

Privacy-Preserving Recommendation Based on Kernel Method in Cloud Computing

Tao Li¹, Qi Qian², Yongjun Ren^{3,*}, Yongzhen Ren⁴ and Jinyue Xia⁵

¹College of Artificial Intelligence, Nanjing University of Information Science and Technology, Nanjing, 210044, China

²College of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing, 210044, China

³College of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China

⁴College of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing, 210044, China

⁵International Business Machines Corporation (IBM), NY, USA

*Corresponding Author: Yongjun Ren. Email: renyj100@126.com

Received: 04 March 2020; Accepted: 08 May 2020

Abstract: The application field of the Internet of Things (IoT) involves all aspects, and its application in the fields of industry, agriculture, environment, transportation, logistics, security and other infrastructure has effectively promoted the intelligent development of these aspects. Although the IoT has gradually grown in recent years, there are still many problems that need to be overcome in terms of technology, management, cost, policy, and security. We need to constantly weigh the benefits of trusting IoT products and the risk of leaking private data. To avoid the leakage and loss of various user data, this paper developed a hybrid algorithm of kernel function and random perturbation method based on the algorithm of non-negative matrix factorization, which realizes personalized recommendation and solves the problem of user privacy data protection in the process of personalized recommendation. Compared to non-negative matrix factorization privacy-preserving algorithm, the new algorithm does not need to know the detailed information of the data, only need to know the connection between each data; and the new algorithm can process the data points with negative characteristics. Experiments show that the new algorithm can produce recommendation results with certain accuracy under the premise of preserving users' personal privacy.

Keywords: IoT; kernel method; privacy-preserving; personalized recommendation; random perturbation

1 Introduction

As an emerging product, the Internet of Things has a more complex architecture, no unified standards, and more prominent security issues. While providing various convenient services, it is inevitable that more and more detailed personal information needs to be provided in order to obtain better services. On the other



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

hand, more and more personal information is made public, which makes human beings have no privacy. In particular, government agencies and public service agencies are increasingly publishing data containing personal information. Whether it is privacy in data distribution or location privacy in location services, the protection of users' personal information is particularly important [1,2]. To solve this problem, people use privacy protection technology to protect users' information. But inevitably, more and more detailed personal information needs to be provided in order to get better and convenient services. Collaborative filtering can help with effective personalized recommendations [3,4]. A personalized recommendation system is used to collect user ratings for projects and to search for users with similar interests to help users decide which product to buy [5–7]. So far, there has been a lot of progress in personalization and privacy-preserving, and the relevant progress is as follows.

Personalized recommendation is the technical support that the Internet relies on today. In 2014, Min et al. [8] proposed a model-based collaborative filtering method recommendation algorithm and it can avoid the impact of time factors. Gupta et al. [9] proposed a collaborative filtering prediction for demographics. In 2015, Zheng et al. [10] proposed an optimization algorithm that is the neighbor's choice and predicted audience rating. In the same year, Xing et al. [11] applied the case-based reason to the mechanism filtering of the forgetting collaborative solution to the cold start problem, inferred the score of the user's unsuccessful project, and then recommended the TOP-N collaborative filtering project. In 2016, Qin et al. [12] proposed a collaborative filtering recommendation algorithm for weighted project categories. In 2017, Li et al. [13] proposed a list of user item type ratings based on user-rated and collaborative filtering algorithms. Zayet et al. [14] proposed a new similarity measure weighting technique. In 2018, Yu et al. [15] developed an improved algorithm relied on historical order data for restaurants. Fan et al. [16] proposed a reliability-based similarity calculation metric. The two similarity predictions are combined to predict the user's rating more accurately and improve the reliability of the similarity calculation. In 2019, Zhang et al. [17] proposed a novel algorithm named as Fuzzy Rough Set Theory Based Collaborative Filtering Algorithm, which is used to provide efficient advisory tools for the younger generation. In this year, Kumarl et al. [18] applied the Apriori algorithm to the field of e-commerce. Through the sales data in the transaction database to mine various interesting links between the products purchased by the customers, it can help merchants to formulate marketing strategies, reasonably arranges shelf-guided sales, and attracts more customers. In the same year, Zhang [19] proposed a novel service recommendation approach, which is designed for interactive scenario of service composition, and it mines the user implicit interests and the service correlations for service recommendation.

In terms of privacy-preserving, in 2014, Wang et al. [20] proposed a privacy-preserving method that can be solved data mining. In 2015, Mochizuki et al. [21] proposed a method for updating similarity in privacy protection collaborative filtering. Zhu et al. [22] proposed a simple and effective framework for privacy-preserving through application data interference technology. In 2016, Xia et al. [23] proposed a privacy-preserving method that can encrypt images to avoid leaking sensitive information. Improved recommendation systems based on random interference technology is proposed to privacy-preserving and makes effective recommendations [24]. In 2017, Yang et al. [25] protect user privacy by directly disrupting the original data set. Badsha et al. [26] proposed a privacy-based user-based CF technology based on homomorphic encryption, which can determine the similarity between users and then generate recommendations without revealing any private information. In 2018, Badsha et al. [27] developed a privacy protection protocol based on past history.

Based on above-mentioned development of personalized recommendation and privacy protection, the personalized recommendation privacy protection technology in the current IoT mobile service is still in an early stage, and most of the results have not been discussed in an effective recommendation system for privacy protection [28,29]. To make up for the shortcomings of the recommendation method in the existing IoT mobile service, this paper proposes a new core-based effective personalization algorithm. It

effectively combines random perturbation techniques so that perturbed user data not only protects user privacy, but also enables effective personalized recommendation.

The main idea of this paper is as follows. The related work section mainly introduces preliminary knowledge related to the new algorithm, including the basic idea kernel method. The third section gives the main steps of the new kernel method. The fourth section shows the results of experiment and analysis of relevant results. Finally, the fifth section summarizes this paper and briefly explains the follow-up research work arrangement.

2 Related Works

2.1 Non-Negative Matrix Factorization (NMF)

NMF is to find a non-negative base-matrix and a coefficient-matrix, and it meet equation of $R \approx WH$. It makes all components after decomposition non-negative, and at the same time achieves a non-linear dimension reduction [30–32]. It has good explanation of the local characteristics of things and it can be used to discover image features in the database, to facilitate rapid and automatic identification of applications; to discover the semantic relevance of documents for automatic indexing and extraction of information; to identify genes in DNA array analysis, and so on [33–36].

The raw matrix $R_{n \times m}$ is decomposed into the product of two matrices $W_{n \times t}$ and $H_{t \times m}$:

$$R \approx WH = \sum_{a=1}^t W_{ia} H_{a\mu} \quad (1)$$

where the choice of t value usually satisfied $(n + m)t < nm$, the raw matrix R is compressed to WH . Each column in the R matrix represents an observation, and each row represents a feature. By replacing the raw matrix with the coefficient matrix H , it is possible to obtain a dimensionality reduction matrix of the data features, thereby reducing the storage space [37–39].

2.2 Kernel Non-Negative Matrix Factorization (KNMF)

The literature [40–43] pointed out that kernel method mapping data by a kernel function. New space, then use non-negative matrix factorization for features extraction and analysis in new spaces. On the other hand, kernel method does not require knowledge of the details of the data, only the connection between each data, and finally, the kernel method can handle those data points with negative characteristics [44,45].

Kernel method firstly performs data mapping:

$$\phi : x \in R \rightarrow \phi(x) \in \phi(R) \quad (2)$$

Then do the normal NMF in the new space:

$$\phi(R) = W_\phi H \quad (3)$$

Because it does not know the specific mapping function, the paper need to use the kernel method to get:

$$(\phi(R))^T \phi(R) = (\phi(R))^T W_\phi H \quad (4)$$

It is easy to see that the left side of the above equation is the definition of the kernel. The paper does not need to know the detailed mapping definitions, just need to know their inner product. The choice of kernel can make Gaussian kernel, polynomial kernel and so on. By replacing the above formula with a nuclear function, it can get:

$$K = YH \quad (5)$$

where, $K = (\phi(R))^T \phi(R)$, $Y = (\phi(R))^T W_\phi$

Kernel function is to map data from low-dimensional to a new space, to facilitate the conversion of data that cannot be linearly segmented into data that can be linearly segmented, usually can be described as:

$$F(a, b) = \langle \phi(a), \phi(b) \rangle = (\phi(a))^T \phi(b) \quad (6)$$

It can be seen that the equation and the ordinary non-negative matrix factorization have the same representation, so the same method can be used for solving.

Given a new matrix R_{new} , it can get a new coefficient matrix:

$$\begin{aligned} H_{new} &= (W_\phi)^{-1} \phi(R_{new}) \\ &= (W_\phi)^{-1} ((\phi(R))^T)^{-1} (\phi(R_{new}))^T \phi(R_{new}) \\ &= Y^{-1} K_{new} \end{aligned} \quad (7)$$

where, $Y^{-1} = (W_\phi)^{-1} ((\phi(R))^T)^{-1}$, $K_{new} = (\phi(R))^T \phi(R_{new})$.

3 Privacy Protection Personalized Recommendation Algorithm

The new algorithm is mainly composed of two parts: The data privacy protection process and the data personalization recommendation process. The data protection process is mainly based on random interference technology to hide data; the personalized recommendation process of data is mainly based on the similarity between data to obtain personalized recommendation results.

3.1 User Data Privacy-Preserving Process

The flow diagram of privacy-preserving process of user data is shown in Fig. 1. Privacy-preserving hides raw data through random perturbation techniques. The specific steps are as follows:

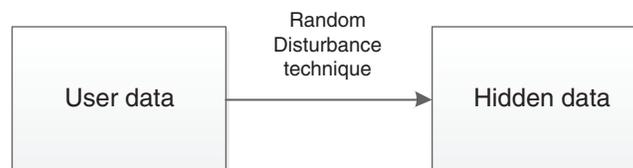


Figure 1: Privacy protection process

First, random perturbation techniques are used in the privacy-preserving of mining. An intuitive method is to add a number of d , so that $a + d$ appears in the database instead of the raw data a , where d is a random number obeying a certain distribution. Although we can do not specific operations on a single data a , if we care about the entire database rather than a single data, then we can still perform the corresponding operations. The method is to randomly perturb the raw data, so that the database in the server saves the changed data instead of the raw data, thereby achieving the purpose of hiding information and privacy-preserving.

Given a recommendation system with n items, m users, for reasons of privacy-preserving, the side of server do not know the raw rating of each user and items the user rated. To do this, it uses a uniform distribution to generate random data. In a uniform distribution, all users produce a random value in the interval $[\mu - \alpha, \mu + \alpha]$. In a normal distribution, all users produce a normal distribution random value and

it combine the mean of μ with the standard deviation of α . The user hides the rating data before sending its rating data to the server. The specific data hiding steps are as follows.

The server determines the specific distribution (uniform distribution or normal distribution) of the disturbance data and the corresponding parameters (α, μ, σ) and informs each user of this information.

Each user fills the unsorted items with the mean of their existing ratings.

For each user u use a certain distribution to generate n random numbers, $i = 1, 2, \dots, n$. Then the user data adds a random number to get a vector of hidden information:

$$z'_{ui} = z_{ui} + d_{ui}, \quad i = 1, 2, \dots, n \quad (8)$$

Finally, the server uses the Eq. (8) to form a rating matrix R' of hidden information.

3.2 User Data Recommendation Process

The flow diagram of the recommendation process of user data is shown in the Fig. 2. The feature matrix is obtained by matrix decomposition of the hidden data obtained above, and then the user-related data is calculated by using the new user data and the feature matrix, and the neighbors are found by the similarity, and finally weighted to obtain the recommended data. Specific steps are as follows.



Figure 2: User data recommendation process

3.3 Non-Negative Matrix Factorization-Based Personalized Recommendation of Privacy-Preserving

The steps of NMF for privacy-preserving are as follows:

1. The rating matrix R' with hidden information is factorized into W and H .
2. Given a new user R_{new} , the user predicted rating for item i . First use the Eq. (1):

$$H_{new} = W^{-1} \phi(R_{new}) \quad (9)$$

3. Then use the new feature matrix H_{new} to compare with the NMF of the H , and using similarity to make recommendation, here you can use the Euclidean distance: Two N -dimensional vectors x_1, x_2 :

$$d_{1,2} = \sqrt{\sum_{k=1}^n (x_{1k} - x_{2k})^2}, k = 1, 2, 3, \dots, N \quad (10)$$

4. Finally, by setting the number of neighbors, some similar users are found and compared to the raw data, it can weighted to obtain the rating of the item i by the user u .

3.4 Kernel Method-Based Personalized Recommendation of Privacy-Preserving

Kernel method has improved the basic idea of NMF. The privacy-preserving step is similar to the NMF, and finally a rating matrix of hidden information is obtained. The kernel method of the hidden matrix is decomposed as follows.

1. A matrix for mapping the data to new spaces through nonlinear mapping. This paper selected the Gaussian kernel function for mapping, and then the NMF is performed to obtain the matrices Y and H .

2. Given a new user and its rating information for the items R_{new} , the user's predicted rating for item i is calculated during the recommendation process. First use the Eq. (7):

$$H_{new} = Y^{-1}\phi(R_{new}) \quad (11)$$

3. Then, using the new feature matrix H_{new} , compare it with the H , and using the similarity to make recommendation. Here, the Euclidean distance can be used: it is consistent with the Eq. (10).

4. Finally, by setting the number of neighbors, some similar users are found and compared to the raw data, it can weighted to obtain the rating of the item i by the user u .

3.5 Time Complexity Analysis

This algorithm consists of two parts: offline data preparation and online data processing. The first part is offline data preparation. It mainly does the nonnegative matrix decomposition of the hidden matrix. Because this part is offline, it is prepared for the second part in advance, which does not affect the online recommendation generation, so the time complexity of this part will not be considered. The second part includes the calculation of H_{new} , the calculation of Euclidean distance, neighbors search and recommendation generation. The time complexity of H_{new} calculation is $O(t * m)$, the time complexity of Euclidean distance is $O(t * n)$, the time complexity of neighbors search is $O(n * \log n)$, and the time complexity of recommendation generation is $O(k * n)$. So, the time complexity of the second part is $O(t * m) + O(t * n) + O(n * \log n) + O(k * n)$. Since k and t are constants, m and n have the same order of magnitude, the time complexity of the second part is $O(n * \log n)$. In conclusion, the time complexity of the algorithm is $O(n * \log n)$.

4 Experiments

4.1 Data

MovieLens is the oldest recommendation system. The MovieLens dataset contains rating data for multiple movies from multiple users, as well as movie data information and user attribute information. This data set is often used as a test data set for recommendation systems, machine learning algorithms. The content in the file contains the rating of each user for each movie. The data in our experiments consists of 1,000,000 ratings for 6,040 users with 3,952 movies, and all users must rate at least 20 movies.

4.2 Metric

The mean absolute deviation is a statistic that describes the degree of data dispersion. The mean absolute error (MAE) is:

$$MAE = \frac{\sum_{i=1}^N |p_i - q_i|}{N} \quad (12)$$

where, p_i indicates the prediction rating of the recommendation system for the i item, q_i indicates real ratings of the i items, and N indicates the number of items.

It can be known from the Eq. (12) that the accuracy of the prediction is represented by calculating the MAE value between the predicted rating and the real ratings.

4.3 Results

This paper demonstrates the effectiveness of the proposed algorithm by comparing the kernel method privacy-preserving algorithm with the non-negative matrix factorization privacy-preserving algorithm. At first, find the mean of the user's rated movie to fill the corresponding unrated movie. Then, each user creates a new privacy-preserving data rating matrix by creating N random values using a Gaussian distribution to hide the raw data.

This experiment mainly verifies the performance of the recommendation system by predicting the rating of the known movie and comparing the real rating of the movie with the predicted rating. Basically, it can be understood that the rating value of the predicted movie is set to null, and the prediction rating is performed by using the hidden matrix and the kernel method-based privacy-preserving algorithm proposed in this paper. Since the matrix decomposition results close to the hidden matrix each time, but the results of each decompose are different, this paper performs 20 matrix decomposition to narrow the difference of prediction results, and finally takes the mean value of the prediction results as the movie rating prediction value, it can narrow the difference of the results.

First, this paper examines the influence of the value of t about the matrix decomposition on the prediction accuracy, and the t value of 5 to 15. Experiments are performed on 6040 users and 3952 projects using non-negative matrix factorization and kernel method respectively to examine the effect of t -value on prediction accuracy. The result is shown in Fig. 3.

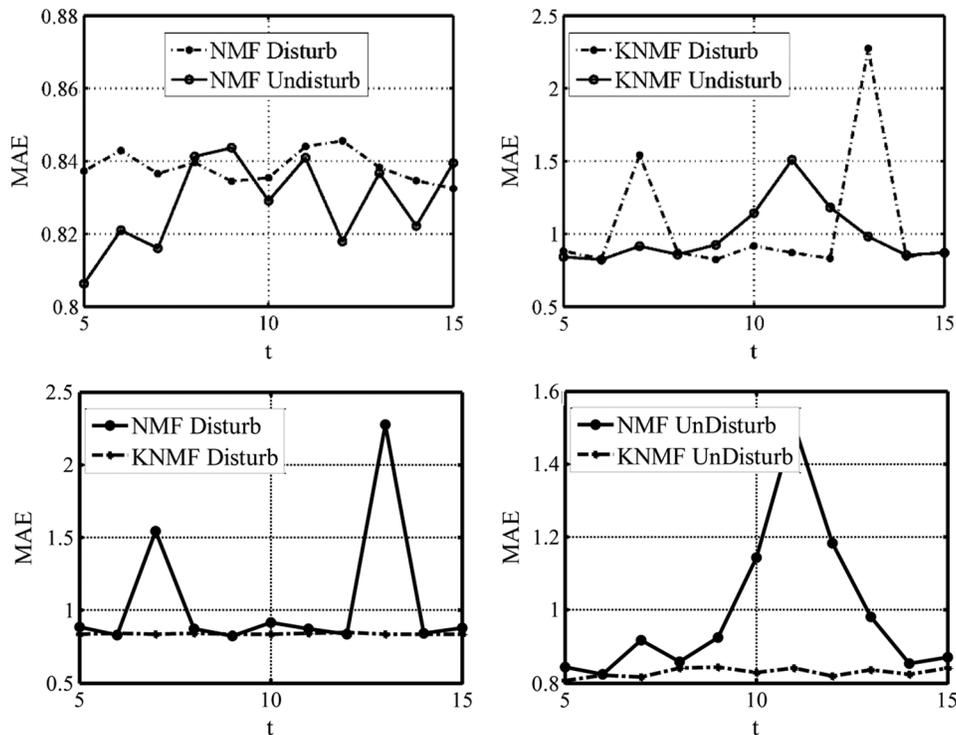


Figure 3: The relationship between the t and the prediction accuracy

In Fig. 3, with the increasing of the value of t after decomposition, the value of MAE shows a steady trend, indicating that the number of t has no significant influence on the prediction accuracy, and is basically in a flat state. The reason should be that when the user or project data is sufficiently rich, the sample mean and variance of the perturbed data will converge to their expected μ . Therefore, the value of users or projects are relatively rich, the system prediction accuracy has no significant impact. In general, due to the using of hidden information for prediction, the accuracy of non-negative matrix factorization and kernel method is slightly lower than that of the direct use of the original score data. The error between the interference and the pre-interference is small, and certain recommendation accuracy can be achieved.

In Fig. 3, when the value of t after decomposition is 6 and 9, the prediction accuracy is high. The following is a comparison of the MAE cases with different neighbors k when the value of t after decomposition is 6 and 9, respectively.

When t after decomposition is 6, the value of MAE of different neighbor k . As shown in Fig. 4.

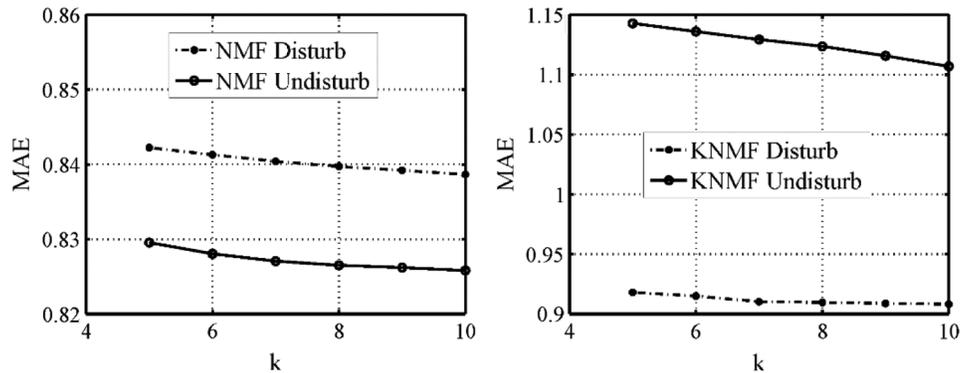


Figure 4: The relationship between prediction accuracy under different k numbers when t is 6 after decomposition

When t after decomposition is 9, the value of MAE of different neighbor k . As shown in Fig. 5.

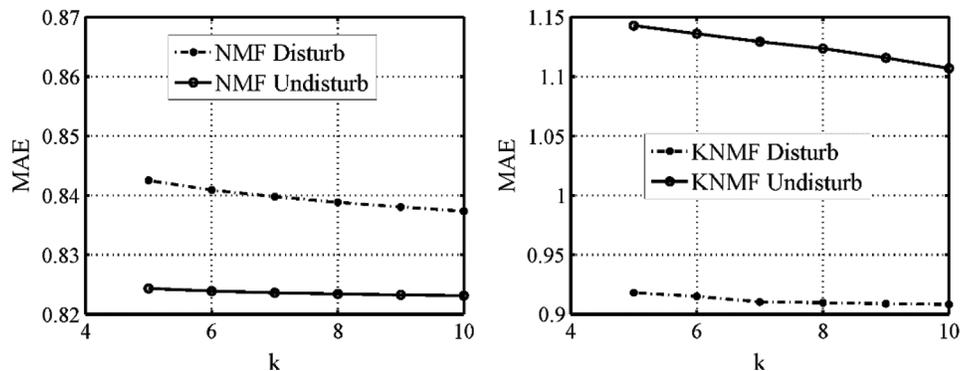


Figure 5: The relationship between prediction accuracy under different k numbers when t is 9 after decomposition

Because non-negative matrix factorization and kernel method predictions mainly use the similarity between new users and existing scoring users to make recommendations, the impact of the number of neighbors on prediction accuracy is investigated. Using the data set experiment of 6040 by 3952, the number of neighbors is changed separately, and the corresponding prediction result is obtained. The results of experiment are shown in Fig. 6.

In Fig. 6, with the increasing of the value of neighbors k , the value of MAE shows a steady trend, indicating that the prediction accuracy is not sensitive to k . The reason should be that when the user or project data is sufficiently rich, that is, the data is relatively rich, and the sample mean and variance of the disturbance data will converge to their desired μ . Therefore, as the number of k increases, the prediction accuracy of the system tends to be stable. It can be proved that the kernel method is slightly higher than non-negative matrix factorization. Kernel method maps data to a new space, and the data

range is reduced, and the corresponding error will also be smaller. Therefore, compared to non-negative matrix factorization, the predictive performance of the kernel method is relatively better.

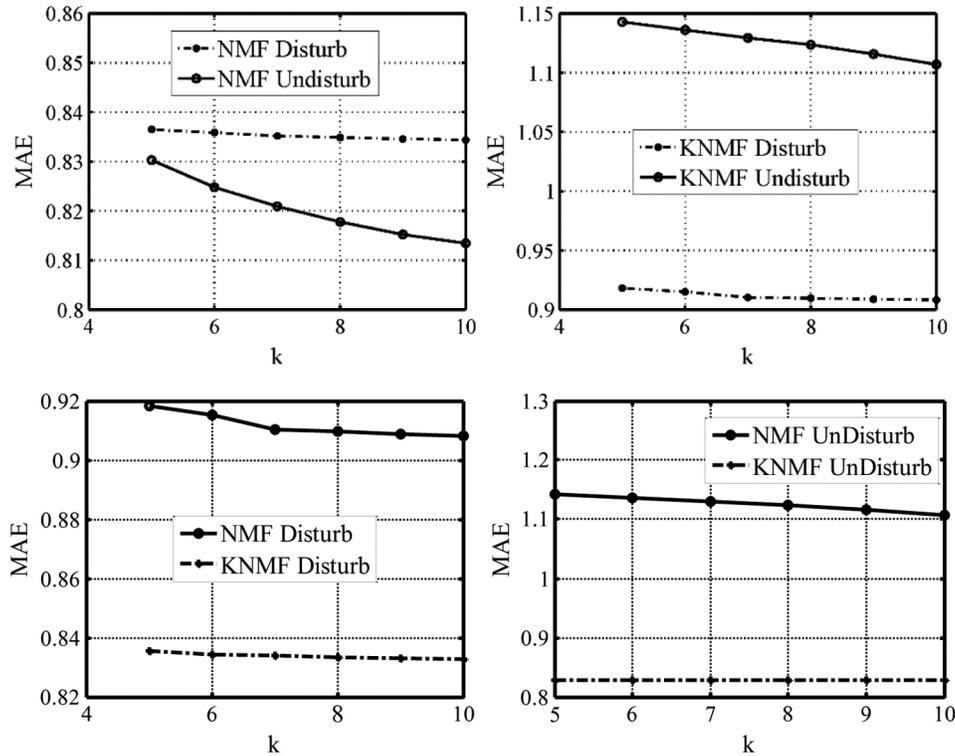


Figure 6: The relationship between the k and the prediction accuracy

In Fig. 6, when the value of k is 9, 10, the prediction accuracy is high. The following compares the prediction accuracy of the value of t after different decompositions when k is 9, 10, respectively.

When k is 9, the value of MAE of t is different after decomposition. As shown in Fig. 7.

When k is 10, the value of MAE of t is different after decomposition. As shown in Fig. 8.

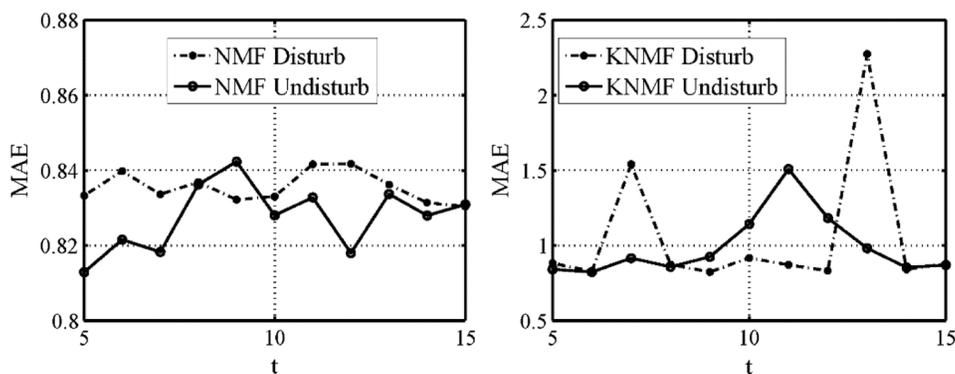


Figure 7: Relationship between prediction accuracy and the number of different decompositions t when the number of neighbors k is 9

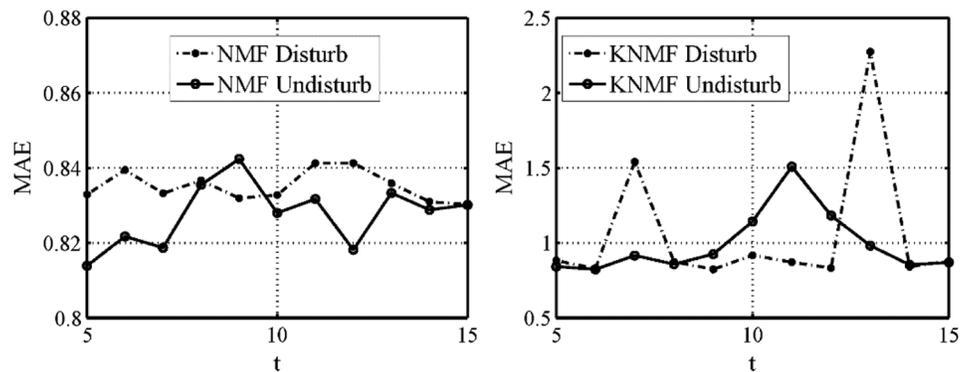


Figure 8: Relationship between prediction accuracy and the number of different decompositions t when the number of neighbors k is 10

In order to examine the influence of the dispersion degree of the disturbance data on the prediction accuracy, a 6040 by 3952 data set experiment was used to change the variance of the disturbance data and examine the results of the corresponding prediction. The results of experiment are shown in Fig. 9.

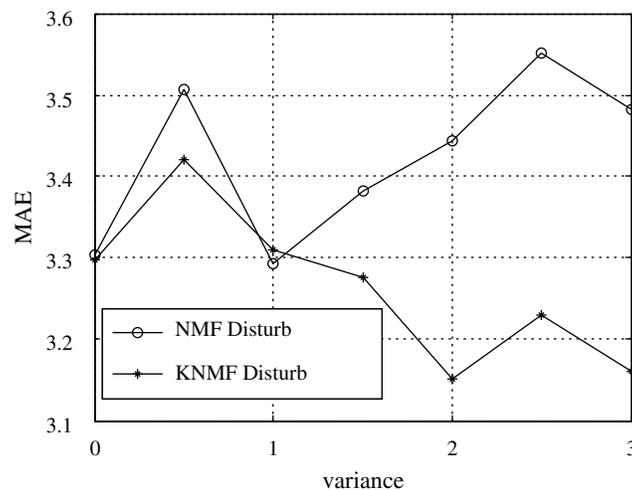


Figure 9: Relationship between variance and prediction accuracy

Obviously, the degree of interference of raw data has a greater impact on the prediction. When the interference degree of the raw data is small, the accuracy of the prediction result of the recommended system is better.

From above experiments, the results of the perturbation data using kernel method are slightly better than non-negative matrix factorization. Moreover, from the previous validity analysis, no matter what kind of disturbance distribution, the mean absolute error using the same algorithm should converge to the error of the undisturbed data in the large samples.

This paper proposed a kernel method-based privacy-preserving collaborative filtering algorithm that is easy to implement and can guarantee effectiveness of recommendation. This algorithm mainly involves two parameters, one is the dimension value t in matrix decomposition, the other is the number of neighbors k of the current user. The experimental results on page 8–9 show that the algorithm is relatively insensitive to t value, and small changes have little impact on the results; the experimental results on page 9–10 show that

the algorithm is also insensitive to k value, and the small changes of its value can be ignored. To sum up, the settings of these two parameters can be adjusted according to the actual application scenarios. Compared to the NMF-based privacy-preserving algorithm, its corresponding prediction accuracy has been improved. And compared to the direct recommendation on non-hidden data, although the accuracy is reduced, the performance is acceptable as a compromise of privacy-preserving. The limitation of this algorithm is that when the number of users and items is large, the time required for NMF or KNMF matrix decomposition is relatively long. However, matrix decomposition can be carried out offline, it has little effect on online user neighbors search and recommendation generation.

5 Conclusions

This paper developed an algorithm of kernel nonnegative matrix factorization and random perturbation technology. The algorithm has a privacy-preserving function, which enables the Internet of Things service system to easily collect the necessary personalized recommendation data while protecting the privacy of users. The actual analysis demonstrates that the kernel method is not sensitive to k and intermediate dimension size t on the basis of preserving the user's privacy. It can improve recommendation accuracy, achieve the effectiveness of recommendation, and meet the needs of the recommendation system. Of course, there are still some problems in the algorithm that need further research, such as the value of users or projects in kernel nonnegative matrix factorization.

Funding Statement: This research was supported by the National Natural Science Foundation of China under Grant No. 61772280; by the China Special Fund for Meteorological Research in the Public Interest under Grant GYHY201306070; and by the Jiangsu Province Innovation and Entrepreneurship Training Program for College Students under Grant No. 201910300122Y.

Conflicts of Interest: We declare that there is no conflict of interests regarding the publication of this article.

References

- [1] Y. J. Ren, Y. Leng, Y. P. Cheng and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Mathematical Biosciences and Engineering*, vol. 16, no. 4, pp. 1874–1892, 2019.
- [2] S. M. H. Rostami, A. K. Sangaiah, J. Wang and X. Liu, "Obstacle avoidance of mobile robots using modified artificial potential field algorithm," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 70, 2019.
- [3] Y. Ren, Y. Leng, F. Zhu, J. Wang and H. J. Kim, "Data storage mechanism based on blockchain with privacy protection in wireless body area network," *Sensors*, vol. 19, no. 10, pp. 2395, 2019.
- [4] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah and H. J. Kim, "An intelligent data gathering schema with data fusion supported for mobile sink in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 15, no. 3, pp. 15501477–19839581, 2019.
- [5] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Information Systems*, vol. 2018, pp. 1–10, 2018.
- [6] J. Wang, Y. Gao, W. Liu, W. Wu and S. J. Lim, "An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks," *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.
- [7] J. Wang, X. Gu, W. Liu, A. K. Sangaiah and H. J. Kim, "An empower Hamilton loop based data collection algorithm with mobile agent for WSNs," *Human-Centric Computing and Information Sciences*, vol. 9, no. 1, pp. 18, 2019.
- [8] Z. Min and S. Yao, "A collaborative filtering recommender algorithm based on the user interest model," in *IEEE 17th Int. Conf. on Computational Science and Engineering*, Chengdu, China, pp. 198–202, 2014.

- [9] J. Gupta and J. Gadge, "A framework for a recommendation system based on collaborative filtering and demographics," in *Int. Conf. on Circuits, Systems, Communication and Information Technology Applications*, Mumbai, India, pp. 300–304, 2014.
- [10] S. Zheng, Y. J. Shen and G. D. Zhang, "A collaborative filtering recommendation algorithm based on dynamic and reliable neighbors," in *Int. Conf. on Software Engineering and Service Science*, Beijing, China, pp. 690–693, 2015.
- [11] L. Xing, C. Xu, W. Wang and Z. Kang, "An improved collaborative filtering recommendation algorithm based on case-based reasoning," in *4th Int. Conf. on Computer Science and Network Technology*, Harbin, China, pp. 740–744, 2015.
- [12] J. Qin, L. Cao and H. Peng, "Collaborative filtering recommendation algorithm based on weighted item category," in *Chinese Control and Decision Conf.*, Yinchuan, China, pp. 2782–2786, 2016.
- [13] L. Li, F. Guo and S. Qin, "A listwise collaborative filtering based on Plackett-Luce model," in *3rd IEEE Int. Conf. on Computer and Communications*, Chengdu, China, pp. 2159–2163, 2017.
- [14] T. Zayet and M. E. Karşılıgil, "A new weighting algorithm for collaborative filtering," in *25th Signal Processing and Communications Applications Conf.*, Antalya, Turkey, pp. 1–4, 2017.
- [15] C. Yu, Q. Tang, Z. Liu, B. Dong and Z. Wei, "A recommender system for ordering platform based on an improved collaborative filtering algorithm," in *Int. Conf. on Audio, Language and Image Processing*, Shanghai, China, pp. 298–302, 2018.
- [16] S. Fan, H. Yu and H. Huang, "An improved collaborative filtering recommendation algorithm based on reliability," in *IEEE 3rd Int. Conf. on Cloud Computing and Big Data Analysis*, Chengdu, China, pp. 45–51, 2018.
- [17] Y. M. Zhang, X. Geng and S. J. Deng, "A novel service recommendation approach in mashup creation," *Intelligent Automation and Soft Computing*, vol. 25, no. 3, pp. 513–525, 2019.
- [18] C. R. Kumarl and V. E. Jayanthi, "A novel fuzzy rough sets theory based CF recommendation system," *Computer Systems Science and Engineering*, vol. 34, no. 3, pp. 123–129, 2019.
- [19] J. T. Zhang, "Personalized product recommendation model based on user interest," *Computer Systems Science and Engineering*, vol. 34, no. 4, pp. 231–236, 2019.
- [20] Q. Wang, W. Zeng and J. Tian, "Compressive sensing based secure multiparty privacy preserving framework for collaborative data-mining and signal processing," in *IEEE Int. Conf. on Multimedia and Expo*, Chengdu, China, pp. 1–6, 2014.
- [21] Y. Mochizuki and Y. Manabe, "A privacy-preserving collaborative filtering protocol considering updates," in *10th Asia-Pacific Sym. on Information and Telecommunication Technologies*, Colombo, Sri Lanka, pp. 1–3, 2015.
- [22] J. Zhu, P. He, Z. Zheng and M. R. Lyu, "A privacy-preserving QoS prediction framework for web service recommendation," in *IEEE Int. Conf. on Web Services*, New York, NY, USA, pp. 241–248, 2015.
- [23] Z. H. Xia, X. H. Wang, L. G. Zhang, Z. Qin, X. M. Sun *et al.*, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2594–2608, 2016.
- [24] F. Zhao, Y. Xiong, X. Liang, X. Gong and Q. Lu, "Privacy-preserving collaborative filtering based on time-drifting characteristic," *Chinese Journal of Electronics*, vol. 25, no. 1, pp. 20–25, 2016.
- [25] M. Yang, T. Zhu, L. Ma, Y. Xiang and W. Zhou, "Privacy preserving collaborative filtering via the Johnson-Lindenstrauss transform," in *IEEE Trustcom/BigData SE/ICSS*, pp. 417–424, 2017.
- [26] S. Badsha, X. Yi, I. Khalil and E. Bertino, "Privacy preserving user-based recommender system," in *IEEE 37th Int. Conf. on Distributed Computing Systems*, Atlanta, GA, USA, pp. 1074–1083, 2017.
- [27] S. Badsha, X. Yi, I. Khalil, D. Liu, S. Nepal *et al.*, "Privacy preserving location-aware personalized web service recommendations," *IEEE Transactions on Services Computing*, 2018.
- [28] J. Wang, Y. Gao, X. Yin, F. Li and H. J. Kim, "An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2018, no. 8, pp. 1–9, 2018.
- [29] D. Zhang, G. Yang, F. Li, J. Wang and A. K. Sangaiah, "Detecting seam carved images using uniform local binary patterns," *Multimedia Tools and Applications*, vol. 79, no. 13–14, pp. 1–16, 2018.

- [30] H. Liu and Z. H. Wu, "Non-negative matrix factorization with constraints," in *Twenty-Fourth AAAI Conf. on Artificial Intelligence*, Atlanta, GA, USA, pp. 506–511, 2010.
- [31] G. Casalino, N. Del Buono and C. Mencar, "Nonnegative matrix factorizations for intelligent data analysis," in *Non-Negative Matrix Factorization Techniques*, 1st ed. Berlin, Germany: Springer-Verlag Berlin Heidelberg, pp. 49–74, 2016.
- [32] J. Jiang and H. Zhang, "Multiplicative update for projective nonnegative matrix factorization with Bregman divergence," in *Third Int. Sym. on Information Processing*, Qingdao, China, pp. 233–237, 2010.
- [33] P. Pande, B. E. Applegate and J. A. Jo, "Application of non-negative matrix factorization to multispectral FLIM data analysis," *Biomedical Optics Express*, vol. 3, no. 9, pp. 2244–2262, 2012.
- [34] A. Asaei, N. Mohammadiha, M. J. Taghizadeh, S. Doclo and H. Bourlard, "On application of non-negative matrix factorization for *ad hoc* microphone array calibration from incomplete noisy distances," in *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, South Brisbane, Queensland, Australia, pp. 2694–2698, 2015.
- [35] G. Alexandridis, G. Siolas and A. Stafylopatis, "Enhancing social collaborative filtering through the application of non-negative matrix factorization and exponential random graph models," *Data Mining and Knowledge Discovery*, vol. 31, no. 6, pp. 1–29, 2017.
- [36] L. Q. Zeng and H. S. Tong, "Application of non-negative matrix factorization and curvelet to remote sensing image fusion," *Journal of East China Institute of Technology*, vol. 188, no. 7, pp. 110–117, 2013.
- [37] Y. Ren, F. Zhu, J. Qi, J. Wang and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial internet of things," *Applied Sciences*, vol. 9, no. 10, pp. 2058, 2019.
- [38] J. Zhang, X. Jin, J. Sun, J. Wang and A. K. Sangaiah, "Spatial and semantic convolutional features for robust visual object tracking," *Multimedia Tools and Applications*, vol. 79, no. 21–22, pp. 1–21, 2018.
- [39] D. Zeng, Y. Dai, F. Li, J. Wang and A. K. Sangaiah, "Aspect based sentiment analysis by a linguistically regularized CNN with gated mechanism," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 3971–3980, 2019.
- [40] J. Yu, J. T. Meng and X. X. Lu, "A kernel based non-negative matrix factorization," in *Second IITA Int. Conf. on Geoscience and Remote Sensing*, Qingdao, China, pp. 376–379, 2010.
- [41] D. Zhang, Z. H. Zhou and S. Chen, "Non-negative matrix factorization on kernels," in *Pacific Rim Int. Conf. on Artificial Intelligence*, Guilin, China, pp. 404–412, 2006.
- [42] F. Zhu and P. Honeine, "Online kernel nonnegative matrix factorization," *Signal Processing*, vol. 131, pp. 143–153, 2017.
- [43] B. Pan, J. Lai and W. S. Chen, "Nonlinear nonnegative matrix factorization based on Mercer kernel construction," *Pattern Recognition*, vol. 44, no. 10–11, pp. 2800–2810, 2011.
- [44] Y. Chen, J. Wang, R. Xia, Q. Zhang, Z. Cao *et al.*, "The visual object tracking algorithm research based on adaptive combination kernel," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 4855–4867, 2019.
- [45] W. Li, H. Liu, J. Wang, L. Xiang and Y. Yang, "An improved linear kernel for complementary maximal strip recovery: Simpler and smaller," *Theoretical Computer Science*, vol. 786, pp. 55–66, 2018.