Li, Social collaborative filtering by trust, IEEE transactions on pattern analysis and machine intelligence 39 (8) (2016) 1633–1647.
[202] H. Polat, W. Du, Privacy-preserving top-n recommendation on distributed data, Journal of the American Society for Information Science and Technology 59 (7) (2008) 1093–1108.
[203] G. Farnadi, P. Kouki, S. K. Thompson, S. Srinivasan, L. Getoor, A fairness-aware hybrid recommender system, arXiv preprint arXiv:1809.09030 (2018).
[204] Y. Ge, S. Zhao, H. Zhou, C. Pei, F. Sun, W. Ou, Y. Zhang, Understanding echo chambers in e-commerce recommender systems, in: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 2020, pp. 2261–

2270.
[205] Y. Zhang, H. Abbas, Y. Sun, Smart e-commerce integration with recommender systems, Electronic Markets 29 (2) (2019) 219–220.
[206] R. M. Frey, D. Vuckovac, A. Ilic, A secure shopping experience based on blockchain and beacon technology., in: RecSys Posters, 2016.
[207] Y. Zhang, J. Xiao, S. Hao, H. Wang, S. Zhu, S. Jajodia, Understanding the manipulation on recommender systems through web injection, IEEE Transactions on Information Forensics and Security 15 (2019) 3807–3818.
[208] Z. Liu, Z. Li, A blockchain-based framework of cross-border e-commerce supply chain, International Journal of Information Management 52 (2020) 102059.
[209] J. R. Shaikh, M. Nenova, G. Iliev, Z. Valkova-Jarvis, Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained e-commerce applications, in: 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), IEEE, 2017, pp. 1–4.
[210] Y. Han, Z. Han, J. Wu, Y. Yu, S. Gao, D. Hua, A. Yang, Artificial intelligence recommendation system of cancer rehabilitation scheme based on iot technology, IEEE Access 8 (2020) 44924–44935.
[211] C. C. Yang, L. Jiang, Enriching user experience in online health communities through thread recommendations and heterogeneous information network mining, IEEE Transactions on Computational Social Systems 5 (4) (2018) 1049–1060.
[212] H. Wen, J. Song, X. Pan, Physician recommendation on healthcare appointment platforms considering patient choice, IEEE Transactions on Automation Science and Engineering 17 (2) (2019) 886–899.
[213] X. Zhou, W. Liang, I. Kevin, K. Wang, S. Shimizu, Multi-modality behavioral influence analysis for personalized recommendations in health social media environment, IEEE Transactions on Computational Social Systems 6 (5) (2019) 888–897.
[214] L. Burbach, P. Belavadi, P. Halbach, N. Plettenberg, J. Nakayama, L. Kojan, A. C. Valdez, On the importance of context: Privacy perceptions of general vs. health-specific data in health recommender systems, in: Conference on Recommender Systems (HealthRecSysĂćâĆňâĎć 20), 2020.
[215] C. Xu, J. Wang, L. Zhu, C. Zhang, K. Sharif, Ppmr: a privacy-preserving online medical service recommendation scheme in ehealthcare system, IEEE Internet of Things Journal 6 (3) (2019) 5665–5673.
[216] A. Vadavalli, R. Subhashini, An improved differential privacy-preserving truth discovery approach in healthcare, in: 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, 2019, pp. 1031–1037.
[217] S. Zhang, X. Li, Z. Tan, T. Peng, G. Wang, A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services, Future Generation Computer Systems 94 (2019) 40–50.
[218] J. A. Onesimu, J. Karthikeyan, Y. Sei, An efficient clustering-based anonymization scheme for privacy-preserving data collection in iot based healthcare services, Peer-to-Peer Networking and Applications 14 (3) (2021) 1629–1649.
[219] T. M. Selvi, V. Kavitha, A privacy-aware deep learning framework for health recommendation system on analysis of big data, The Visual Computer (2021) 1–19.
[220] F. Alsubaei, A. Abuhussein, S. Shiva, Ontology-based security recommendation for the internet of medical things, IEEE Access 7 (2019) 48948–48960.
[221] A. Alsalemi, Y. Himeur, F. Bensaali, A. Amira, C. Sardianos, I. Varlamis, G. Dimitrakopoulos, Achieving domestic energy efficiency using micro-moments and intelligent recommendations, IEEE Access 8 (2020) 15047–15055.
[222] C. Sardianos, I. Varlamis, G. Dimitrakopoulos, D. Anagnostopoulos, A. Alsalemi, F. Bensaali, Y. Himeur, A. Amira, Rehab-c: Recommendations for energy habits change, Future Generation Computer Systems 112 (2020) 394–407.
[223] C. Sardianos, I. Varlamis, C. Chronis, G. Dimitrakopoulos, A. Alsalemi, Y. Himeur, F. Bensaali, A. Amira, The emergence of explainability of intelligent systems: Delivering explainable and personalized recommendations for energy efficiency, International Journal of Intelligent Systems 36 (2) (2021) 656–680.
[224] Q. Li, J. Kim, A deep learning-based course recommender system for sustainable development in education, Applied Sciences 11 (19) (2021) 8993.
[225] P. V. Kulkarni, S. Rai, R. Kale, Recommender system in elearning: a survey, in: Proceeding of International Conference on Computational Science and Applications, Springer, 2020, pp. 119–126.
[226] S. Benhamdi, A. Babouri, R. Chiky, Personalized recommender system for e-learning environment, Education and Information Technologies 22 (4) (2017) 1455–1477.
[227] P. Wang, Iot service recommendation scheme based on matter diffusion, IEEE Access 8 (2020) 51500–51509.
[228] A. Yang, Y. Zhansu, Y. Shi, H. Liu, Y. Chen, R. Li, Iot system for pellet proportioning based on bas intelligent recommendation model, IEEE Transactions on Industrial Informatics 17 (2) (2019) 934–942.
[229] Z. Cui, X. Xu, X. Fei, X. Cai, Y. Cao, W. Zhang, J. Chen, Personalized recommendation system based on collaborative filtering for iot scenarios, IEEE Transactions on Services Computing 13 (4) (2020) 685–695.
[230] L. Hu, G. Wu, Y. Xing, F. Wang, Things2vec: Semantic modeling in the internet of things with graph representation learning, IEEE Internet of Things Journal 7 (3) (2019) 1939–1948.
[231] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, A. Sahafi, Trust-based recommendation systems in internet of things: a systematic literature review, Human-centric Computing and Information Sciences 9 (1) (2019) 1–61.
[232] W. Lin, X. Zhang, L. Qi, W. Li, S. Li, V. S. Sheng, S. Nepal, Location-aware service recommendations with privacy-preservation in the internet of things, IEEE Transactions on Computational Social Systems (2020).
[233] P. Bahirat, Y. He, A. Menon, B. Knijnenburg, A data-driven approach to developing iot privacy-setting interfaces, in: 23rd International Conference on Intelligent User Interfaces, 2018, pp. 165–176.
[234] Z. Huang, X. Xu, J. Ni, H. Zhu, C. Wang, Multimodal representation learning for recommendation in internet of things, IEEE Internet of Things Journal 6 (6) (2019) 10675–10685.
[235] A. Khelloufi, H. Ning, S. Dhelim, T. Qiu, J. Ma, R. Huang, L. Atzori, A social relationships based service recommendation system for siot devices, IEEE Internet of Things Journal (2020).
[236] Y. Chen, M. Zhou, Z. Zheng, D. Chen, Time-aware smart object recommendation in social internet of things, IEEE Internet of Things Journal 7 (3) (2019) 2014–2027.

[237] M. Eirinaki, J. Gao, I. Varlamis, K. Tserpes, Recommender systems for large-scale social networks: A review of challenges and solutions (2018).
[238] S. Puglisi, J. Parra-Arnau, J. Forné, D. Rebollo-Monedero, On content-based recommendation and user privacy in social-tagging systems, Computer Standards & Interfaces 41 (2015) 17–27.
[239] T. B. Ogunseyi, T. Bo, C. Yang, A privacy-preserving framework for cross-domain recommender systems, Computers & Electrical Engineering 93 (2021) 107213.
[240] C. Gao, C. Huang, Y. Yu, H. Wang, Y. Li, D. Jin, Privacy-preserving cross-domain location recommendation, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3 (1) (2019) 1–21.
[241] Y. Xin, et al., Challenges in recommender systems: scalability, privacy, and structured recommendations, Ph.D. thesis, Massachusetts Institute of Technology (2015).
[242] A. Baldominos, Y. Saez, E. Albacete, I. Marrero, An efficient and scalable recommender system for the smart web, in: 2015 11th International Conference on Innovations in Information Technology (IIT), IEEE, 2015, pp. 296–301.
[243] H. Samin, T. Azim, Knowledge based recommender system for academia using machine learning: A case study on higher education landscape of pakistan, IEEE Access 7 (2019) 67081–67093.
[244] M. Qamhieh, H. Sammaneh, M. N. Demaidi, Pcrs: Personalized career-path recommender system for engineering students, IEEE Access 8 (2020) 214039–214049.
[245] S. Banihashemi, J. Li, A. Abhari, Scalable machine learning algorithms for a twitter followee recommender system, in: 2019 Spring Simulation Conference (SpringSim), IEEE, 2019, pp. 1–8.
[246] X. Zhao, A study on e-commerce recommender system based on big data, in: 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), IEEE, 2019, pp. 222–226.
[247] N. S. Nizamkari, A graph-based trust-enhanced recommender system for service selection in iot, in: 2017 International Conference on Inventive Systems and Control (ICISC), IEEE, 2017, pp. 1–5.
[248] S. Taheri, I. Irajian, Deepmovrs: a unified framework for deep learning-based movie recommender systems, in: 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), IEEE, 2018, pp. 200–204.
[249] A. M. Jorge, J. Vinagre, M. Domingues, J. Gama, C. Soares, P. Matuszyk, M. Spiliopoulou, Scalable online top-n recommender systems, in: International Conference on Electronic Commerce and Web Technologies, Springer, 2016, pp. 3–20.
[250] D. Hyun, C. Park, M.-C. Yang, I. Song, J.-T. Lee, H. Yu, Review sentiment-guided scalable deep recommender system, in: The 41st international ACM SIGIR conference on research & development in information retrieval, 2018, pp. 965–968.
[251] P. Zhou, K. Wang, L. Guo, S. Gong, B. Zheng, A privacy-preserving distributed contextual federated online learning framework with big data support in social recommender systems, IEEE Transactions on Knowledge and Data Engineering (2019).
[252] B. V. Srivastava, S. Sharma, D. Datta, G. Sriram, S. Jambhulkar, S. Naik, G. J. Reddy, Genetic algorithm based parallel matrix factorization for recommender systems, in: 2016 International Conference on Information Technology (ICIT), IEEE, 2016, pp. 212–217.
[253] H. Li, K. Li, J. An, K. Li, Msgd: A novel matrix factorization approach for large-scale collaborative filtering recommender systems on gpus, IEEE Transactions on Parallel and Distributed Systems 29 (7) (2017) 1530–1544.
[254] X. Zhang, Z. Zhao, C. Li, Y. Zhang, J. Zhao, An interpretable and scalable recommendation method based on network embedding, IEEE Access 7 (2019) 9384–9394.
[255] B. Yi, X. Shen, H. Liu, Z. Zhang, W. Zhang, S. Liu, N. Xiong, Deep matrix factorization with implicit feedback embedding for recommendation system, IEEE Transactions on Industrial Informatics 15 (8) (2019) 4591–4601.
[256] H.-T. Cheng, L. Koc, J. Harmsen, T. Shaked, T. Chandra, H. Aradhye, G. Anderson, G. Corrado, W. Chai, M. Ispir, et al., Wide & deep learning for recommender systems, in: Proceedings of the 1st workshop on deep learning for recommender systems, 2016, pp. 7–10.
[257] H. Guo, R. Tang, Y. Ye, Z. Li, X. He, Deepfm: a factorization-machine based neural network for ctr prediction, arXiv preprint arXiv:1703.04247 (2017).
[258] J. Lian, X. Zhou, F. Zhang, Z. Chen, X. Xie, G. Sun, xdeepfm: Combining explicit and implicit feature interactions for recommender systems, in: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2018, pp. 1754–1763.
[259] A. Lisi, A. De Salve, P. Mori, L. Ricci, Practical application and evaluation of atomic swaps for blockchain-based recommender systems, in: 2020 the 3rd International Conference on Blockchain Technology and Applications, ICBTA 2020, Association for Computing Machinery, New York, NY, USA, 2020, p. 67ĂćâĆňâĂIJ74.
[260] Y. Abuidris, R. Kumar, W. Wenyong, A survey of blockchain based on e-voting systems, in: Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, 2019, pp. 99–104.
[261] F. Casino, C. Patsakis, An efficient blockchain-based privacy-preserving collaborative filtering architecture, IEEE Transactions on Engineering Management 67 (4) (2019) 1501–1513.
[262] Y. Zhang, X. Chen, Now Foundations and Trends, 2020.
[263] A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins, et al., Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai, Information Fusion 58 (2020) 82–115.
[264] A. Ghazimatin, O. Balalau, R. Saha Roy, G. Weikum, Prince: provider-side interpretability with counterfactual explanations in recommender systems, in: Proceedings of the 13th International Conference on Web Search and Data Mining, 2020, pp. 196–204.
[265] M. Naiseh, N. Jiang, J. Ma, R. Ali, Explainable recommendations in intelligent systems: delivery methods, modalities and risks, in: International Conference on Research Challenges in Information Science, Springer, 2020, pp. 212–228.
[266] Y. Himeur, A. Alsalemi, A. Al-Kababji, F. Bensaali, A. Amira, C. Sardianos, G. Dimitrakopoulos, I. Varlamis, A survey of recommender systems for energy efficiency in buildings: Principles, challenges and prospects, Information Fusion 72 (2021) 1–21.
[267] D. Gunning, Explainable artificial intelligence (xai), Defense Advanced Research Projects Agency (DARPA), nd Web 2 (2) (2017).
[268] D. Gunning, D. Aha, DarpaĂćâĆňâĎćs explainable artificial intelligence (xai) program, AI Magazine 40 (2) (2019) 44–58.
[269] L. Viganò, D. Magazzeni, Explainable security, in: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),

IEEE, 2020, pp. 293–300.
[270] D. L. Marino, C. S. Wickramasinghe, M. Manic, An adversarial approach for explainable ai in intrusion detection systems, in: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2018, pp. 3237–3243.
[271] A. K. Sarica, P. Angin, Explainable security in sdn-based iot networks, Sensors 20 (24) (2020) 7326.
[272] A. Kuppa, N.-A. Le-Khac, Black box attacks on explainable artificial intelligence (xai) methods in cyber security, in: 2020 International Joint Conference on Neural Networks (IJCNN), IEEE, 2020, pp. 1–8.
[273] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, J. Zhang, Edge intelligence: Paving the last mile of artificial intelligence with edge computing, Proceedings of the IEEE 107 (8) (2019) 1738–1762.
[274] R. Wang, Y. Liu, P. Zhang, X. Li, X. Kang, Edge and cloud collaborative entity recommendation method towards the iot search, Sensors 20 (7) (2020) 1918.
[275] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar, A. Y. Zomaya, Edge intelligence: the confluence of edge computing and artificial intelligence, IEEE Internet of Things Journal 7 (8) (2020) 7457–7469.
[276] Y. Gong, Z. Jiang, Y. Feng, B. Hu, K. Zhao, Q. Liu, W. Ou, Edgerec: Recommender system on edge in mobile taobao, in: Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 2020, pp. 2477–2484.
[277] C. Sun, H. Li, X. Li, J. Wen, Q. Xiong, W. Zhou, Convergence of recommender systems and edge computing: A comprehensive survey, IEEE Access 8 (2020) 47118–47132.
[278] A. M. Ghosh, K. Grolinger, Edge-cloud computing for internet of things data analytics: Embedding intelligence in the edge with deep learning, IEEE Transactions on Industrial Informatics 17 (3) (2020) 2191–2200.
[279] X. Su, G. Sperlì, V. Moscato, A. Picariello, C. Esposito, C. Choi, An edge intelligence empowered recommender system enabling cultural heritage applications, IEEE Transactions on Industrial Informatics 15 (7) (2019) 4266–4275.
[280] F. Lin, Y. Zhou, I. You, J. Lin, X. An, X. Lü, Content recommendation algorithm for intelligent navigator in fog computing based iot environment, IEEE Access 7 (2019) 53677–53686.
[281] X. Wang, B. Gu, Y. Ren, W. Ye, S. Yu, Y. Xiang, L. Gao, A fog-based recommender system, IEEE Internet of Things Journal 7 (2) (2019) 1048–1060.
[282] T. S. Ibrahim, A. I. Saleh, N. Elgaml, M. M. Abdelsalam, A fog based recommendation system for promoting the performance of e-learning environments, Computers & Electrical Engineering 87 (2020) 106791.
[283] X. Wang, B. Gu, Y. Qu, Y. Ren, Y. Xiang, L. Gao, A privacy preserving aggregation scheme for fog-based recommender system, in: International Conference on Network and System Security, Springer, 2020, pp. 408–418.

Biographical sketch

Dr. Yassine Himeur received the master's degree in electronic from the University of Science and Technology (USTHB), Algiers, Algeria, in 2011, and the Ph.D. degree from Jijel University, in 2015. He was a Senior Researcher, from 2013 to 2019, and the Head of TELECOM Division, from 2018 to 2019, at the Algerian Center for Development of Advanced Technologies (CDTA), Algiers (Algeria). He is currently a Postdoctoral Research Fellow in the Department of Electrical Engineering at Qatar University. He has authored over 50 research papers in refereed journals and international conference proceedings. He is the recipient of the Best Paper Award in the 11th International Conference on Signal Processing and Multimedia Applications SIGMAP 2014 (Austria) and Best student paper award at IEEE GPECOM 2020 conference (Turkey). His current research interests are artificial intelligence and deep learning, IoT, energy efficiency, recommender systems and multimedia security.

Dr. Shahab Saquib Sohail is currently working as an Assistant professor in the Department of Computer Science and Engineering, Jamia Hamdard (Deemed to be) University. He has completed his Doctoral thesis in Recommender Systems from AMU, Aligarh. He is working in the trust area of data mining, soft computing, affective computing, sentiment analysis and machine learning. He has published several articles in highly reputed journal from the publishers like Elsevier, Wiley, Springer, IEEE, etc. He is a TPC member of IEEE SMC society. He is the recipient of Hakeem Abdul Hameed Award.

Prof. Faycal Bensaali (S'03-M'06-SM'15) obtained a Dipl-Ing (M.Eng.) in electronics from University of Constantine and a Ph.D. in Electronic and Computer Engineering from Queen's University, Belfast. He is currently a Professor of Electrical Engineering at Qatar University. Prof. Bensaali took other academic positions at Queen's University Belfast-UK and the University of Hertfordshire-UK. His research interests are mainly in embedded systems and high performance computing, inteligent systems and connected health. Prof. Bensaali served as Guest Editor of IEEE IoT journal, Future Generation Computer Systems and Journal of Sensor and Actuator Networks. He has also acted as General Chair, Workshop Chair and TPC Member of a number of international conferences and workshops. He has authored/co-authored over 170 scientific papers in international journals and conference proceedings. He is an HEA Associate and IEEE senior member.

Prof. Abbes Amira received his Ph.D. in Computer Engineering in 2001 from Queen's University Belfast, United Kingdom. Since then, he has taken many academic and consultancy positions in the United Kingdom, Europe, Asia, and the Middleast. Between 2017 and 2019, he was the Associate Dean for research and graduate studies in the College of Engineering at Qatar University, Qatar. In the United Kingdom, he has taken academic and leadership positions at Queen's University Belfast, Brunel University London and the University of Ulster. Currently, he is the Dean College of Computing and Informatics University of Sharjah,UAE, previous to that, he was the Associate Dean of Research and Innovation in the School of Computer Science and Informatics at De Montfort University. During his career to date, Prof. Amira has been successful in securing substantial funding from government agencies and industry; he has supervised more than 25 PhD students and has over 300 publications in top journals and conferences in the area of embedded systems, IoT, image and signal processing. He has been invited to give keynote talks, short courses and tutorials at many universities and international conferences and has been chair and program

committee for several IEEE conferences including; tutorial and invited talks at the prestigious ICIP 2009, ICECS 2018, ICCV 2009, ISSPA 2012, ISSPIT 2015. He was the General CoChair of ECVW 2011, Program Chair of ECVW2010, Program Co-Chair of ICM12, DELTA 2008, IMVIP 2005 and General Co-Chair of ICM 2014. He is also a member of the IEEE Technical Committee for Biomedical Circuits and systems. His current research interests include embedded systems, high-performance computing, big data and IoT, connected health, image and vision systems, biometric and security.

Dr Mamoun Alazab is an Associate Professor at the College of Engineering, IT and Environment at Charles Darwin University, Australia. He received his PhD degree in Computer Science from the Federation University of Australia, School of Science, Information Technology and Engineering. He is a cyber security researcher and practitioner with industry and academic experience. Alazab's research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention. He has more than 150 research papers in many international journals and conferences, such as IEEE transactions on Industrial Informatics, IEEE Transactions on Industry Applications, IEEE Transactions on Big Data, IEEE Transactions on Vehicular Technology, Computers & Security, and Future Generation Computing Systems. He delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police (AFP), the Australian Communications and Media Authority (ACMA), Westpac, United Nations Office on Drugs and Crime (UNODC), and the Attorney General's Department. He is a Senior Member of the IEEE. He is the Founding chair of the IEEE Northern Territory (NT) Subsection.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: