International Journal for Modern Trends in Science and Technology, 8(09): 138-142, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809028
Available online at: http://www.ijmtst.com/vol8issue09.html

Social Media Data Publication with Privacy Protection for Personalized Ranking-Based Recommendations by using Machine Learning Techniques

A.Krishna Madhavi [1] | K.Lakshmana Reddy [2]

[1]Master of Computer Applications (MCA), SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
A.Krishna Madhavi and K.Lakshmana Reddy. Social Media Data Publication with Privacy Protection for Personalized Ranking-Based Recommendations by using Machine Learning Techniques. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 138-142. https://doi.org/10.46501/IJMTST0809028

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

To assist users in finding relevant information, personalized recommendations are essential. To mine user preferences, it frequently uses a sizable collection of user data, particularly information about users' online behaviour (such as tagging, rating, and checking in on social media). However, making such user activity data publicly available exposes users to inference attacks because it is frequently possible to infer personal information (such as gender) from user activity data. In this study, we developed PrivRank, a continuously adaptable framework for publishing social media data that safeguards users' privacy while providing personalized ranking-based suggestions. Its main concept is to continuously obfuscate user activity data so that privacy leakage of user-specified private data is minimized within a defined data distortion budget, which limits the ranking loss resulting from the data obfuscation process to maintain the data's usefulness for enabling recommendations.

KEYWORDS:Inference attacks, Social media, Private data, Recommendation, Personalized, Obfuscate, Distortion, Ranking-Based.

1. INTRODUCTION

In the Big Data era, building efficient recommendation engines is essential to giving people the right information. Online services like ecommerce applications often rely on a sizable collection of user data to give high-quality and personalized suggestions, particularly user activity data on social media like tagging/rating records, comments, check-ins, or other sorts of user activity data. In reality, a lot of users are open to sharing their social media activity data (or streams of data) with a service provider in exchange for receiving individualized, high-quality recommendations. We refer to these user activity data as public data in this essay.However, people frequently see certain information from their social media profile as private, such as gender, economic level, political views, or social acquaintances. These data are referred to as private data in the sections that follow. Although users may choose not to disclose private information, the intrinsic link between public and private information frequently results in substantial privacy breaches. For instance, one's gender can be inferred from her actions on

location-based social networks [2] and one's political allegiance can be deduced from how they rate TV shows [1]. These studies demonstrate that inference attacks [3], when an adversary examines a user's public data to illegitimately learn about her private data, frequently cause harm to private data.Therefore, it is essential to safeguard user private information while providing recommendation engines with public data.

By manipulating the public data before it is published, it is possible to secure private information while reducing the utility of the public data during later processing phases. Utility in the context of recommendation engines refers to how well they do personalization based on distorted public data, or more specifically, how well they are able to forecast a person's preferences based on distorted data. Privacy and personalization are inherently in conflict.

One way or another, greater public data distortion improves privacy protection by making it more difficult for adversaries to deduce private information. On the other side, it also results in a bigger loss in utility, as excessively skewed public data makes it impossible for recommendation engines to effectively forecast consumers' true preferences.

One quick solution is to obscure user public data before it is delivered to social media in order to employ privacy-preserving data publishing procedures in the event of social media-based recommendation. Such a strategy is unrealistic, though, as it undermines important user benefits. In practical applications, social media gives users a platform for social sharing through which they can communicate with their peers by willfully disclosing their thoughts on products, blogs, pictures, videos, or even their current whereabouts.

As an illustration, if a user enjoys a movie and wants to recommend it to her friends, she does not want the rating to be obscured in any way.

An alternate method, as it is improper to obfuscate user public data before sending it to social media, is to preserve user privacy while distributing their public data from social media to any other third-party services. For example, in order to supply them with data, many third-party social media services demand access to user activity data (or data streams). Optional access to users' profiles may also be needed by these services.While some users who value their privacy wish to keep certain information from their profiles private (such as their gender), other users who value their privacy may not care as much and decide to share such information. By discovering the association between the public and private data from the non-privacy-conscious users, an attacker could then improperly deduce the private data of the privacy-conscious users. Therefore, while publishing user public data through social media, privacy protection is essential.

2. LITERATURE SURVEY

1)Smart soul guide: A model for guiding soul with image matching algorithm. J. Sindhu Sri; N. V. Sri Sravani; P. Suresh Kumar In today's life move has become a passion. but move is not simple unless we tend to all understand the place and its details. once we tend to visit a replacement place therefore on perceive the most points of that place, we've got a bent to usually take facilitate of native people sometimes there might arise a state of affairs where we've got a bent to cannot communicate with them. in numerous ways that during which we've got a bent to browse concerning the place this approach could to boot lead to confusion and does not solve the matter. once a soul takes a snap offers|andprovides|and offers} it's input to the applying then it compares the input with the current photos in data and it selects the foremost correct image and thereby offers the data related to the image. so the soul feels comfortable in knowing concerning the place.

2)KAMO - mobile guide for city soul J. Liikka; J. Lahti; P. Alahuhta; M. Rosenberg Author gift a mobile public transportation guide application called KAMO, that gives journey coming up with and stop-specific timetable information for public transportation passengers. Passengers could get their fare exploitation the application; travel news concerning current problems or changes to the overall conveyance are on the market via the KAMO application. Author describe the KAMO service style, compare it with connected work, and illustrate a typical application state of affairs from the user's purpose of browse. Our work takes development in combining journey coming up with and thus the amount of your time positioning-based observance of the buses among constant application and advancing the application's usability of the by utilizing the getting

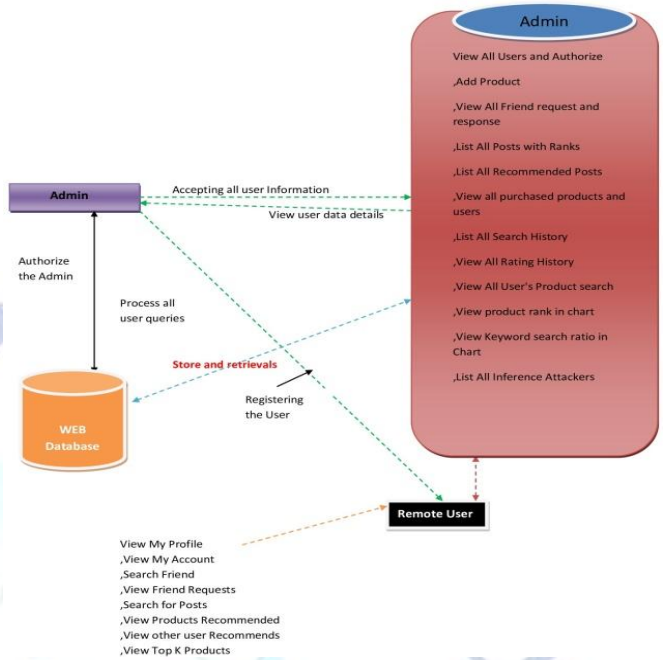
ready to Field Communication (NFC) technology. Author summaries initial user trial results, that demonstrate that NFC are going to be used with public transportation services. supported the user trial results and our own experience, Author gift the long run development directions for KAMO.

3)Route different decision-marking analysis supported congestion charging Zhenggang Li; Jian Wang; Qiu Yan; Ling dynasty The congestion charging would become the required issue of travelers' route different once cities do the congestion charging. this text problems the matter of route optimization different supported congestion charging of the route. per that, use variable weigh analytic hierarchy methodology (VWAHP) to research the route different decision-marking. Results show that the approach of analysis could not exclusively profit exploitation low-cost charging live, but collectively guide travelers' travel.

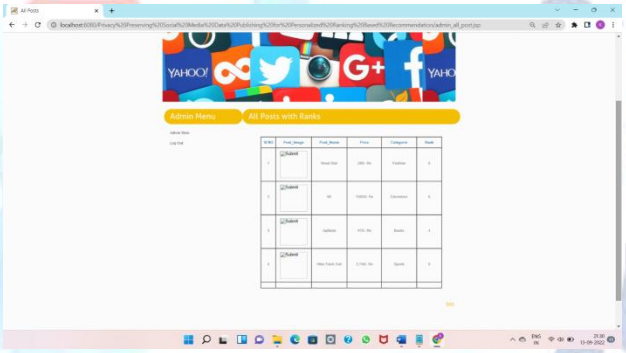
3. PROBLEM STATEMENT

The current practice generally relies on regulations or user agreements, such as those on the use and storage of the published data, to guarantee user privacy while publishing user data. This strategy, however, cannot ensure that a hostile attacker won't gain access to the users' sensitive data. Therefore, privacy-preserving data publishing has been extensively researched in order to offer appropriate privacy protection when releasing user data. Its fundamental concept is to obfuscate user data so that it can be released and still be relevant in specific application circumstances while maintaining the privacy of the user. Existing work can be divided into two categories based on the attacks taken into consideration. The first group relies on heuristic methods to safeguard the privacy of users who have made specific requests. Specific solutions mainly tackle the privacy threat when attackers are able to link the data owner's identity to a record, or an attribute in the published data. The second category is theory-based and 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.

4. ARCHITECTURE DIAGRAM



5. RESULTS



6. CONCLUSION

This study proposed PrivRank, a framework for ongoing and customised privacy-preserving social media data posting. By publicly disseminating obfuscated user activity data, it continuously defends user-specified data against inference assaults while preserving the usefulness of the data for generating individualised ranking-based suggestions. We consider both the

historical and online activity data publishing to provide continuous privacy protection, learn the best data obfuscation to provide customised protection, and bound the ranking loss resulting from the data obfuscation process using the Kendall-rank distance. Finally, we ensure the data utility for enabling ranking-based recommendation.We demonstrated through in-depth testing that PrivRank can protect private information effectively and efficiently while maintaining the usefulness of the published data for various ranking-based recommendation use cases.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] S. Salamatian, A. Zhang, F. du Pin Calmon, S. Bhamidipati, N. Fawaz, B. Kveton, P. Oliveira, and N. Taft, "How to hide the elephant-or the donkey-in the room: Practical privacy against statistical inference for large data," in Proc. of GlobalSIP. IEEE, 2013.

[2] D. Yang, D. Zhang, Q. Bingqing, and P. Cudre-Mauroux, "Privcheck: Privacy-preserving check-in data publishing for personalized location based services," in Proc. of UbiComp'16. ACM, 2016.

[3] C. Li, H. Shirani-Mehr, and X. Yang, "Protecting individual information against inference attacks in data publishing," in Advances in Databases: Concepts, Systems and Applications. Springer, 2007, pp. 422–433.

[4] B. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Computer Survey, vol. 42, no. 4, p. 14, 2010.

[5] I. A. Junglas, N. A. Johnson, and C. Spitzm ¨ uller, "Personality traits and concern for privacy: an empirical study in the context of location-based services," European Journal of Information Systems, vol. 17, no. 4, pp. 387–402, 2008.

[6] P. Cremonesi, Y. Koren, and R. Turrin, "Performance of recommender algorithms on top-n recommendation tasks," in Proc. of RecSys'10. ACM, 2010, pp. 39–46.

[7] N. Li, R. Jin, and Z.-H. Zhou, "Top rank optimization in linear time," in Advances in neural information processing systems, 2014, pp. 1502–1510.

[8] M. G. Kendall, "Rank correlation methods." 1948.

[9] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 557–570, 2002.

[10] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 838–852, 2013.

[11] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," ACM Transactions on Knowledge Discovery from Data, vol. 1, no. 1, p. 3, 2007.

[12] C. Dwork, "Differential privacy," in Automata, languages and programming. Springer, 2006, pp. 1–12.

[13] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in Proc. of Allerton'12. IEEE, 2012, pp. 1401–1408.

[14] A. Zhang, S. Bhamidipati, N. Fawaz, and B. Kveton, "Priview: Media consumption and recommendation meet privacy against inference attacks," IEEE Web, vol. 2, 2014.

[15] S. Salamatian, A. Zhang, F. du Pin Calmon, S. Bhamidipati, N. Fawaz, B. Kveton, P. Oliveira, and N. Taft, "Managing your private and public data: Bringing down inference attacks against your privacy," IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1240–1255, 2015.

[16] W. Chen, T.-Y. Liu, Y. Lan, Z.-M. Ma, and H. Li, "Ranking measures and loss functions in learning to rank," in Proc. of NIPS, 2009, pp. 315–323.

[17] M. B. Eisen, P. T. Spellman, P. O. Brown, and D. Botstein, "Cluster analysis and display of genome-wide expression patterns," PNAS, vol. 95, no. 25, pp. 14 863–14 868, 1998.

[18] R. Baeza-Yates, B. Ribeiro-Neto et al., Modern information retrieval. ACM press New York, 1999, vol. 463.

[19] K. J¨arvelin and J. Kek¨al¨ainen, "Cumulated gain-based evaluation of ir techniques," ACM Transactions on Information Systems (TOIS), vol. 20, no. 4, pp. 422–446, 2002.

[20] B. Efron and R. J. Tibshirani, An introduction to the bootstrap. CRC press, 1994.

[21] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in Recent Advances in Learning and Control. Springer, 2008, pp. 95–110.

[22] G. S. Manku, S. Rajagopalan, and B. G. Lindsay, "Approximate medians and other quantiles in one pass and with limited memory," in ACM SIGMOD Record, vol. 27, no. 2. ACM, 1998, pp. 426–435.

[23] D. Yang, D. Zhang, Z. Yu, and Z. Wang, "A sentiment-enhanced personalized location recommendation system," in Proc. of HT'13. ACM, 2013, pp. 119–128.

[24] D. Yang, D. Zhang, V. W. Zheng, and Z. Yu, "Modeling user activity preference by leveraging user spatial temporal characteristics in lbsns," IEEE Transactions on System, Man, Cybernetics: System, vol. 45, no. 1, pp. 129–142, 2015.

[25] Z. Yu, H. Xu, Z. Yang, and B. Guo, "Personalized travel package with multi-point-of-interest recommendation based on crowdsourced user footprints," IEEE Transactions on Human-Machine Systems, vol. 46, no. 1, pp. 151–158, 2016.

[26] D. Yang, D. Zhang, L. Chen, and B. Qu, "Nationtelescope: Monitoring and visualizing large-scale collective behavior in lbsns," Journal of Network and Computer Applications, vol. 55, pp. 170–180, 2015.

[27] D. Yang, D. Zhang, and B. Qu, "Participatory cultural mapping based on collective behavior data in location-based social networks," ACM Transactions on Intelligent Systems and Technology (TIST), vol. 7, no. 3, p. 30, 2016.

[28] Z. Cheng, J. Caverlee, K. Lee, and D. Z. Sui, "Exploring millions of footprints in location sharing services." Proc. of ICWSM'11, vol. 2011, pp. 81–88, 2011.

[29] X. Zhao, L. Li, and G. Xue, "Checking in without worries: Location privacy in location based social networks," in Proc. of INFOCOM' 13. IEEE, 2013, pp. 3003–3011.

Authors Biography

A.Krishna Madhavi currently pursuing MCA in SVKP &Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. Her research interests include Data Structures, Web Technologies, Operating Systems, Data Science and Artificial Intelligence.

K.Lakshamana Reddy is working as Associate Professor in SVKP & Dr K S Raju Arts & Science College,Penugonda,West Godavari District, A.P. He received MCA from Andhra University, 'C' level from DOEACC, New Delhi and M.Tech from Acharya Nagarjuna University, A.P. He attended and presented papers in conferences and seminars. He has done online certifications in several courses from NPTEL. His areas of interests include Computer Networks, Network Security and Cryptography, Formal Languages and Automata Theory and Object Oriented programming languages.