Survey of Privacy-Preserving Collaborative Filtering

Islam Elnabarawy, *Student Member, IEEE,* Wei Jiang, *Member, IEEE,* and Donald C. Wunsch II, *Fellow, IEEE*

***Abstract*—Collaborative filtering recommendation systems provide recommendations to users based on their own past preferences, as well as those of other users who share similar interests. The use of recommendation systems has grown widely in recent years, helping people choose which movies to watch, books to read, and items to buy. However, users are often concerned about their privacy when using such systems, and many users are reluctant to provide accurate information to most online services. Privacy-preserving collaborative filtering recommendation systems aim to provide users with accurate recommendations while maintaining certain guarantees about the privacy of their data. This survey examines the recent literature in privacy-preserving collaborative filtering, providing a broad perspective of the field and classifying the key contributions in the literature using two different criteria: the type of vulnerability they address and the type of approach they use to solve it.**

***Index Terms*—privacy preserving, collaborative filtering, survey, recommendation system**

I. Introduction

The use of recommendation systems has grown significantly in recent years. Shopping websites present users with item recommendations based on their history and demographics; movie and book recommendation websites are being used every day to pick new favorites; and online music streaming services generate dynamic playlists to suit each user's preferences.

Collaborative filtering (CF) is a popular and successful approach to providing user recommendations using knowledge about the user's preferences and the preferences of other users with similar interests to predict which items the user is most likely to be interested in [1], [2]. There is a large body of literature on CF algorithms [1]–[12], which can be categorized into memory-based and model-based techniques [1], [2].

Since the key point in CF systems relies on users' preferences and past actions to make predictions, many users may feel uneasy because of privacy concerns [13], [14]. Additionally, the need may arise for two or more CF systems to leverage their combined data to provide their users with more accurate recommendations. This type of computation that relies on data from more than one party is referred to as multi-party computation [15]. To leverage this type of computation, the parties need to be able to do it securely, without allowing the other parties to read and store the user data. This is when privacy-preserving data mining techniques [16] become necessary, leading to many different algorithms for privacy-preserving CF (PPCF); e.g: [17]–[24].

This survey examines a large number of contributions to PPCF recommendation systems in published literature. It divides the papers into broad categories multiple times based on different factors, with the goal of providing a comprehensive overview of the recent literature in the field. This is a broad perspective that the authors believe to be missing from the recent PPCF literature. The remainder of this survey is organized as follows: Section II provides some background information on privacy-preserving data mining (Section II-A) and CF recommendation systems (Section II-B). Section III contains a survey of the recent PPCF literature, organized into subsections corresponding to the different classifications. Finally, Section IV concludes the survey with a summary of the researchers' observations after examining the recent literature.

I. Elnabarawy is with the Department of Computer Science, Missouri University of Science and Technology, Rolla, Missouri 65409. E-mail: elnabarawy@ieee.org

W. Jiang is with the Department of Electrical Engineering and Computer Science in the College of Engineering and the Management Department in the College of Business at the University of Missouri-Columbia, Columbia, Missouri 65211. E-mail: wjiang@missouri.edu

D. Wunsch is with the Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, Missouri 65409. E-mail: dwunsch@ieee.org.

I. Elnabarawy and D. Wunsch are affiliated with the Applied Computational Intelligence Laboratory, Missouri University of Science and Technology, Rolla, Missouri 65409. Website: acil.mst.edu

II. Background

A. Common Privacy-Preserving Techniques

- *Secure Multiparty Computation*
  To maximize privacy or minimize information disclosure, Secure Multiparty Computation (SMC) is the goto technique which was first introduced by Yao's Millionaire problem [25]. This was extended to multiparty computations by Goldreich et al. [26]. SMC can be categorized as either information theoretic or computational [27]. In the computational model, the adversary is assumed to be bounded by polynomial-time. In the information theoretic model, the adversary is assumed to be unbounded. Much work exists to address various aspects (e.g., complexity, adversarial behaviors, the number of corrupted parties) of SMC. There are generally two types of adversaries related to the SMC definitions: semi-honest and malicious [28]. The semi-honest adversarial model often leads to more efficient privacy-preserving protocols, but the malicious model is less restrictive and thus more realistic.
- *Randomization and Perturbation*
  The main idea in the perturbation approach is that data are modified (e.g., adding noise but preserving the underlying statistics) before being disclosed and analyzed. The key is that the original distribution can be roughly reconstructed from the perturbed data. The paper by Agrawal and Srikant [29] introduced this notion. In addition to additive noise, multiplicative noise can also be used [30].
- *k-Anonymity*
  The technique was developed to prevent external linking

attacks [31], [32]. The basic idea is that a dataset is k-anonymous if each record appears at least k times according to a pre-defined set of quasi-identifier attributes. The main approach to achieve k-anonymity is information generalization and suppression.

B. Collaborative Filtering

CF addresses the problem of finding the degree to which a given user would like an item based on the knowledge of what similar users thought of that item and other similar items [2]. It is primarily based on the assumption that users who share similar interests for a subset of items will share the same opinion for other items [1], [17].

In formal terms, the system is given a set of N items

$$\mathbb{X} = \{x_i : i \in 1, 2, ..., N\},$$

a set of M users

$$\mathbb{U} = \{u_j : j \in 1, 2, ..., M\},$$

and a set of ratings $r_{i,j}$, where $r_{i,j}$ corresponds with the rating that item x_i received from user u_j. Given a set of known ratings, CF attempts to find the predicted rating $\tilde{r}_{t,k}$ that user u_k is most likely to assign to item x_t.

The range of values for the ratings varies by domain. Some domains only consider the explicit ratings that the users make, either by assigning a rating to an item or by making a purchase through the system [9]. Other domains that lack access to this type of information often rely on other metrics, such as the number of user clicks on web pages and the relative time the user spends looking at a certain web page [4].

CF techniques face many challenges, such as dealing with sparse rating datasets and large volumes of user and item data. They are often required to generate recommendations in real-time or with near real-time requirements, and incorporate new ratings from users while the system is in operation. Additionally, rating data is often noisy and subjective, which may lead to inaccurate recommendations [2].

One of the main challenges for CF systems is maintaining the privacy of user information. Various attacks can be used on recommendation systems to expose the preferences and behavioral patterns of a specific user or identify a user within a particular dataset [33].

CF approaches can be classified into two categories; memory-based and model-based. There are also hybrid techniques that incorporate both the memory-based and model-based approaches [1], [2].

In memory-based CF techniques, a heuristic is used to make rating predictions based on some or all of the ratings that are already known [1], [2]. They often rely on identifying users that share similar interests with a given user, and use the known ratings of those users to make predictions about the preferences of the user.

Different memory-based CF approaches employ different measures to compute the similarity between users and how they make their predictions. For example, GroupLens, one of the early generation CF systems [11] used the Pearson correlation measure to find similar users, then made its prediction using an average of the ratings of similar users for the same item, weighted by the absolute value of the correlation between each of those users and the user in question.

Model-based CF techniques learn a model based on the known ratings, and use that model to predict how a user would rate a previously-unrated item [1], [2]. The learning system uses the training data to build a model that represents the patterns and relationships in the training data, and then it uses that model to make predictions about the preferences of the users in the system.

Model-based CF systems vary based on the type of data they are analyzing. For categorical ratings, classification-based algorithms are often used to build the CF model. Conversely, regression models are often used when the ratings are numerical or continuous. An example of some early work on model-based CF [3] used Bayesian models, where a probabilistic Bayesian network is built using the known ratings, and used later to predict the value for an unknown rating.

Hybrid CF techniques join multiple approaches to build a more flexible and robust recommendation system. They often rely on domain knowledge and heuristics to take advantage of multiple aspects of the problem and provide more accurate and personalized recommendations. They may rely on item content, user demographic information, or combine both memory-based and model-based approaches to build the CF system [2]. Some work in the literature, such as [4], joins both memory-based and model-based techniques into hybrid techniques. These aim at leveraging some details about the problem domain to build systems that bridge the gap between memory-based and model-based techniques, thus providing an added advantage in cases where a new user or item is being introduced to the system.

The interested reader is referred to [2] and [34], which provide surveys of the key developments to the different CF approaches as well as an evaluation of the advantages and disadvantages of each approach.

C. Related Studies

There have been some recent studies with similar goals that examined recent PPCF literature. In one of the more recent studies [35], the authors looked at the current trends in PPCF and considered possible future trends for the field. The study looks at other recent survey papers, examines their strengths and shortcomings and then classifies the recent papers in the field with respect to the trends common between them and the different aspects of the CF algorithms used. The authors provided an analysis of the number of publications in the field over the past two decades, and identified three main goals that they think future research should address simultaneously: privacy, accuracy and online performance.

The authors of [36] provided a comprehensive survey of the PPCF literature until 2013. They used several different attributes to classify the PPCF literature, including data partitioning cases and the techniques they used to preserve privacy, and presented guidelines and potential future directions for research in the PPCF field. It is one of the most comprehensive survey papers in recent years.

The study by [37] provides a thorough comparison between different clustering-based PPCF approaches. It evaluates the capabilities of recent literature in clustering-based CF in terms of privacy, and provides ways to apply different families of clustering algorithms to the CF problem while keeping the user information private.

In [13], the authors classify the recent PPCF literature into two categories based on the centrality of data. They consider centralized methods to be ones in which the data is stored in one central location and decentralized methods to be ones where the data is distributed between multiple parties, or where users maintain control of their own rating profile. They discuss the current trends based on their survey of the literature and list a number of current PPCF challenges as well as new ones that they anticipate.

Other recent studies include [38] and [39], which provide a more general examination of privacy in recommendation systems, as well as [40] and [41], which focus on one specific vulnerability known as shilling attacks.

III. Survey of Recent Work

Due to the popularity of CF systems, and the prevalence of privacy concerns among users and developers of CF recommendation systems, there have been many contributions to this area of the literature in recent years. The study presented here takes a different approach that was not found in recent surveys on PPCF. It examines and classifies the papers in the field multiple times into broad categories, based on different factors. First, it highlights the way authors of different papers defined privacy and identifies the problem each paper was trying to solve. Then, the papers were classified with respect to how they solved the general PPCF problem, breaking them up into multiple categories corresponding to the most commonly used approaches in the literature. This classification is meant to provide a broad perspective of the field and help researchers and practitioners interested in PPCF identify the approach that is best suited to their needs.

A. Vulnerability

Online CF recommendation systems can be subject to different vulnerabilities that compromise the privacy of the users' data and the overall integrity of the system. In this section, the recent PPCF literature is examined and the type of vulnerability that each study attempts to address is identified.

1) User Profile Exposure: Most of the recent PPCF literature attempts to address the general problem of user profile exposure by providing guarantees that the users' preferences remain private and are not exposed to other system users or system admins or being sold to marketing agencies. Table I cites examples from recent PPCF literature where the studies focused on solving this problem.

The definition of the profile exposure vulnerability often varies, but the common factor used to identify papers addressing this vulnerability is that they focus on protecting the user profile data before it is stored or transmitted, using obfuscation, microaggregation or cryptographic approaches. Sometimes the objective is to protect the data from semi-honest third parties, while other times it is providing the user with guarantees that their profile data is safe from prying eyes, even within the domain of the service providing the CF recommendations.

2) Inference Attacks: The second most popular problem addressed by PPCF literature is that of inference attacks. In this category, the main challenge is protecting against malicious system users who try to inject fake profiles into the system or collect a lot of recommendation data, with the goal of inferring or identifying profiles of other users in the system. This can apply to either a semi-honest or a malicious attack model, depending on the level of security guarantee that the system provides. In contrast with user profile exposure, the system can have access to the complete user profile data, and the objective is to prevent other parties or system users from inferring information about that data. Examples of this category are cited in Table I.

Studies that address vulnerability to inference attacks often rely on providing k-anonymity guarantees to user profiles such that a user profile cannot be identified within a group of k profiles. They may rely on data obfuscation or clustering approaches, as well as microaggregation, to provide these guarantees. This is a more challenging problem in the area of PPCF, where a trade-off may be necessary between the accuracy of the provided recommendations and the degree of anonymity that the system provides.

3) Shilling Attacks: Another popular vulnerability that PPCF studies attempt to address is shilling attacks. This is an attack in which a malicious entity can create a large number of fake profiles that have false ratings with the goal of influencing the system towards or away from recommending certain items. The last row of Table I cites examples of this type of study.

The study by [42] discusses the sensitivity of different CF schemes to shilling attacks, and suggests that clustering-based CF methods are more robust and can detect and exclude fake profiles. Although this vulnerability may not influence the privacy of user data directly, it can greatly bias a CF recommendation system and decrease its accuracy and usability significantly.

TABLE I
Papers divided by vulnerability

Type of Vulnerability	Papers
User Profile Exposure	[17]–[22], [36], [37], [43]–[100]
Inference Attacks	[14], [23], [24], [33], [101]–[119]
Shilling Attacks	[40]–[42], [120]–[125]

B. Approaches to Privacy

This survey's authors used their observations of the recent literature to divide the contributions into several categories below based on their approach to preserving privacy: cryptography-based, obfuscation-based, clustering-based, and heuristic-based techniques.

Cryptography-based techniques (III-B1) rely on using cryptography to secure the user data and often use homomorphic

encryption to allow computations to be applied to the data securely. Obfuscation-based techniques (III-B2), on the other hand, rely on applying transformations to the data to obfuscate or anonymize it, such that the individual users cannot be identified within the data or results. Clustering-based techniques (III-B3) use clustering to group users together into small communities, then extract features that are representative of this community as a whole, and use those to generate the recommendations. Therefore, this guarantees that no individual user's data will be identified. Finally, other techniques in the literature (III-B4) rely on alternate methods, such as generating recommendations based on items instead of users, to generate the recommendations without exposing the user data.

In the following subsections, some of the recent work is categorized in terms of the approach to preserving privacy, and some potential advantages and disadvantages to each type of approach are examined.

1) Cryptography-based techniques: Cryptography-based PPCF appears to be the most popular category in recent literature. Techniques in this group rely on cryptographic measures to carry out the calculations needed for providing recommendations securely, without compromising the privacy of the users' data. They are often used to prevent the user profile exposure vulnerability discussed earlier, which most commonly occurs under a semi-honest attack model.

One of the earlier contributions to this area was by Canny [18], [101]. In [18], a cryptographic algorithm for computing a public aggregate of the data was presented that can then be used to securely generate personalized recommendations for individuals. It uses homomorphic encryption to apply the CF calculations on the data and decrypt the results without exposing the individual users' data. The work in [101] extends the idea further by creating a method based on an Expectation Maximization probabilistic factor analysis model and using a privacy-preserving peer-to-peer homomorphic encryption protocol to apply the CF calculations. The interested reader is referred to [18] and [101] for a complete exposition of the approach summarized here.

In [17], the authors present an architecture for PPCF using the notion of distributed trust, which relies on a coalition of trusted servers instead of a single server. This distribution of trust among multiple servers makes the system more resilient against faults and attacks while providing an element of privacy for the users' data. The implementation of this architecture relies on a threshold homomorphic encryption protocol and was implemented and evaluated in an experimental setting.

The work presented in [19] attempts to address one of the drawbacks of cryptography-based techniques, which is the high computational overhead of encrypting and decrypting large amounts of data. In this contribution, the authors rely on clustering the items and sampling the user data to reduce the computational burden of the cryptographic protocol. The reduced data is then used in a homomorphic cryptography scheme to securely generate CF recommendations with a significant reduction in computational time. In [71], the authors continue to address the goal of improving the time performance of cryptographic PPCF by introducing a quasi-homomorphic similarity measure that allows the use of local similarities to approximate the global similarity and analyze the accuracy of this approximation approach in addition to its running time improvement.

The contributions in [22] and [52] discuss some important practical considerations for implementing CF on cloud platforms, privacy and security being among the chief concerns of implementing such systems. In [22], they present a practical implementation of a PPCF system, based on the Google App Engine for Java (GAE/J) cloud platform. They designed algorithms that rely on a homomorphic encryption scheme to preserve the privacy of user data in the cloud. This work is further analyzed and extended in [52] to address real world Software-as-a-service and Platform-as-a-service cloud settings.

Some of the more recent contributions addressed more specific concerns, such as horizontally-partitioned datasets [67], overlapped ratings [21], and updating the user preferences in real time [79]. Others, such as [94] and [91], designed cryptography-based PPCF algorithms for other tasks [94] or incorporated cryptographic methods with other approaches to create efficient PPCF systems [91].

While cryptography-based techniques have the advantage of providing reliable security without sacrificing the accuracy of their results, one of the main concerns for this family of techniques is the scalability to systems that require the processing of millions of items and users, especially in online settings where the response time needs to be minimal while providing accurate recommendations.

2) Obfuscation-based techniques: In obfuscation-based techniques, user profile data is transformed in some way that prevents individual users from being identified by using the data or the system's output, while maintaining the same or a close level of accuracy in the generated recommendations. This is often used to guard against inference attacks by other system users or external entities, following either a semi-honest or a malicious attack model.

The work introduced in [84] relies on randomized perturbation techniques to introduce randomness in the data such that a user could not be individually identified with any certainty. Similarly, [72] applies some randomness to the response provided by the system to prevent the preferences of individual users from being inferred from the system's responses while allowing the users to calculate the exact response using the randomized one.

Another popular approach in this category is based on the obfuscation of user data, and was examined by [20], [23], [118]. Similar to perturbation, the relevant fields in user data are obfuscated to mask any identifying information in the data, preventing anyone from inferring the original users' preferences and information based on the obfuscated data.

Anonymization schemes combine the two previous approaches by removing the identifying fields from the data, obfuscating the values in other fields, and adding randomness to the data all to guarantee a level of k-anonimity for each user in the dataset. Examples of this scheme in recent literature include [77] and [102].

Obfuscation-based techniques have the advantage of being scalable since the transformations usually only need to be

applied to the data at the point of origin, after which the obfuscated data can be used directly. However, the security of these techniques is harder to prove since it relies on randomness and anonymity, and it is harder to prove that a clever inference attack might not be able to re-identify some of the users. Another concern for this family of techniques is the accuracy, since adding randomness to the data can lead to the loss of some key information that some CF algorithms might be able to benefit from in providing more accurate recommendations.

3) Clustering-based techniques: Clustering-based techniques for PPCF rely on grouping the users into clusters or communities, then extracting a representation of that cluster and using it, providing anonymity for the users within each cluster. This can be used to protect against inference attacks by semi-honest or malicious adversaries, provided that the clusters are large enough and are chosen appropriately. It can also be used as a user profile privacy guarantee, if the user profile data is not stored in the system, and only the cluster information is used to provide recommendations.

Contributions under this category may overlap the other categories, often relying on cryptographic techniques [17], [19], [21], [91] or hashing [62] to extract the representation of each cluster and perform the CF calculations securely.

This approach has an obvious advantage in terms of scalability over the sole use of cryptographic techniques, since a reduced representation of the data is used instead of trying to encrypt the entire data set. However, care must be taken when implementing such a technique, to ensure that the accuracy of the results does not suffer due to this reduced representation.

4) Other Approaches: Some contributions in recent literature (e.g.: [24], [43], [81], [90], [99], [100]) resorted to the use of alternative approaches to provide a reasonable compromise that still maintains users' privacy without incurring the computation cost required by other methods. These approaches are often based on knowledge of the problem domain and rely on algorithms that are especially designed to leverage this knowledge.

In [43], the authors built a CF system based on expert opinions, in which the items are rated by domain experts instead of relying on user ratings, thus eliminating the privacy concerns altogether. Similarly, the authors in [90] substituted item-similarity in place of user-similarity in their CF scheme, which removed the need for user profile data in the system and instead used the item data to calculate the recommendations. Another item-based approach was used in [24] and [100]. They used a distributed belief propagation approach that relies on statistical measures to provide the users with recommendations based on item-similarity without the need to store the user preferences in the system.

Alternative approaches to PPCF have the advantage of leveraging the problem domain knowledge to avoid the need for costly cryptographic operations or applying transformations to the data. However, they can potentially be of limited use since they rely on knowledge from specific domains. Item-based approaches may also sacrifice on recommendation accuracy since the users' preferences may contain key information that helps the CF system provide accurate and relevant recommendations.

IV. Conclusion

This survey examined the recent literature on PPCF recommendation systems from a broad perspective. The contributions were classified based on the vulnerability they address, then divided into a number of categories representing the type of approach used in each contribution. The different categories were discussed in terms of the different vulnerabilities they address, and a discussion of some of the potential advantages and disadvantages of each category was provided. Considering the rising popularity of CF systems and the equal rise of privacy awareness by users, this survey aims to assist researchers and practitioners interested in the development of practical and secure CF systems identify the most suitable approach for their particular problem based on the recent contributions in the field.

Acknowledgement

Partial support for this research was received from the Missouri University of Science and Technology Intelligent Systems Center, the Mary K. Finley Missouri Endowment, the National Science Foundation, the Lifelong Learning Machines program from DARPA/Microsystems Technology Office, and the Army Research Laboratory (ARL); and it was accomplished under Cooperative Agreement Number W911NF-18-2-0260. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

The authors would like to thank Emma Powell for her invaluable assistance with the organizational effort put into this survey.

References

[1] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, pp. 734–749, jun 2005.

[2] X. Su and T. M. Khoshgoftaar, "A survey of collaborative filtering techniques," *Advances in Artificial Intelligence*, vol. 2009, no. Section 3, pp. 1–19, 2009.

[3] J. S. Breese, D. Heckerman, and C. Kadie, "Empirical analysis of predictive algorithms for collaborative filtering," in *Proceedings of the 14th Annual Conference on Uncertainty in Artificial Intelligence*, ser. UAI'98. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1998, pp. 43—-52.

[4] A. Das, M. Datar, A. Garg, and S. Rajaram, "Google news personalization: scalable online collaborative filtering," in *Proceedings of the 16th international conference on*, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 271–280.

[5] P. A. D. De Castro, F. O. De França, H. M. Ferreira, and F. J. Von Zuben, "Evaluating the performance of a biclustering algorithm applied to collaborative filtering - A comparative analysis," in *Proceedings - 7th International Conference on Hybrid Intelligent Systems, HIS 2007*. Ieee, sep 2007, pp. 65–70.

[6] ——, "Applying biclustering to perform collaborative filtering," in *Proceedings of The 7th International Conference on Intelligent Systems Design and Applications, ISDA 2007*. Ieee, oct 2007, pp. 421–426.

[7] T. George and S. Merugu, "A scalable collaborative filtering framework based on co-clustering," in *Proceedings - IEEE International Conference on Data Mining, ICDM*, nov 2005, pp. 625–628.

[8] J. L. Herlocker, J. A. Konstan, L. G. Terveen, and J. T. Riedl, "Evaluating collaborative filtering recommender systems," *ACM Transactions on Information Systems (TOIS)*, vol. 22, no. 1, pp. 5–53, 2004.

[9] G. Linden, B. Smith, and J. York, "Amazon.com recommendations: Item-to-item collaborative filtering," *IEEE Internet Computing*, vol. 7, no. 1, pp. 76–80, jan 2003.

[10] R. J. Meuth, P. Robinette, and D. C. Wunsch, "Computational intelligence meets the NetFlix prize," in *Proceedings of the International Joint Conference on Neural Networks*, jun 2008, pp. 686–691.

[11] P. Resnick, N. Iacovou, M. Suchak, P. Bergstrom, and J. Riedl, "GroupLens," in *Proceedings of the 1994 ACM conference on Computer supported cooperative work - CSCW '94*, ser. CSCW '94. New York, NY, USA: ACM, 1994, pp. 175–186.

[12] R. R. Zhu and S. S. Gong, "Analyzing of collaborative filtering using clustering technology," in *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, vol. 4. IEEE, aug 2009, pp. 57–59.

[13] F. Casino, C. Patsakis, D. Puig, and A. Solanas, "On Privacy Preserving Collaborative Filtering: Current Trends, Open Problems, and New Issues," in *e-Business Engineering (ICEBE), 2013 IEEE 10th International Conference on*. IEEE, sep 2013, pp. 244–249.

[14] J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V. Shmatikov, ""You might also like:" Privacy risks of collaborative filtering," in *Proceedings - IEEE Symposium on Security and Privacy*. IEEE, may 2011, pp. 231–246.

[15] O. Goldreich, "Secure multi-party computation," 1998.

[16] R. Agrawal and R. Srikant, "Privacy-preserving data mining," *Proceedings of the 2000 ACM SIGMOD international conference on Management of data - SIGMOD '00*, vol. 29, no. 2, pp. 439–450, jun 2000.

[17] W. Ahmad and A. Khokhar, "An architecture for privacy preserving collaborative filtering on web portals," in *Proceedings - IAS 2007 3rd Internationl Symposium on Information Assurance and Security*, IEEE. Ieee, aug 2007, pp. 273–278.

[18] J. Canny, "Collaborative filtering with privacy," in *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2002-Janua, 2002, pp. 45–57.

[19] H. Kikuchi, H. Kizawa, and M. Tada, "Privacy-preserving collaborative filtering schemes," in *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*. IEEE, mar 2009, pp. 911–916.

[20] R. Parameswaran and D. M. Blough, "Privacy Preserving Collaborative Filtering Using Data Obfuscation," in *Granular Computing, 2007. GRC 2007. IEEE International Conference on*. IEEE, nov 2007, p. 380.

[21] B. Memis and I. Yakut, "Privacy-preserving collaborative filtering on overlapped ratings," in *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*. IEEE, jun 2013, pp. 166–171.

[22] A. Basu, J. Vaidya, H. Kikuchi, and T. Dimitrakos, "Privacy-preserving collaborative filtering for the cloud," in *Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011*. IEEE, nov 2011, pp. 223–230.

[23] T. Kandappu, A. Friedman, R. Boreli, and V. Sivaraman, "PrivacyCanary: Privacy-Aware Recommenders with Adaptive Input Obfuscation," in *Modelling, Analysis Simulation of Computer and Telecommunication Systems (MASCOTS), 2014 IEEE 22nd International Symposium on*, sep 2014, pp. 453–462.

[24] T. Zhu, G. Li, Y. Ren, W. Zhou, and P. Xiong, "Differential privacy for neighborhood-based Collaborative Filtering," in *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on*, ser. ASONAM '13. New York, New York, USA: ACM Press, aug 2013, pp. 752–759.

[25] A. C.-C. Yao, "How to generate and exchange secrets," in *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, no. 1. IEEE, 1986, pp. 162–167.

[26] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game - a completeness theorem for protocols with honest majority," in *19th ACM Symposium on the Theory of Computing*, New York, New York, United States, 1987, pp. 218–229. [Online]. Available: http://doi.acm.org/10.1145/28395.28420

[27] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, Chicago, Illinois, May2-4 1988, pp. 1–10.

[28] O. Goldreich, *The Foundations of Cryptography*. Cambridge University Press, 2004, vol. 2, ch. General Cryptographic Protocols. [Online]. Available: http://www.wisdom.weizmann.ac.il/~oded/PSBookFrag/prot.ps

[29] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *Proceedings of the 2000 ACM SIGMOD Conference on Management of Data*. Dallas, TX: ACM, May 14-19 2000, pp. 439–450. [Online]. Available: http://doi.acm.org/10.1145/342009.335438

[30] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Transactions on Knowledge and Data Engineering*, vol. 18, no. 1, pp. 92–106, jan 2006.

[31] L. Sweeney, "*k*-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557–570, 2002. [Online]. Available: http://privacy.cs.cmu.edu/dataprivacy/projects/kanonymity/kanonymity.html

[32] P. Samarati, "Protecting respondent's privacy in microdata release," *IEEE Transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010–1027, Nov./Dec. 2001. [Online]. Available: http://dx.doi.org/10.1109/69.971193

[33] P. M. Aonghusa and D. J. Leith, "Don't Let Google Know I'm Lonely," *ACM Transactions on Privacy and Security*, vol. 19, no. 1, pp. 1–25, 2016.

[34] E. Karydi and K. Margaritis, "Parallel and Distributed Collaborative Filtering: A Survey," *ACM Comput. Surv. Article*, vol. 49, no. 37, 2016.

[35] A. Ozturk and H. Polat, "From existing trends to future trends in privacy-preserving collaborative filtering," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 5, no. 6, pp. 276–291, 2015.

[36] A. BILGE, C. KALELI, I. YAKUT, I. GUNES, and H. POLAT, "a Survey of Privacy-Preserving Collaborative Filtering Schemes," *International Journal of Software Engineering and Knowledge Engineering*, vol. 23, no. 08, pp. 1085–1108, oct 2013.

[37] A. Bilge and H. Polat, "A comparison of clustering-based privacy-preserving collaborative filtering schemes," *Applied Soft Computing Journal*, vol. 13, no. 5, pp. 2478–2489, may 2013.

[38] A. J. P. Jeckmans, M. Beye, Z. Erkin, P. Hartel, R. L. Lagendijk, and Q. Tang, "Privacy in Recommender Systems," *Social Media Retrieval*, pp. 263–281, 2013.

[39] Z. Batmaz and C. Kaleli, "Methods of privacy preserving in collaborative filtering," in *2017 International Conference on Computer Science and Engineering (UBMK)*. IEEE, oct 2017, pp. 261–266.

[40] I. Gunes, C. Kaleli, A. Bilge, and H. Polat, "Shilling attacks against recommender systems: a comprehensive survey," *Artificial Intelligence Review*, vol. 42, no. 4, pp. 767–799, 2012.

[41] S. K. Lam and J. Riedl, "Shilling recommender systems for fun and profit," *Proceedings of the 13th conference on World Wide Web WWW 04*, pp. 393–402, 2004.

[42] A. Bilge, I. Gunes, and H. Polat, "Robustness analysis of privacy-preserving model-based recommendation schemes," *Expert Systems with Applications*, vol. 41, no. 8, pp. 3671–3681, 2014.

[43] J. W. Ahn and X. Amatriain, "Towards fully distributed and privacy-preserving recommendations via expert collaborative filtering and restful linked data," in *Proceedings - 2010 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2010*, vol. 1. IEEE, aug 2010, pp. 66–73.

[44] E. Aïmeur, G. Brassard, J. M. Fernandez, and F. S. Mani Onana, "Alambic: A privacy-preserving recommender system for electronic commerce," *International Journal of Information Security*, vol. 7, no. 5, pp. 307–334, feb 2008.

[45] X. Amatriain, N. Lathia, J. M. Pujol, H. Kwak, and N. Oliver, "The wisdom of the few," *Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval SIGIR 09*, vol. 61, no. 6, p. 532, 2009.

[46] F. Armknecht and T. Strufe, "An efficient distributed privacy-preserving recommendation system," *2011 the 10th IFIP Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net'2011*, pp. 65–70, 2011.

[47] S. Banerjee, N. Hegde, and L. Massoulie, "The price of privacy in untrusted recommender systems," in *IEEE Journal on Selected Topics in Signal Processing*, vol. 9, no. 7, oct 2015, pp. 1319–1331.

[48] R. Baraglia, C. Lucchese, S. Orlando, R. Perego, and F. Silvestri, "Preserving Privacy in Web Recommender Systems," *Privacy-Aware Knowledge Discovery Novel Applications and New Techniques*, pp. 369–391, 2011.

[49] R. Baraglia, C. Lucchese, S. Orlando, M. Serrano', and F. Silvestri, "A privacy preserving web recommender system," *Proceedings of the 2006 ACM symposium on Applied computing - SAC '06*, p. 559, 2006.

[50] A. Basu, J. Corena, S. Kiyomoto, and S. Marsh, "Privacy preserving trusted social feedback," *Sac*, vol. 14, no. 3, pp. 0–5, 2014.

[51] A. Basu, J. Vaidya, T. Dimitrakos, and H. Kikuchi, "Feasibility of a privacy preserving collaborative filtering scheme on the Google App Engine," *ACM Symposium on Applied Computing*, p. 447, 2012.

[52] A. Basu, J. Vaidya, H. Kikuchi, and T. Dimitrakos, "Privacy-preserving collaborative filtering on the cloud and practical implementation experiences," in *IEEE International Conference on Cloud Computing, CLOUD*. IEEE, jun 2013, pp. 406–413.

[53] A. Basu, J. Vaidya, H. Kikuchi, T. Dimitrakos, and S. K. Nair, "Privacy preserving collaborative filtering for SaaS enabling PaaS clouds," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 1, no. 1, p. 8, 2012.

[54] A. Bilge and H. Polat, "Improving privacy-preserving NBC-based recommendations by preprocessing," in *Proceedings - 2010 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2010*, vol. 1. IEEE, aug 2010, pp. 143–147.

[55] ——, "An improved privacy-preserving DWT-based collaborative filtering scheme," *Expert Systems with Applications*, vol. 39, no. 3, pp. 3841–3854, feb 2012.

[56] ——, "A scalable privacy-preserving recommendation scheme via bisecting k-means clustering," *Information Processing and Management*, vol. 49, no. 4, pp. 912–927, jul 2013.

[57] D. Bogdanov and R. Sassoon, "Institute of Information Security Privacy preserving collaborative filtering with Sharemind," *Cybernetica research report*, pp. T–4–2, 2008.

[58] S. Borole and S. B. Javheri, "Private recommendation based on Elgamal homomorphic encryption scheme," *Int J Adv Res Comput Sci Soft Eng*, vol. 4, pp. 1364–1367, 2014.

[59] A. Boutet, D. Frey, R. Guerraoui, A. Jégou, and A.-M. Kermarrec, "Privacy-Preserving Distributed Collaborative Filtering," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8593 LNCS, pp. 169–184, 2014.

[60] S. Spiekermann, "Individual Price Discriminaton - An impossibility?" *Proceedings of the CHI2006 Workshop on Privacy-Enhanced Personalization*, no. April, pp. 47–52, 2006.

[61] S. Castagnos, *Privacy Concerns when Modeling Users in Collaborative Filtering Recommender Systems*, 2008.

[62] R. Chow, M. A. Pathak, and C. Wang, "A practical system for privacy-preserving collaborative filtering," in *Proceedings - 12th IEEE International Conference on Data Mining Workshops, ICDMW 2012*. IEEE, dec 2012, pp. 547–554.

[63] Z. Erkin, T. Veugen, and R. Lagendijk, "Privacy-preserving recommender systems in dynamic environments," *Proceedings of the 2013 IEEE International Workshop on Information Forensics and Security, WIFS 2013*, pp. 61–66, 2013.

[64] Z. Erkin, M. Beye, T. Veugen, and R. L. Lagendijk, "Privacy-preserving content-based recommender system," *Proceedings of the on Multimedia and security - MM&Sec '12*, p. 77, 2012.

[65] A. J. P. Jeckmans, *Cryptographically-enhanced privacy for recommender systems*. University of Twente, 2014.

[66] A. Jeckmans, A. Peter, and P. Hartel, "Efficient privacy-enhanced familiarity-based recommender system," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8134 LNCS, pp. 400–417, 2013.

[67] A. Jeckmans, Q. Tang, and P. Hartel, "Privacy-preserving collaborative filtering based on horizontally partitioned dataset," in *Proceedings of the 2012 International Conference on Collaboration Technologies and Systems, CTS 2012*. IEEE, may 2012, pp. 439–446.

[68] C. Kaleli and H. Polat, "Privacy-preserving SOM-based recommendations on horizontally distributed data," *Knowledge-Based Systems*, vol. 33, pp. 124–135, sep 2012.

[69] ——, "P2P collaborative filtering with privacy," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 18, no. 1, pp. 101–111, 2010.

[70] ——, "Privacy-preserving na??ve Bayesian classifier-based recommendations on distributed data," *Computational Intelligence*, vol. 31, no. 1, pp. 47–68, 2015.

[71] H. Kikuchi, Y. Aoki, M. Terada, K. Ishii, and K. Sekino, "Accuracy of privacy-preserving collaborative filtering based on quasi-homomorphic similarity," in *Proceedings - IEEE 9th International Conference on Ubiquitous Intelligence and Computing and IEEE 9th International Conference on Autonomic and Trusted Computing, UIC-ATC 2012*. IEEE, sep 2012, pp. 555–562.

[72] H. Kikuchi and A. Mochizuki, "Privacy-Preserving Collaborative Filtering Using Randomized Response," *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, vol. 21, no. 4, pp. 671–676, jul 2012.

[73] D. Li, C. Chen, Q. Lv, L. Shang, Y. Zhao, T. Lu, and N. Gu, "An algorithm for efficient privacy-preserving item-based collaborative filtering," *Future Generation Computer Systems*, vol. 55, pp. 311–320, 2016.

[74] D. Li, Q. Lv, H. Xia, L. Shang, T. Lu, and N. Gu, "Pistis: A privacy-preserving content recommender system for online social communities," in *Proceedings - 2011 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2011*, vol. 1. IEEE, aug 2011, pp. 79–86.

[75] S. Liu, A. Liu, G. Liu, Z. Li, J. Xu, P. Zhao, and L. Zhao, "A secure and efficient framework for privacy preserving social recommendation," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9313, pp. 781–792, 2015.

[76] Y. Luo, J. Le, and H. Chen, "A privacy-preserving book recommendation model based on multi-agent," in *2nd International Workshop on Computer Science and Engineering, WCSE 2009*, vol. 2. IEEE, 2009, pp. 323–327.

[77] Z. Luo, S. Chen, and Y. Li, "A distributed anonymization scheme for privacy-preserving recommendation systems," in *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, may 2013, pp. 491–494.

[78] B. Memis and I. Yakut, "Privacy-preserving two-party collaborative filtering on overlapped ratings," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 8, pp. 2948–2966, 2014.

[79] Y. Mochizuki and Y. Manabe, "A privacy-preserving collaborative filtering protocol considering updates," in *2015 10th Asia-Pacific Symposium on Information and Telecommunication Technologies, APSITT 2015*. IEEE, aug 2015, pp. 142–144.

[80] M. Montaner, B. Lopez, and J. Lluis de la Rosa, "Opinion-Based Filtering through Trust," in *Proceedings of the 6th International Workshop on Cooperative Information Agents VI*, vol. 2446 LNAI, 2002, pp. 164–178.

[81] T. Nakamura, S. Kiyomoto, R. Watanabe, and Y. Miyake, "P3MCF: Practical privacy-preserving multi-domain collaborative filtering," in *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013*. IEEE, jul 2013, pp. 354–361.

[82] M. Okkalioglu, M. Koc, and H. Polat, "On the privacy of horizontally partitioned binary data-based privacy-preserving collaborative filtering," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9481, pp. 199–214, 2016.

[83] H. Polat and W. Du, "Privacy-preserving top-N recommendation on horizontally partitioned data," in *Proceedings - 2005 IEEE/WIC/ACM InternationalConference on Web Intelligence, WI 2005*, vol. 2005. IEEE, 2005, pp. 725–731.

[84] ——, "Privacy-preserving collaborative filtering using randomized perturbation techniques," in *Data Mining, 2003. ICDM 2003. Third IEEE International Conference on*. IEEE Comput. Soc, nov 2003, pp. 625–628.

[85] ——, "Privacy-Preserving Collaborative Filtering," *International Journal of Electronic Commerce*, vol. 9, no. 4, pp. 9–35, 2005.

[86] N. Polatidis, C. K. Georgiadis, E. Pimenidis, and E. Stiakakis, "A method for privacy-preserving context-aware mobile recommendations," *Communications in Computer and Information Science*, vol. 570, pp. 62–74, 2015.

[87] M. P. Scipioni, "Towards Privacy-Aware Location-Based Recommender Systems," *IFIP Summerschool 2011. Trento, Italy, September 2011*, p. 2011, 2011.

[88] S. Shang, Y. Hui, P. Hui, P. Cuff, and S. Kulkarni, "Privacy Preserving Recommendation System Based on Groups," *Privacy Preserving Recommendation System Based On Groups*, pp. 1–28, 2013.

[89] A. Smirnov and A. Ponomarev, "Locality-sensitive hashing for distributed privacy-preserving collaborative filtering: An approach and system architecture," *Lecture Notes in Business Information Processing*, vol. 241, pp. 455–475, 2015.

[90] M. Tada, H. Kikuchi, and S. Puntheeranurak, "Privacy-preserving collaborative filtering protocol based on similarity between items," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*. IEEE, apr 2010, pp. 573–578.

[91] D. Tanaka, T. Oda, K. Honda, and A. Notsu, "Privacy preserving fuzzy co-clustering with distributed cooccurrence matrices," in *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems, SCIS 2014 and 15th International Symposium on Advanced Intelligent Systems, ISIS 2014*, dec 2014, pp. 700–705.

[92] S. D. O. Ilboudo, I. Sombi??, A. K. Soubeiga, and T. Dr??bel, "Facteurs influen??ant le refus de consulter au centre de sant?? dans la r??gion rurale Ouest du Burkina Faso," *Sante Publique*, vol. 28, no. 3, pp. 391–397, 2016.

[93] L. Troiano and I. D??az, "A Model for Preserving Privacy in Recommendation Systems," *Communications in Computer and Information Science*, vol. 443 CCIS, no. PART 2, pp. 56–65, 2014.

[94] Q. Wang, W. Zeng, and J. Tian, "Compressive sensing based secure multiparty privacy preserving framework for collaborative data-mining and signal processing," in *Multimedia and Expo (ICME), 2014 IEEE International Conference on*, jul 2014, pp. 1–6.

[95] X. Wang and J. Zhang, "Handling the data growth with privacy preservation in collaborative filtering," *Lecture Notes in Electrical Engineering*, vol. 229 LNEE, pp. 231–243, 2013.

[96] J. Wu, L. Yang, and Z. Li, "Variable weighted BSVD-based privacy-preserving collaborative filtering," in *Proceedings - The 2015 10th International Conference on Intelligent Systems and Knowledge Engineering, ISKE 2015*, 2016, pp. 144–148.

[97] I. Yakut and H. Polat, "Privacy-preserving hybrid collaborative filtering on cross distributed data," *Knowledge and Information Systems*, vol. 30, no. 2, pp. 405–433, apr 2012.

[98] J. Zhang, T. Liu, and S.-S. Feng, "an Improved Privacy-Preserving Collaborative Filtering Recommendation Algorithm," *Computer Engineering*, vol. 16, p. 048, 2010.

[99] J. Zou, A. Einolghozati, and F. Fekri, "Privacy-preserving item-based collaborative filtering using semi-distributed belief propagation," in *2013 IEEE Conference on Communications and Network Security, CNS 2013*. IEEE, oct 2013, pp. 189–197.

[100] J. Zou and F. Fekri, "A belief propagation approach to privacy-preserving item-based collaborative filtering," *IEEE Journal on Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1306–1318, oct 2015.

[101] J. Canny, "Collaborative Filtering with Privacy via Factor Analysis," in *Proceeding SIGIR '02 Proceedings of the 25th annual international ACM SIGIR conference on Research and development in information retrieval*, no. i, 2002, pp. 238–245.

[102] F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig, and A. Solanas, "Privacy Preserving Collaborative Filtering with k-anonymity through microaggregation," in *Proceedings - 2013 IEEE 10th International Conference on e-Business Engineering, ICEBE 2013*. IEEE, sep 2013, pp. 490–497.

[103] ——, "A k-anonymous approach to privacy preserving collaborative filtering," *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 1000–1011, 2015.

[104] R. Chen, M. Xie, and L. V. S. Lakshmanan, "Thwarting passive privacy attacks in collaborative filtering," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8422 LNCS, no. PART 2, pp. 218–233, 2014.

[105] F. J. G. Clemente, "A privacy-preserving recommender system for mobile commerce," in *2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015*, 2015, pp. 725–726.

[106] D. Frey, R. Guerraoui, A.-M. Kermarrec, and A. Rault, "Collaborative Filtering Under a Sybil Attack: Analysis of a Privacy Threat," *Proceedings of the Eighth European Workshop on System Security*, pp. 5:1—-5:6, 2015.

[107] Y. Gao, J. B. Xia, J. J. Ji, and L. Ma, "Robust analysis on a privacy preserving recommendation algorithm under the KNN attack," *Applied Mechanics and Materials*, vol. 610, pp. 717–721, 2014.

[108] K. Honda, A. Kawano, and A. Notsu, "A greedy fuzzy k-member co-clustering algorithm and collaborative filtering applicability," *Smart Innovation, Systems and Technologies*, vol. 30, pp. 39–50, 2015.

[109] K. Honda, Y. Matsumoto, A. Kawano, A. Notsu, and H. Ichihashi, "A study on privacy preserving collaborative filtering with data anonymization by clustering," *Smart Innovation, Systems and Technologies*, vol. 14, pp. 43–52, 2012.

[110] N. Ramakrishnan, B. J. Keller, B. J. Mirza, A. Grama, and G. Karypis, "When being Weak is Brave: Privacy in Recommender Systems," *CoRR*, vol. cs.CG/0105, 2001.

[111] J. Shao, R. Lu, and X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices," in *Proceedings - IEEE INFOCOM*, apr 2014, pp. 244–252.

[112] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and J.-P. Hubaux, "Preserving privacy in collaborative filtering through distributed aggregation of offline profiles," in *Proceedings of the third ACM conference on Recommender systems RecSys 09*. New York, New York, USA: ACM Press, 2009, p. 157.

[113] X. Wang, J. Zhang, P. Lin, N. Thapa, Y. Wang, and J. Wang, "Incorporating auxiliary information in collaborative filtering data update with privacy preservation," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 4, pp. 224–235, 2014.

[114] U. Weinsberg, S. Bhagat, S. Ioannidis, and N. Taft, "BlurMe," in *Proceedings of the sixth ACM conference on Recommender systems - RecSys '12*, ser. RecSys '12. New York, NY, USA: ACM, 2012, p. 195.

[115] F. Zhang, V. E. Lee, and R. Jin, "k-CoRating: Filling Up Data to Obtain Privacy and Utility," *Twenty-Eighth AAAI Conference on Artificial ...*, pp. 320–327, 2014.

[116] S. Zhang, J. Ford, and F. Makedon, "A privacy-preserving collaborative filtering scheme with two-way communication," in *Proceedings of the ACM Conference on Electronic Commerce*, vol. 2006, 2006, pp. 316–323.

[117] Y. Zhao and S. S. M. Chow, "Privacy preserving collaborative filtering from asymmetric randomized encoding," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8975, pp. 459–477, 2015.

[118] J. Zhu, P. He, Z. Zheng, and M. R. Lyu, "A Privacy-Preserving QoS Prediction Framework for Web Service Recommendation," in *Proceedings - 2015 IEEE International Conference on Web Services, ICWS 2015*, jun 2015, pp. 241–248.

[119] T. Zhu, Y. Ren, W. Zhou, J. Rong, and P. Xiong, "An effective privacy preserving algorithm for neighborhood-based collaborative filtering," *Future Generation Computer Systems*, vol. 36, pp. 142–155, jul 2014.

[120] A. Bilge, I. Gunes, and H. Polat, "A Robust Privacy-Preserving Recommendation Algorithm," *Proceedings of the 2nd Asian Conference on Information Systems*, pp. 95–102, 2013.

[121] P.-A. Chirita, W. Nejdl, and C. Zamfir, "Preventing shilling attacks in online recommender systems," *Proceedings of the seventh ACM international workshop on Web information and data management WIDM 05*, vol. 55, no. 2, p. 67, 2005.

[122] I. Gunes and H. Polat, "Robustness analysis of privacy-preserving hybrid recommendation algorithm," *Int J Inf Secur Sci*, vol. 4, pp. 13–25, 2015.

[123] I. Gunes, A. Bilge, C. Kaleli, and H. Polat, "Shilling Attacks against Privacy-Preserving Collaborative Filtering," *Journal of Advanced Management Science*, vol. 1, no. 1, pp. 54–60, 2013.

[124] I. Gunes and H. Polat, "Detecting shilling attacks in private environments," *Information Retrieval Journal*, vol. 19, no. 6, pp. 547–572, 2016.

[125] M. Okkalioglu, M. Koc, and H. Polat, "On the Discovery of Fake Binary Ratings," *SAC 2015: Proceedings of the 30th Annual ACM Symposium on Applied Computing*, pp. 901–907, 2015.