International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Personalised privacy-preserving social recommendation Based on Ranking systems

G.Bindhu Harshitha[1], J. Priyanka[2], A.Pravallika[3] , A.Jasmine Gilda[4]

[1] *Computer Science and Engineering Dept of RMK Engineering College*
[2] *Computer Science and Engineering Dept of RMK Engineering College*
[3]*Computer Science and Engineering Dept of RMK Engineering College*
[4]*Associate Professor, Computer Science and Engineering Dept of RMK Engineering College,Tamil Nadu,Chennai*

Abstract - Personalized recommendation is crucial to help the users find pertinent information as the user requested but in this paper we need to obfuscate the users data without being socialized ,where a user has both their public data and private data .Some of the users would prefer to publish their private data where some of them would refuse to so in order to overcome this issue we have proposed PrivRank, a customizable and continues privacy preserving social media data publishing frame work protecting users against inference attacks while enabling personalized ranking-based recommendations, while enabling the privacy preserving we will not be allowing an 3rd party user to know the users information. This helps the user's data to be protected and obfuscate it. The frame work helps the user get the information correctly as requested in a trusted way. Our frame work can efficiently provide effective and continues protection of user-specified private data, while still preserving the utility of the obfuscated data for personalized ranking-based recommendation, in which users can model ratings and social relationships privately The social Recommendation with least privacy leakage to un-trusted recommender and other users (i.e., friends) is an important yet Challenging problem.

Key Words: Privacy-preserving data publishing, customized privacy protection, personalization, ranking-based recommendation, Social media, location based social networks.

1.INTRODUCTION

The recommender system has become an important component on this online platform. With increasing of social networks, recommender systems can take advantage of these social relationships to further improve effectiveness of recommendation Despite their effectiveness, these social relationship-based recommender systems (i.e., social recommendation), may introduce another source of privacy leakage. For example, by observing a users' ratings on products such as adult or medical items, the attacker may infer the users private information. In practice, privacy-preserving social recommender systems, which can provide an accurate recommendation results without sacrificing users' privacy, is very necessary. The major issue faced by the user is leakage of their private information when ever recommended or posted. First, a vast majority of existing efforts heavily depend on an assumption that the recommender is fully trusted network and start to use it. They neglect the fact that the recommender itself may be un-trusted and produce malicious behaviours, causing serious privacy leakage. Second, some other works rely on cryptography to prevent users' exact inputs from being leaked to the un-trusted recommender. Moreover, it has been shown that attackers can still infer sensitive information from the user based by their influence on the final results. Third, some of the existing works rely on friend's history ratings to make recommendations. Social media sites such as IMDB and Facebook allow users to specify the visibility of their ratings on products. Treating equally all the sensitive ratings and thus not exposing any non-sensitive ratings will make it difficult to attract common-interest friends and make effective recommendations, sacrificing user experience in the long run. Our work actually allows to disclosing the non-sensitive rating, but prevents sensitive ratings from being leaked from the exposed non-sensitive ratings. Resolving all the above mentioned defects is necessary for building an effective privacy-preserving social recommender
system, which is a very challenging task due to the following reasons: First, to eliminate the assumption that a recommender is fully trustful, we need to change the recommender system to a semi-centralized manner from a fully centralized. In other words, instead of fully relying on the Challenging, we now allow users and the recommender to collaborate together in the course of recommendation.
Specifically, users can take part in publishing their own ratings, while the recommender can only have access to non-sensitive(public data) ratings, and both parties interact with each other to make the final recommendation. Second, is that when a user unknowingly collaborates with the 3rd part users then their historical data and their future data can also be known to the 3rd part users, the second challenge is to continuously preserve the user data stream without leakage of their data. Third issue noticed is on the ranking based recommendation where the user recommends to get their data , here it is being adopted b man of the users to get the higher ranking output, so when the data is obfuscated ranking loss is occurred not in all cases but to overcome this

loss it requires high cost, the third challenge is to efficiently bound the ranking –loss when the data is obfuscated.

1.1 Historical data publishing

When a user subscribes to a third-party service for the first time, the service provider has access to the user's entire historical public data to obfuscate the user's historical data, we minimize the privacy leakage from her historical data by obfuscating her data using data from another user whose historical data is similar but with less privacy leakage.

1.2 Online data publishing

After the user subscribed to third-party services, the service provider also has real-time access to her future public data stream. Due to efficiency considerations, online data publishing should be performed based on incoming data instances only (e.g., a rating/tagging/checking-in activity on an item), without accessing the user's historical data. Therefore, we minimize the privacy leakage from individual activity data instance by obfuscating the data stream on-the-fly.

2. RELATED WORK

To protect and continuously provide privacy to the user published data the existing system depends on some policies where even it cannot guaranty that the stored and published user data can be protected from malicious attackers. So, the key idea is to mainly obfuscate the data when published data remains useful for some application scenarios while the individual's privacy is preserved.
According to the issues occurs they are categorized into 2 types:

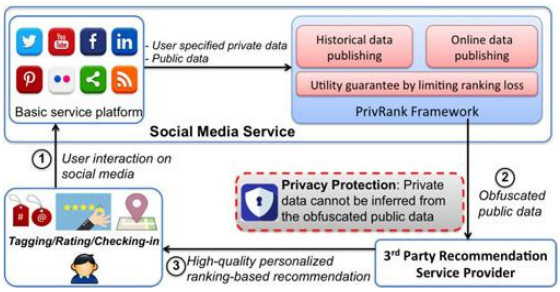

Fig -1: System workflow for privacy-preserving publishing of social media data: 1) Users report their activity (i.e., public data) on social media services; 2) PrivRank publishes the obfuscated public data to third-party service providers; and 3) the third-party service providers can still deliver high-quality personalized ranking-based recommendation to user

The first category is based on heuristic techniques to protect the ad-hoc defined user privacy. Specific solutions mainly tackle the privacy threat when attackers are able to link the data user's identity to a record based on the published data. For example, to protect user privacy from identity disclosure, K-anonymity obfuscates the produced data so that each record cannot be distinguished from at least k-1 other records. However, since these techniques usually have ad-hoc privacy definitions, they have been proven to be non-universal and can only be successful against limited adversaries. The second category focuses on the uninformative principle, i.e., on the fact that the published data should provide attackers with as little additional information as possible beyond background knowledge provided.

Differential privacy is a well-known technique that is known to guarantee user privacy against attackers with unknown background knowledge. They try to quantitatively measure privacy leakage based on various entropy-based metrics such as conditional entropy and mutual information and to design privacy protection mechanisms based on those measures. Although the idea of differential privacy is stricter (i.e., against attackers with arbitrary background knowledge) than that of information-theoretic approaches. Where, information theory can provide informative guidelines to quantitatively measure the amount of a user's private information that an adversary can know by observing and analyzing the user's public data
(i.e., the privacy leakage of private data from public data).
In this case stud we support the information-theoretic approach. The privacy leakage of private data from the published public data, this is minimized by obfuscating the users data In the current literature, the obfuscation methods mainly ensures data utility by bounding the data distortion using metrics such as Euclidean distance , Squared L2 distance , Hamming distance or Jensen-Shannon distance. They are similar to limiting the loss of predicting user ratings on items, where the goal is to minimize the overall difference (e.g., mean absolute error) between the predicted and the real ratings from the users. Therefore minimizing such a rating prediction error is widely adopted by the research community, ranking-based (or top-N) recommendation is more practical and is actually adopted by many of the e-commercial platforms. Specifically, different from rating prediction that tries to infer the user rating information, where as ranking-based recommendation show the mostly liked pages to appear on the top, we argue that the bounding of data of ranking based is occurred due to obfuscation where it shows the wrong data rather than the correct produced ranking data in order to dissolve this we use Kendall- t method to overcome this issue to provide the actual data to the user.

Items	i_1	i_2	i_3
Original rating: a	1	2	5
Obfuscated rating 1: $\hat{a}_1$	3	4	5
Obfuscated rating 2: $\hat{a}_2$	1	4	3

3. PRELIMINARIES

In the figure shown above about the cycle how PrivRank is made used to protect the user's from attackers. All the user's wishes for a secure search recommendation issue occurs when

1. When a user actually shares their data such as (tagging, commenting, ratings) in social media with anyone else.
2. When the subscribe to an 3rd part users their data gets attacked, Which makes the attacker to use the historical a well as the future data of the particular user. Eg: when a person goes to a movie along with their friends the tag them and make their location available to all the social friends, and the rate the movie according to their wish but the personal data i.e their private data such as their name location must be kept secured in order to prevent this we make use of PrivRank. When a user unknowingly make use of the 3rd party user's we obfuscate the data to avoid inference attacks or leakage problems, instead the 3rd part can act as a privacy protected recommender including high raking- based system. Our system workflow is beneficial to all the involved entities, when a user shares her activities with her friends on a social media, while now experiencing high quality personalized recommendations from a third-party service under a customized privacy guarantee, where only obfuscated user activity data can be seen from the social media platform to the third-party service. Second, the third-party service may attract more users (in particular privacy conscious users), when providing high-quality recommendation services with privacy protection. It can also gain main users to make use of their service by providing personalized and customized information of the user.

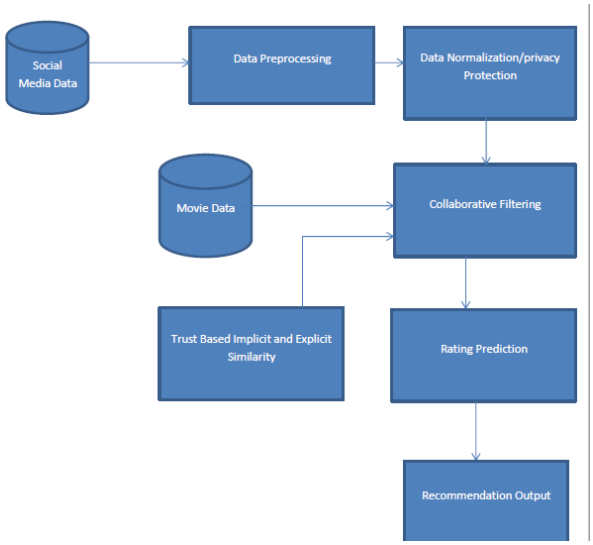

FIG 2: System Architecture

4. CONCLUSION

We consider the personalized security settings of privacy preserving social recommendation as a problem. We propose a novel differential privacy-preserving framework in a semi-centralized way which can protect users' sensitive ratings while being able to retain recommendation effectiveness. Theoretic analysis and experimental evaluation on real-world datasets demonstrate the effectiveness of the proposed framework for recommendation as well as privacy protection. Several directions can be further investigated. Initially, we build in factorization of matrix that is point based model this paper. Study privacy preserving social recommendation using ranking based models such as BPR (Rendle et al. 2009) in the future. Further, we take into consideration of static data. We go through the temporal and dynamic data will be taken as a problem. (Koren 2010) .

5. FUTURE WORK

- Noise perturbation against reconstruction attacks also helps increase the level of privacy protection.

- With the similar privacy budget, the level of privacy protection provided by PrivRank and DPMF are similar. However PrivRank can achieve much better recommendation effectiveness with different privacy

budgets for sensitive and non-sensitive ratings. We perform t-test on recommendation effectiveness of PrivRank and DPMF with the same privacy budgets for sensitive ratings

REFERENCES

[1] Chaudhuri, K.; Monteleoni, C.; and Sarwate, A. D. 2011. Differentially private empirical risk minimization. Journal of Machine Learning Research 12(3):1069–1109.

[2] Dwork, C.; McSherry, F.; Nissim, K.; and Smith, A. 2006. Calibrating noise to sensitivity in private data analysis. In TCC, 265–284.

[3] Fredrikson, M.; Lantz, E.; Jha, S.; Lin, S.; Page, D.; and Ristenpart, T. 2014. Privacy in pharmacogenetics: An end-toend case study of personalized warfarin dosing. In USENIX, 17–32.

[4] Fredrikson, M.; Jha, S.; and Ristenpart, T. 2015. Model inversion attacks that exploit confidence information and basic countermeasures. In CCS, 1322–1333.

[5] Hoens, T. R.; Blanton, M.; and Chawla, N. V. 2010. A private and reliable recommendation system for social networks. In SocialCom, 816–825.

[6] Hua, J.; Xia, C.; and Zhong, S. 2015. Differentially private matrix factorization. In IJCAI, 1763–1770.

[7] Jorgensen, Z., and Yu, T. 2014. A privacy-preserving framework for personalized, social recommendations. In EDBT, 571–582.

[8] Komarova, T.; Nekipelov, D.; and Yakovlev, E. 2013. Estimation of treatment effects from combined data: Identification versus data security. In Iccas-Sice, 3066–3071.

[9] Koren, Y.; Bell, R. M.; and Volinsky, C. 2009. Matrix factorization techniques for recommender systems. IEEE Computer 42(8):30–37.

[10] Koren, Y. 2008. Factorization meets the neighborhood: a multifaceted collaborative filtering model. In SIGKDD, 426–434.