Received June 2, 2020, accepted June 16, 2020, date of publication June 22, 2020, date of current version July 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004250

A Privacy-Preserving Multi-Task Framework for Knowledge Graph Enhanced Recommendation

BIN YU, CHENYU ZHOU, CHEN ZHANG, GUODONG WANG, AND YIMING FAN
School of Computer Science and Technology, Xidian University, Xi'an 710071, China

Corresponding author: Chen Zhang (zhangc@xidian.edu.cn)

This work was supported by the Key Research and Development Program of Shaanxi Province under Grant 2019ZDLGY17-01 and Grant 2019GY-042.

ABSTRACT Multi-task learning (MTL) is a learning paradigm which can improve generalization performance by transferring knowledge among multiple tasks. Traditional collaborative filtering recommendation methods suffer from cold start, sparsity and scalability problems. The latest research has shown that applying side information of knowledge graph can not only solve the problems above, but also improve the accuracy of recommendation. However, existing multi-task methods for knowledge graph enhanced recommendation expose obvious issues of disclosing the private information of training samples. In order to solve these problems, we put forward a privacy-preserving multi-task framework for knowledge graph enhanced recommendation. In specific, Laplacian noise is added into the recommendation module to guarantee the privacy of sensitive data and knowledge graph is utilized to improve the accuracy of recommendation. Extensive experimental results on three datasets demonstrate that the proposed method can not only preserve the privacy of sensitive training data, but also have little effect on the prediction accuracy of the model.

INDEX TERMS Recommendation system, differential privacy, multi-task learning.

I. INTRODUCTION

Recommendation system (RS) is a branch of information filtering systems, which can find out connections between users and items [1], and is widely used in mobile applications, e-commerce, and even robotics. Specifically, it seeks to predict the rating or preference that a user would give to an item. Recommendation system links users with items through user behavior, such as clicking, browsing, collecting or purchasing [2], which can not be separated from the detailed acquisitions of users' personal information, such as medical diagnostic records, personal consumption habits, user preferences and so on. After obtaining the scoring results based on large datasets, recommendation system recommends proper products to users accurately. However, in the process of obtaining user behavior, the training process is easy to be cracked because the large dataset involves a large number of personal privacy information, and the framework of training recommendation system is mostly based on a single-task mode. Once the training parameters are disclosed, the user's privacy can not be guaranteed. Preserving privacy in recommendation system has practical significance in various fields. Integrating differential privacy into the framework of recommendation system based on knowledge graph is one of the most effective ways to solve the current information overload problems and guarantee the information security [3].

Traditional recommendation system only employs explicit or implicit feedbacks of historical interaction information between users and items as input [4], which brings two problems. One is that in the actual scenario, the interaction information between users and items is particularly sparse [5]. For example, a movie application may contain tens of thousands of movies, while a user may overplay only a few dozen movies on average. Using such a small amount of observed data to predict a large amount of unknown information will increase the risk of overfitting of the algorithm significantly. The other is that for new users and items, the system cannot recommend accurately due to the lack of historical interaction information. Previous research has shown that multi-task learning can improve the performance of recommendation system by transferring information between related tasks [6]. A common way to solve sparsity and cold start problems is to introduce additional auxiliary information into input in recommendation algorithms, such as social networks [7], user

The associate editor coordinating the review of this manuscript and approving it for publication was Ting Wang.

personality [8], item attributes [9], and context [10]. Knowledge graph [11] is an effective kind of auxiliary information, which provides potential features for recommendation systems. Knowledge graph enhanced recommendation system is an alternative learning method that combines knowledge graph feature learning with recommendation system. Integrating knowledge graph into recommendation system can improve the accuracy of recommendation through the enhancement of semantic information.

In previous studies, the vague concept of privacy lacks the corresponding theoretical basis, which affecting the credibility of recommendation results. With the development of information security, existing methods have proposed a variety of privacy-preserving frameworks, such as k-anonymity [12], l-diversity [13], t-closeness [14] and ε-differential privacy [15]. Differential privacy, which is defined by strict mathematical formulas, provides a quantitative evaluation method to compare the level of privacy preservation under different parameters. Moreover, the differential privacy preservation model can still handle with all kinds of attacks even the attacker has strong knowledge backgrounds. In general, differential privacy is usually implemented by Laplacian mechanism or Exponential mechanism to realize differential privacy preservation. Laplacian mechanism [16] is utilized to add random noise which obeys Laplacian distribution to the query results, and differential privacy preservation is realized. Exponential mechanism is used to protect discrete results for non-numerical functions [17]. Boutet *et al.* [18] proposed an algorithm by applying differential privacy to matrix factorization, which adds noise that satisfies different privacy conditions in the user rating data and in the process of random gradient descent [19]. However, the recommendation results of this method is applied to a single-task recommendation system. Motivated by this, we design a provable differential privacy model, which can provide strict privacy guarantee for multi-task recommendation system.

In our model, the carefully designed noise perturbation is added to the gradient descent process and correlative training parameters of the multi-task model. This method can effectively improve the security of the recommendation system, while ensuring the diversity and accuracy of the recommendation results. More specifically, we add the differential privacy mechanism to the recommendation task which has a large amount of private personal data. In order to reduce noise, sensitive data can not be used directly in the knowledge graph module. In theory, adding noise to user's privacy data generally reduces the accuracy of recommended results. However, the performance of multi-task recommendation system can be improved when knowledge graph is used as an auxiliary task. Therefore, the proposed method regards feature learning of knowledge graph and recommendation algorithm as two independent tasks with relevance and compensates the noise perturbation. Our contributions can be summarized as follows:

- We propose a privacy-preserving framework for multi-task recommendation system, which can protect the privacy of sensitive data by adding noise in the process of model training.
- We add Laplacian noise to the recommendation module of our multi-task framework, which ensures the accuracy of the recommendation results on the premise of preserving sensitive data privacy.
- Extensive experimental results show that our algorithm enhances the performance of the recommendation algorithm. Meanwhile, it guarantees the privacy of individual data.

The rest of this paper is organized as follows. The next section reviews related works on the knowledge graph enhanced recommendation system and the privacy-preserving recommendation system. Section 3 describes the proposed approach in detail. Section 4 introduces the experiment and analyses the experimental results of our approach. Section 5 concludes the paper.

II. RELATED WORKS

In this section, we review the existing works of knowledge graph enhanced recommendation system and privacy-preserving recommendation system.

A. KNOWLEDGE GRAPH ENHANCED RECOMMENDATION SYSTEM

Inspired by the successful application of knowledge graph in multi-task learning, researchers has attempted to improve predictive performance in recommendation systems by adopting the advantages of knowledge graphs recently. RippleNet [20] takes knowledge graph as the source of side information, and solves the limitations of existing embedding-based and path-based knowledge graph enhanced recommendation methods. Particularly, an end-to-end Ripple network framework is proposed, which incorporates knowledge graph into recommendation system naturally. This network automatically and iteratively expands users' potential interests along the links in the knowledge graph, and stimulates users' preferences to propagate on the knowledge entity set. DKN [21] proposes a deep knowledge perception network which combines knowledge graph representations with news recommendation. PER [22] studies entity recommendation in heterogeneous information networks. In detail, it suggests integrating heterogeneous relationship information of different users, and provide high-quality recommendation results by using users' implicit feedback data and the personalized recommendation model. However, this kind of method cannot be applied in scenarios where entities do not belong to the same field (such as news recommendation scenarios), because it cannot predefine meta-path or meta-graph for such scenarios. In addition, it also has certain limitations in extending to practical application. To solve these problems, MKR [23] proposes a deep end-to-end framework, which adopts knowledge graph embedding to assist recommendation tasks. Multi-task learning can automatically share potential features and learn the high-order internal relations among items, which can make feature vectors more accurately to describe the complete knowledge graph.

B. PRIVACY-PRESERVING RECOMMENTATION SYSTEM

Differential privacy provides a rigorous and quantitative paradigm to ensure data security. Differential privacy [24] can preserve users' privacy by minimizing the possibility of privacy disclosure and maximizing the accuracy of queries in the case of making statistical queries to databases. Gupta *et al.* [25] studied a novel differentially private multi-task learning algorithm that builds a privacy-preserving variant and learns relationship of tasks based on a covariance matrix. They also developed an attribute-wise noise addition scheme in their algorithm. Xie *et al.* [26] proposed a distributed multi-task framework for privacy preservation to preserve sensitive data and private information that may be contained in the distributed data. The proposed method is a privacy-preserving proximal gradient algorithm which asynchronously updates models of the learning tasks and solves a general class of multi-task learning formulations.

Recommendation system combined with knowledge graph is one of the most popular recommendation strategies nowadays. However, there is a potential risk of privacy disclosure in the recommendation process [27]. Calandrino *et al.* [28] incorporated a differential privacy mechanism to the traditional recommendation algorithm by adding Laplacian noise to the covariance matrix. Friedman *et al.* [29] addressed the problem of privacy-preserving matrix factorization by utilizing differential privacy, which is a rigorous and provable approach to preserve privacy in statistical datasets. What's more, it proposes a generic framework of private-preserving singular value decomposition (SVG) to deal with the privacy problem in matrix factorization based recommendation systems. Liu *et al.* [30] proposed a hybrid method that combines differential privacy with random perturbation. It can not only hide users private data from the server, but also prevent privacy inference from public users.

The existing methods can integrate auxiliary information in recommendation system, but suffer from the problem of privacy leakage. Our model is proposed for the multi-task recommendation system, and the differential privacy preservation mechanism is added in the training process. The sharing of model parameters is not easy to be cracked. Meanwhile, the original information is extracted as feature vectors in the knowledge graph, which solves the shortages of high-dimensional auxiliary information, such as heavy load and low security.

III. METHODOLOGY

This section outlines the definition of related problems and notations. Next, we introduce the proposed framework in detail.

A. PRELIMINARIES

1) RECOMMENDATION SYSTEM

Typically, a recommendation system inputs a set of M users $U = \{u_1, u_2, \ldots, u_M\}$ and a set of N items $V = \{v_1, v_2, \ldots, v_N\}$. The implicit feedback of users to items reflects users' behavior. For an user-item interaction matrix $Y_{M\times N}$, $y_{uv} = 1$ means user u has engaged in item v, and otherwise, $y_{uv} = 0$. The inputs of recommendation system are the information of users and items, and the output is the predictive score of items without users' rating.

2) KNOWLEDGE GRAPH

We define a knowledge graph $\mathcal{G}$ consisting of entity relational triads (h, r, t). Here h, r and t represent the head, the relation and the tail of the knowledge triad respectively. In the recommendation scenario, an item $v \in V$ may be associated with one or more entities in $\mathcal{G}$. Similar to the recommendation module, for a given knowledge triad (h, r, t), we utilize interactive units and nonlinear layers to process the raw feature vectors of head h and relation r (including ID, types, textual descriptions, etc.), respectively. These latent features are then concatenated together, followed by a K-layer multi-layer perception for predicting the tail t. Combined the definition of user-item interaction matrix Y with knowledge graph $\mathcal{G}$, we aim to predict whether user u has potential interests on item v without interactions.

3) DIFFERENTIAL PRIVACY PRESERVATION

Differential privacy, proposed by McSherry *et al.* [31], defines a notion of privacy for a learning algorithm. Given a dataset D, a set of queries is represented by $F = \{f_1, f_2, \ldots f_N\}$. In order to satisfy the condition of privacy preserving, we define the algorithm M to process the query results. The formal definition of differential privacy is as follows:

Definition 1 (Differential Privacy): M is a random algorithm with dataset D as input and ε is a positive real number. P_M is a set of all possible outputs of M. For any two adjacent datasets, and any subset S_M of P_M, the algorithm M satisfies:

$$P_r\left[M(D) \in S_M\right] \leqslant \mathrm{e}^{\varepsilon} \times P_R\left[M\left(D'\right) \in S_M\right] \tag{1}$$

where the parameter ε is the privacy budget and P_r denotes the probability of an event occurring.

Definition 2 (Sensitivity): Given a function $f : D \to \mathcal{R}^d$ over a dataset D where d is the dimension of the feature set $\mathcal{R}$, the sensitivity of f is defined as:

$$S(f) = \max \|f(D_1) - f(D_2)\|_1 \tag{2}$$

where $\|\cdot\|_1$ denotes the L_1-norm. D_1 and D_2 represent a pair of adjacent datasets, which have the same attribute structures, and there is only one individual record difference between two datasets [30]. Sensitivity $S(f)$ essentially reflects the amount of the change in the algorithm M made by a single data point after adding noise:

Definition 3 (Laplace Distribution): In Laplace distribution, λ is an important parameter, which determines the

TABLE 1. Notations and symbols.

Notations	Descriptions
$U = \{u_1, u_2, \dots u_M\}$	The set of M users
$[-i]$	The index set with index i removed
$V = \{v_1, v_2, \dots v_N\}$	The set of N items
$Y_{M \times N}$	User-item interaction matrix
(h, r, t)	The triad of head, relationship and tail
$F = \{f_1, f_2, \dots f_N\}$	A set of queries
ε	Privacy budget
Δf	Sensitivity
λ	A parameter of Laplacian noise
$\widehat{y}$	The predicted probability
$\mathcal{J}$	The cross-entropy function

variance of distribution. The privacy budget ε is a positive real number which is a measure used to control privacy, and A is a randomized algorithm that takes a dataset with user information as input. The following computation maintains ε-differential privacy:

$$\mathrm{H}_A(x) = f(x) + Y \tag{3}$$

$$Y \sim \mathrm{Lap}(\lambda) \tag{4}$$

$$Q(f) = \frac{S(f)}{\lambda} \tag{5}$$

As can be seen from the definition above, $\mathrm{H}_A(x)$ can be considered as a continuous random variable and $Q(f)$ can be considered as the privacy budget ε.

The notations and symbols used in this paper are summarized in Table 1.

B. FRAMEWORK

In this subsection, we propose a privacy-preserving multi-task framework for knowledge graph enhanced recommendation system, not only aiming at solving the privacy leakage problem in recommendation system, but also trying to improve the prediction accuracy of recommendation results. We preserve privacy by adding Laplacian noise to sensitive data in recommendation system. The framework is shown in Figure 1, which consists of two main components: a multi-task recommendation module and a privacy preservation module.

As the central module, the multi-task recommendation module takes advantages of knowledge graph embedding to improve recommendation system. The task of recommendation has at least three layers of multi-layer perceptions: input layer, hidden layer and output layer. Multi-layer perceptions extract compact and dense features for users and items. Each layer of multi-layer perceptions outputs the extracted feature information to the next layer, and finally outputs the prediction probability. Knowledge graph has the head and the relationship of the knowledge triad. Othermore, it also extracts features from the head and the relationship of multiple levels, and finally obtains the prediction tail. The interaction unit interacts with the feature information of items and entities between the two tasks [32], which breaks down the independent interaction assumption by linking items with their attributes [33].

The privacy preservation module preserves the sensitive input data and adds noise through Laplace transformations. In one dataset D, there has basic information and feature attributes extracted by the recommendation algorithm. Adding Laplacian noise can preserve privacy of sensitive information and attribute ratings.

1) MULTI-TASK RECOMMENDATION MODULE

In our model, we use the L-layer multi-layer perception to pass the sensitive information of user u and extract its potential features. The multi-layer perception can be seen as a directed graph, which consists of multiple node layers, and each of nodes is fully connected to the next layer. In addition to the input layer, each node is a processing unit with a nonlinear activation function. Knowledge graph embedding is an effective way to parameterize entities and relationships into vector representations. knowledge graph feature learning method is used to process the triads of knowledge graph, which can obtain the low-dimensional dense vector representation of entities and relationships, and naturally interact with the recommendation system. Here we employ interaction unit to associate with the entities of knowledge graph corresponding to the items and extract their latent features.

In the multi-layer perception, we first vectorize $\{u_1, u_2 \dots u_m\}$ into a set U and define the weight W_l and the bias b_l between layer l and layer $(l+1)$ in the multi-layer perception. W_l is vectorized into $W_{[l]}$, where subscript $[l]$ represents the weight of layer l. The L-layer multi-layer perception is defined as:

$$Z_{l+1} = W_l U + b_l \tag{6}$$

$$\mathcal{M}_{l+1} = \sigma(Z_{l+1}) \tag{7}$$

where Z is the linear combination of the input. In the layer l, it can be seen that the input is U and the output is $\mathcal{M}$ which corresponds to the input of the next layer. The calculation propagates forward, and finally the output of L layer is obtained.

For users' feature vector u, we use the multi-layer perception represented by Formulas 6 and 7 to extract its condensed features. For the item v, we employ an interaction unit to extract features. In the interaction unit, we firstly model latent feature vectors between items and entities. We define d as the dimension of hidden layers and construct the cross-feature matrix I_L of the layer L:

$$I_L = v_l e_l^{\mathsf{T}} = \begin{bmatrix} v_l^{(1)} e_l^{(1)} & \dots & v_l^{(1)} e_l^{(d)} \\ \dots & & \dots \\ v_l^{(d)} e_l^{(1)} & \dots & v_l^{(d)} e_l^{(d)} \end{bmatrix} \tag{8}$$

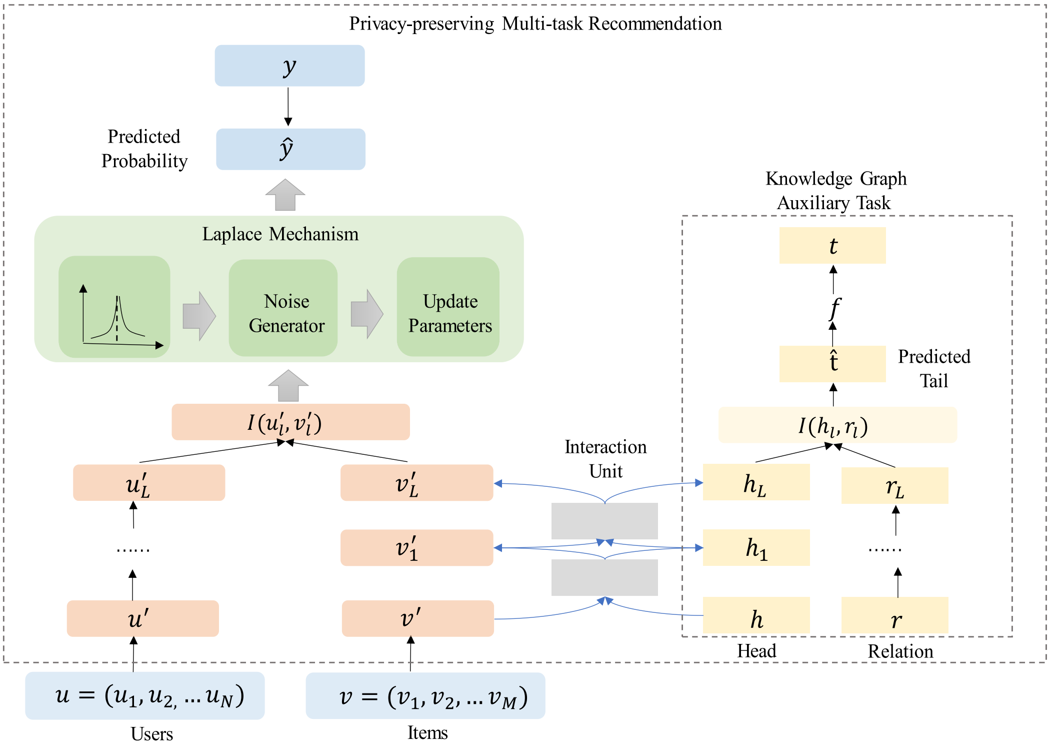


FIGURE 1. A privacy-preserving multi-task framework for knowledge graph enhanced recommendation.

This cross-feature matrix can be embedded into the latent representation space of the items and entities at the next layer to obtain feature vectors. Through multiplying on I_L and I_L^T by their respective weights, the cross-feature matrix is conversed along both horizontal and vertical directions. The output of the interaction unit is denoted as $I(v_l, e_l)$. The correlation between two tasks can be calculated by adjusting the weight of knowledge transfer through interactive units.

After obtaining user u's latent feature u_l and item v's latent feature v_l by the L-layer multi-layer perception and interactive units respectively, we predict the matching score of user and item representations by inner product operation. Combining the latent features u_l and v_l with a predicting function $f_{\mathcal{R}}$, the final predicted probability of user u engaging item v is:

$$\widehat{y_{\mathcal{R}}} = \sigma\left(f_{\mathcal{R}}\left(u_l', v_l'\right)\right) \tag{9}$$

2) PRIVACY PRESERVATION MODULE

The datasets for recommendation system usually contain a large amount of user information, such as age, location, friendly relationship, historic behavior which reflects product preferences and so on. In this paper, we involve the Laplacian mechanism for constructing private-preserving recommendation system. For a large recommendation dataset, we traverse each row of the dataset and read the attributes column by column. According to the Laplacian mechanism in Definition 3, we take different values of privacy budget ε in the privacy module to compare the different effects in the case of adding noise.

For a given privacy budget ε, the parameter λ is calculated as:

$$\lambda = \frac{\Delta f}{\varepsilon} \tag{10}$$

where Δf is sensitivity and refers to Formula (2).

In addition to obtaining the value of the parameter λ, Laplacian noise also has randomness to guarantee differential privacy. We take two random numbers between zero and one, and denote them as μ_1 and μ_2 respectively. For the different values of random variable,

$$n(\lambda|u) = \begin{cases} -\dfrac{\Delta f}{\varepsilon}\varphi(1. - \mu_2), & \text{if } 0 \leq \mu_1 \leq 0.5 \\ \dfrac{\Delta f}{\varepsilon}\varphi(\mu_2), & \text{if } 0.5 \leq \mu_1 \leq 1 \end{cases} \tag{11}$$

where $\varphi(\cdot)$ is the log function. Thus, the result of adding noise can be defined as:

$$\Lambda' = \Lambda + n(\lambda|\mu) \tag{12}$$

where Λ is the sensitivity data.

3) LEARNING ALGORITHM

For a given triad (h, r, t), its plausibility score is formulated as normalized inner product function:

$$score(h, r, t) = \sigma(t^{\mathsf{T}}\hat{t}) \tag{13}$$

where $\hat{t}$ represents the prediction tail in the knowledge graph. A lower score of the triad (h, r, t) suggests that the triad is more likely to be true, and vice versa. The overall loss function of our framework is as follows:

$$\mathcal{L}_R = \sum_{u\in U, v\in V} \mathcal{J}\left(\widehat{y}_{uv'}, y_{uv}\right) - \beta_1 \left(\sum_{(h,r,t,t')\in\mathcal{T}} (score(h,r,t') - score(h,r,t)) \right) + \beta_2 \|W|_2^2 \tag{14}$$

where $\mathcal{T} = \{(h,r,t,t')|(h,r,t) \in \mathcal{G}, (h,r,t') \notin \mathcal{G}\}$. In the previous formula, $\mathcal{L}_R$ is the loss of the multi-task recommendation module, where u' and v' are the set of users and items after adding noise. $\mathcal{L}_R$ contains the loss function of the main recommendation task and the auxiliary knowledge graph task. $\mathcal{J}$ is the cross-entropy function. In our learning algorithm, we use cross-entropy function to measure the loss of recommendation system. In order to reduce the training time, the sigmoid function is utilized as the activation function of neurons and the cross-entropy cost function is utilized to replace the variance cost function. The third term is a regularization term, which aims to avoid overfitting. β_1 and β_2 are the balancing parameters.

In each training iteration, we optimize two tasks alternatively and sample a minibatch of positive/negative interactions from Y and true/false triples from $\mathcal{G}$ [34] following the negative sampling strategy to make the computation more efficient [35]. Specifically, after the initialization of the parameters, when optimize the parameters of knowledge graph feature learning, the parameters of the recommendation system task are invariable. Similarly, when optimize the parameters of recommendation system task, the parameters of the knowledge graph feature learning are invariable. Finally, the output of the learning algorithm is the prediction probability. The loss function in Formula 14 traverses all possible user-item pairs and knowledge triads. One training sample updates only a part of weights at a time, while all other weights are invariant to reduce the amount of calculation. To some extent, the negative sampling strategy can also increase randomness. We pay more attention to the main task of recommendation system. In each epoch, we train the recommendation task t times (usually $t > 1$), and then train the knowledge graph task one time in each epoch.

IV. EXPERIMENTS

In this section, we evaluate the effectiveness of privacy preservation and the accuracy of the recommendation results on a multi-task knowledge graph enhanced recommendation system. The experiments are conducted on three commonly recommendation system datasets: MovieLens-1M [36], Book-Crossing [37] and Last.FM [38]. The experimental results show that our multi-task recommendation system with differential privacy guarantee is feasible without significant impact on the prediction accuracy of recommendation.

TABLE 2. Basic statistics of the three datasets.

Datasets	Users	Items	Ratings	Range
MovieLens-1M	6040	3952	1,000,000	1,...,5
Book-Crossing	278,858	271,379	1,149,780	1,...,10
Last.FM	1892	17,632	92,834	Implicit

A. DATASET

The experiments are conducted on three recommendation system datasets: MovieLens-1M, Book-Crossing, Last.FM. Table 2 shows the statistics of the three datasets and the basic information of the three datasets is as follows:

MovieLens-1M[1]: MovieLens-1M is a virtual community for movie recommendation. It has the group of 1 million ratings for $4,000$ movies provided by $6,000$ MovieLens users. Movie ratings that are submitted by users are on a scale of $1/2$ a star to the maximum of 5 stars. The dataset contains movie scores, users' information and movie profiles.

Book-Crossing[2]: Book-Crossing is a dataset of the book recommendation system. The Book-Crossing dataset contains $1,149,780$ ratings about $271,379$ books provided by $278,858$ users and comprises 3 tables. BX-Users contains the users' information. Books are identified by their respective ISBN in BX-Books. BX-Book-Ratings contains the book rating information.

Last.FM[3]: Last.FM is a music social network site, which allows users to create user profiles and contains information about users' historic records in Last.FM. Specifically, it includes two-way friends, artists, information (with weight) of users listening to the artist, users to artists tag information, artists tag information.

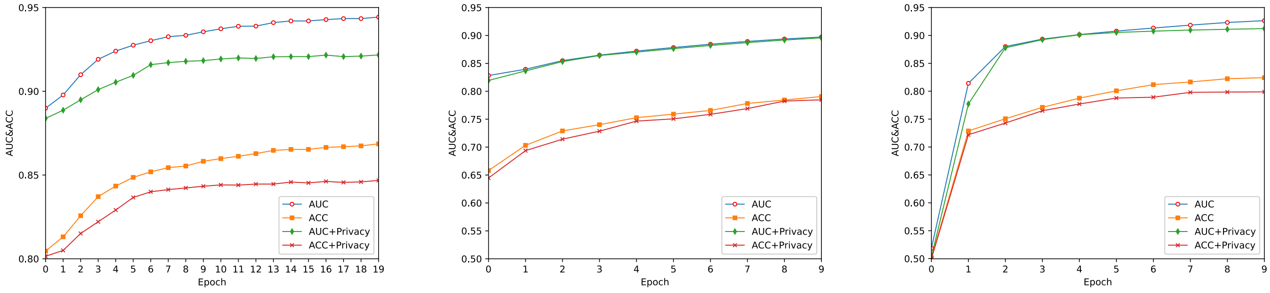
B. EXPERIMENTS SETUP

The above three datasets have explicit feedback, including user ratings and personal information. In our model, explicit feedback is transformed into implicit feedback, which can improve the prediction accuracy of recommendation system effectively. In three datasets, the score which is greater than or equal to 3 can be marked with 1 and else is 0. For MovieLens-1M, the threshold for positive evaluation is 4, while for Book-Crossing and Last.FM, thresholds are not set due to their sparsity.

C. EVALUATION METRICS

In click-through rate prediction scenarios, we use Area Under the ROC Curve (AUC) and accuracy (ACC) to evaluate the performance of prediction. AUC is a model evaluation index. The value of AUC is equal to the area formed by the curve and the False Positive Rate (FPR) axis. As a probability value, AUC can directly evaluate the quality of a classifier. A larger AUC value means that the current classification algorithm

[1] https://grouplens.org/datasets/movielens/
[2] http://www2.informatik.uni-freiburg.de/ cziegler/BX/
[3] http://millionsongdataset.com/lastfm/



(a) MovieLens-1M Dataset.

(b) Book-Crossing Dataset.

(c) Last.FM Dataset.

FIGURE 2. Effect of AUC and ACC on three datasets when $\varepsilon = 1$.

can classify more accurately. The evaluation index AUC is defined as follows:

$$\mathrm{AUC} = \frac{\sum_{i \in \mathrm{PositiveClass}} rank_i - \frac{M(1+M)}{2}}{M \times N} \tag{15}$$

where M is the number of positive class samples and N is the number of negative class samples. In the sample combination, the score of a positive sample is always larger than that of a negative sample, and the rank value in the formula represents the number of combinations that can produce such score.

In top-N recommendation scenarios, prediction accuracy is generally measured by precision/recall@N. Given a list of top-N predicted items for a user, denoted $\widehat{R}_{1:N}(u)$ and a list of user behaviors on test sets, denoted $R(u)$. Then the precision/recall@N of the recommendation results are defined as:

$$\mathrm{Precision@N} = \frac{|R(u) \cap \widehat{R}_{1:N}(u)|}{N} \tag{16}$$

$$\mathrm{Recall@N} = \frac{|R(u) \cap \widehat{R}_{1:N}(u)|}{|R(u)|} \tag{17}$$

Another application scenario of recommendation system is score recommendation. The error of score recommendation is usually calculated by RMSE (Root Mean Square Error). RMSE is defined as:

$$\mathrm{RMSE} = \frac{\sqrt{\sum_{t=1}^{n} (\widehat{y}_t - y_t)^2}}{n} \tag{18}$$

where $\widehat{y}_t$ is the prediction score, y_t is the real score and n denotes the number of samples. RMSE measured errors between the real score and the prediction [39], which can reflect the precision of prediction results effectively. The smaller RMSE represents the smaller prediction error and the better performance of the recommendation system.

D. EXPERIMENT RESULTS

To compare the intensity of differential privacy and its impact on the prediction accuracy of recommendation systems, we take different values for privacy budget in experiments. In the definition of differential privacy, the parameters ε refers to the privacy budget [40] and controls the level of privacy guarantee. A smaller ε represents a stronger privacy level. In order to deviate from the test data and evaluate the model better, we use AUC/ACC and precision/recall@N to evaluate our algorithm at the same time.

Furthermore, it can be noted that privacy requirements inevitably degrade the performance of recommendation system, but knowledge graph as auxiliary information increases the accuracy and diversity of recommendation results. The noise added to the multi-task recommendation system in this paper is determined by the parameter ε. In our experiment, we investigate the effect of adding noise on the original model in two recommended scenarios, and select the appropriate evaluation index according to the different scenarios. ACC/AUC and precision/recall@N are used to evaluate the click-through rate prediction scenario and the top-N recommendation scenarios, respectively. We also empirically show the relationship between the value of the click-through rate and different ε values with respect to the number of iterations.

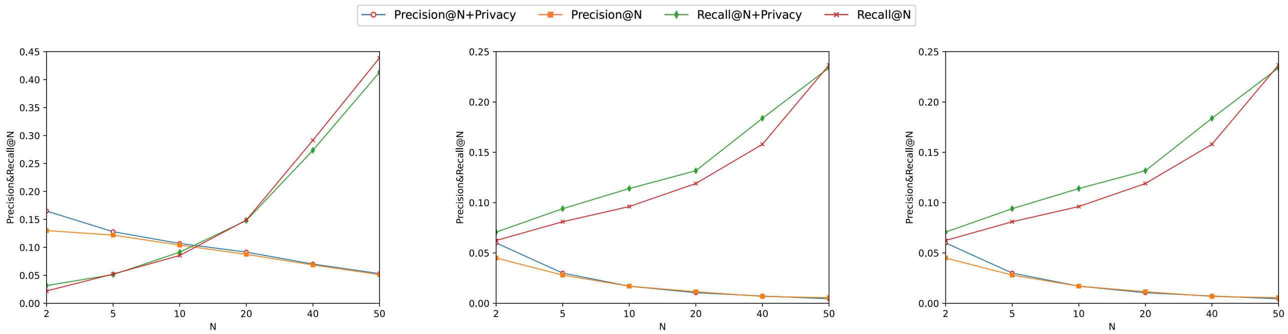
1) EVALUATION OF CLICK-THROUGH RATE PREDICTION

In the click-through rate prediction, we use the Laplacian noise training model to test each interaction in the dataset and output the predicted click rate. In Figure 2, we set the privacy budget $\varepsilon = 1$, and draw functional images based on the performance of three datasets and iterations of multitask learning. Figure 2 shows the effect of adding Laplacian noise on the click-through rate prediction of multi-task recommendation system. Our model is executed under the ε-differential privacy. Obviously, the accuracy decreases on all three datasets.

Table 3 is the decreasing amplitude of AUC and ACC on three datasets in our experiments. When the privacy budget $\varepsilon = 1$, the accuracy after adding Laplacian noise decreases by 1.362% in the Last.FM dataset, 0.99% in the Book-Crossing dataset and 1.585% in the MovieLens dataset respectively. In this experiment, the same amount of noise is added to coefficients of the objective function. A smaller value of ε achieves stronger privacy protection for sensitive information, and the accuracy of the model is worse, which is due to the fact that more noise is added.

2) EVALUATION OF TOP-N RECOMMENDATION

In the Top-N recommendation scenario, we train the privacy-preserving multi-task recommendation model ($\varepsilon = 1$) and the

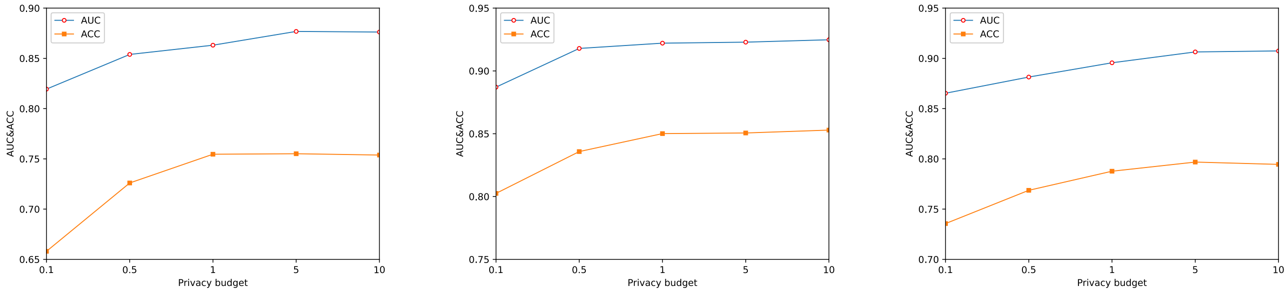


(a) MovieLens-1M Dataset. (b) Book-Crossing Dataset. (c) Last.FM Dataset.

FIGURE 3. Effect of precision/recall@N on three datasets when $\varepsilon = 1$.

TABLE 3. Decreasing amplitude of AUC and ACC on three datasets when $\varepsilon = 1$.

Dataset	MovieLens-1M		Book-Crossing		Last.FM	
	AUC	ACC	AUC	ACC	AUC	ACC
The average of AUC&ACC	0.93069	0.85205	0.87022	0.74611	0.85871	0.76155
	0.91292	0.83646	0.86172	0.73988	0.85879	0.74793
Decreasing amplitude	1.777%	1.5559%	0.85%	0.993%	0.892%	1.362%



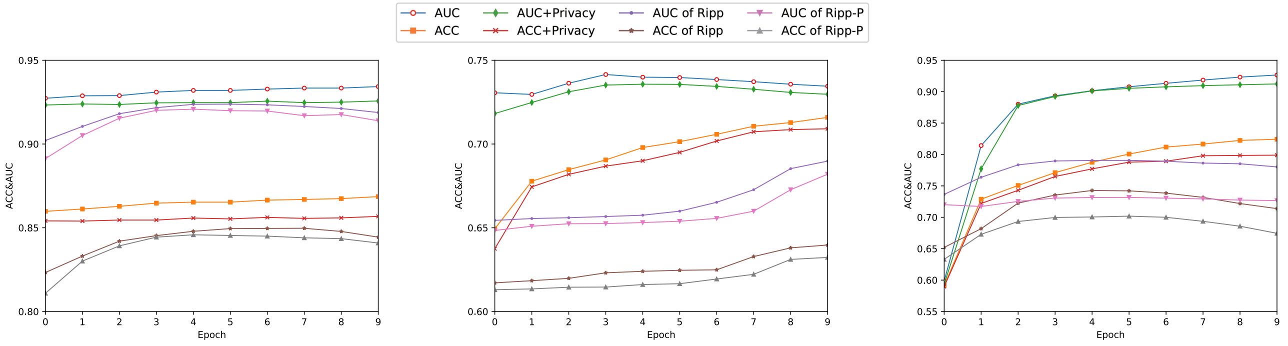
(a) Effect on the Book-Crossing Dataset. (b) Effect on the Last.FM Dataset. (c) Effect on the MovieLens-1M Dataset.

FIGURE 4. The effect of different privacy budgets on AUC and ACC on three datasets.

multi-task recommendation model without privacy preservation respectively. According to the user's behavior on the training set, we predict N items with the highest click probability for each user in the test set. We choose precision/recall@N to compare and evaluate the recommendation effect. Figure 3 shows how precision/recall@N change as N increases on the three real datasets [41]. From figure 3, it can be seen that the curve of precision@N and recall@N shows the opposite trend. On the three datasets, the precision/recall@20 converge faster, reaching more than 50% of their maximum value. In addition, for the training time of the top-N recommended scenario, with the increase of the number of users, the elapsed time to calculate top-N relevance users will increase significantly. Compared with the multi-task recommendation model without privacy preservation, the experimental results of the proposed model show that the difference values of precision/recall@N on the three datasets are less than 2.56%, 2.58% and 1.91% respectively.

3) PRIVACY-ACCURACY TRADE-OFF

Recall that a smaller ε leads to more noise but stronger privacy [42]. We can also draw this conclusion from Figure 4. In Figure 4, to compare the intensity of differential privacy and the impact on the prediction accuracy of the recommendation system, we set different values of privacy budget in this experiment. We include $\varepsilon = \{0.1, 0.5, 1, 5, 10\}$ to see how much accuracy was lost due to Laplacian privacy noise. Figure 4 shows the performance comparison of our model with different values of the privacy budget ε. We also conducted experiments on the above three datasets. The parameter settings are the same as the experimental settings provided in Section 4.2. When we vary privacy budget in the set of $\{0.1, 0.5, 1, 5, 10\}$, the accuracy of the model drops with the decrease of ε. However, when the private budget is larger than 1, the accuracy remains stable at about 90% in the MovieLens dataset, at about 75% in the Last.FM and the Book-Crossing dataset, and then slightly decreases. Overall,



(a) MovieLens-1M Dataset.

(b) Book-Crossing Dataset.

(c) Last.FM Dataset.

FIGURE 5. Comparison of ACC and AUC for three datasets when $\varepsilon = 1$.

TABLE 4. The result of RMSE on multiple epoch for three datasets when $\varepsilon = 1$.

Epoch		0	2	4	6	8
MovieLens-1M	RS	0.5320	0.4871	0.4959	0.4447	0.4244
	RS+KG	0.5206(-1.14%)	0.4783(-0.88%)	0.4237(-7.22%)	0.3589(-8.58%)	0.3608(-6.36%)
Book-Crossing	RS	0.5223	0.5207	0.5205	0.5232	0.5260
	RS+KG	0.5069(-1.54%)	0.4853(-3.54%)	0.4652(-5.53%)	0.4469(-7.66%)	0.4891(-3.69%)
Last.FM	RS	0.6535	0.6830	0.6931	0.6630	0.6839
	RS+KG	0.5825(-7.10%)	0.5735(-10.95%)	0.5826(-11.05%)	0.5786(-8.44%)	0.5683(-11.56%)

the results of experiments show that adding Laplacian noise has little effect on the accuracy of multi-task recommendation system in our method.

E. COMPARISON

We first compare our method with another multi-task-privacy-preserving method to verify the effectiveness of our framework. In order to investigate whether the knowledge graph module enhances the privacy-preserving recommendation system, we also train the privacy-preserving recommendation system module independently and compare the results with the alternative training multi-task model.

1) COMPARISON WITH BASELINES

We compared our approach with a recently proposed multi-task recommendation approach: RippleNet [20]. Although this approach was not designed specially for the multi-task privacy-preserving recommendation system, it seems to be the closest method in the current literature on the aspect of the application scenarios and practical operations.

Different from the alternative training in this paper, RippleNet is a joint training network of knowledge graph enhanced recommendation system. It simulates a spreading process of user's interest in knowledge graph: user's interest is centered on its historical records, spreads out layer by layer through the knowledge graph and decays continuously in the spreading process. We adapt RippleNet to differential privacy setting and show the results on three datasets. The comparison result of ACC and AUC on three datasets is shown in Figure 5, where RippleNet-P denotes RippleNet with privacy preservation. Specifically, our method outperforms the baseline by 0.99% to 4.32%, 2.45% to 8.51%, 4.91% to 12.44% on ACC in movie, book, and music recommendation, respectively.

As can be seen from Figure 5, our method achieves better ACC and AUC than RippleNet and particularly has the advantages in sparse scenarios. RippleNet preforms best in the movie recommendation. Figure 4 shows the little gap between Ripple and our method in ACC on the MovieLens dataset. In the experiments, RippleNet is more sensitive to the density of datasets so that it can capture users' information better when the user-item interaction is intensive. After adding noise, this feature can still be retained. In the book and music recommendation scenarios, our method can still maintain a decent performance even when the user-item interaction is more sparse.

2) RESULTS ON THE ENHANCEMENT OF KNOWLEDGE GRAPH

The aim of the proposed multi-task model is to use the auxiliary information of knowledge graph to assist privacy-preserving recommendation system maintain a good prediction accuracy. Therefore, it is necessary to verify whether the knowledge graph task can enhance the privacy-preserving recommendation system in the experiment. We use RMSE to evaluate the root mean square error between the predicted and real scores of the recommendation system output.

Table 4 shows the RMSE results of the independent training recommendation task and the alternative training knowledge graph task when the privacy budget is 1. "RS" represents the single recommendation task of independent training and "RS+KG" represents the multi-task model of alternative training with knowledge graph. In Table 4, we select the results of 5 epoch from a large number of experiments to illustrate. We found that the method of alternative training multi-task model can reduce the prediction RMSE of the recommendation system by 0.88% - 11.56%. The results show that the knowledge graph can improve the recommendation performance for the privacy-preserving recommendation system as an auxiliary task.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we aim to protect sensitive data in recommendation system and enhance prediction accuracy of multi-task recommendation system. We propose a novel framework for privacy-preserving multi-task knowledge graph enhanced recommendation, which explores Laplacian mechanism for differential privacy in the recommendation task. As an auxiliary task, knowledge graph utilizes entities of triads corresponding to items in recommendation systems, which provides the latent feature embeddings and interacts with the recommendation system. We not only compare the accuracy of noise-added training and original training on three datasets, but also contrast the impact of different privacy budget on the prediction accuracy. Experiments on three datasets commonly used in recommendation systems show that our method can preserve privacy of the multi-task recommendation systems, and the effect of adding noise on accuracy is controlled at about 1 to 2 percent.

For future work, we will explore more effective privacy-preserving model, and further promote the performance of multi-task recommendation system.

ACKNOWLEDGMENT

The authors wish to thank the editors and anonymous reviewers for their valuable comments and helpful suggestions which greatly improved the articles quality. This work was supported by the Key research and development program of Shaanxi Province (Grant no. 2019ZDLGY17-01, 2019GY-042).

REFERENCES

[1] P. Kumar and R. S. Thakur, "Recommendation system techniques and related issues: A survey," *Int. J. Inf. Technol.*, vol. 10, no. 1, pp. 1–7, 2018.

[2] C. Guo, M. Zhang, Y. Liu, and S. Ma, "A picture is worth a thousand words: Introducing visual similarity into recommendation," in *Proc. 7th Int. Conf. Intell. Control Inf. Process. (ICICIP)*, Siem Reap, Cambodia, Dec. 2016, pp. 153–160.

[3] H. Wang, W. U. Xiang, Y. U. Xiao, and H. U. Junfeng, "Differential privacy protection for topn recommendation system," *China Sci.*, vol. 12, no. 20, pp. 2326–2330, 2017.

[4] G. Yang, Q. Yang, and H. Jin, "A novel trust recommendation model for mobile social network based on user motivation," *Electron. Commerce Res.*, Apr. 2019.

[5] E. Terra and C. L. A. Clarke, "Scoring missing terms in information retrieval tasks," in *Proc. 13th ACM Conf. Inf. Knowl. Manage. (CIKM)*, Washington, DC, USA, 2004, pp. 50–58.

[6] K. Liu, N. Uplavikar, W. Jiang, and Y. Fu, "Privacy-preserving multi-task learning," in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, Singapore, Nov. 2018, pp. 1128–1133.

[7] S. P. Borgatti, M. G. Everett, and J. C. Johnson, *Analyzing Social Networks*. London, U.K.: Sage, 2018.

[8] R. Pratt, R. L. Oakley, D. Wynn, and O. Lopez, "Examining the impact of user personality traits on concern for information privacy of personal health information," in *Proc. 25th Amer. Conf. Inf. Syst. (AMCIS)*, Cancún, México, 2019, p. 1.

[9] X. He and X. Jin, "Collaborative filtering recommendation algorithm considering users' preferences for item attributes," in *Proc. 2nd IEEE Int. Conf. Big Data Comput. Intell. (ICBDCI)*, Porto, Portugal, Feb. 2019, pp. 1–6.

[10] S. Nath, M. Goraczko, J. Liu, and A. Mirhoseini, "Optimizing task recommendations in context-aware mobile crowdsourcing," U.S. Patent 9 911 088 B2, Mar. 6, 2018.

[11] H. Paulheim, "Knowledge graph refinement: A survey of approaches and evaluation methods," *Semantic Web*, vol. 8, no. 3, pp. 489–508, 2017.

[12] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.

[13] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," in *Proc. 22nd Int. Conf. Data Eng. (ICDE)*, Atlanta, GA, USA, 2006, p. 24.

[14] N. Li, T. Li, and S. Venkatasubramanian, "T-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Istanbul, Turkey, Apr. 2007, pp. 106–115.

[15] C. Dwork and G. N. Rothblum, "Concentrated differential privacy," *CoRR*, vol. abs/1603.01887, Mar. 2016.

[16] Q. Geng, W. Ding, R. Guo, and S. Kumar, "Truncated Laplacian mechanism for approximate differential privacy," *CoRR*, vol. abs/1810.00877, Oct. 2018.

[17] S. Wang, R. Sinnott, and S. Nepal, "Privacy-protected statistics publication over social media user trajectory streams," *Future Gener. Comput. Syst.*, vol. 87, pp. 792–802, Oct. 2018.

[18] A. Boutet, D. Frey, R. Guerraoui, A. Jégou, and A.-M. Kermarrec, "Privacy-preserving distributed collaborative filtering," *Computing*, vol. 98, no. 8, pp. 827–846, Aug. 2016.

[19] A. Berlioz, A. Friedman, M. A. Kaafar, R. Boreli, and S. Berkovsky, "Applying differential privacy to matrix factorization," in *Proc. 9th ACM Conf. Rec. Syst. (RecSys)*, Vienna, Austria, 2015, pp. 107–114.

[20] H. Wang, F. Zhang, J. Wang, M. Zhao, W. Li, X. Xie, and M. Guo, "RippleNet: Propagating user preferences on the knowledge graph for recommender systems," in *Proc. 27th ACM Int. Conf. Inf. Knowl. Manage.*, Turin, Italy, Oct. 2018, pp. 417–426.

[21] H. Wang, F. Zhang, X. Xie, and M. Guo, "DKN: Deep knowledge-aware network for news recommendation," in *Proc. World Wide Web Conf. (WWW)*, Lyon, France, 2018, pp. 1835–1844.

[22] X. Yu, X. Ren, Y. Sun, Q. Gu, B. Sturt, U. Khandelwal, B. Norick, and J. Han, "Personalized entity recommendation: A heterogeneous information network approach," in *Proc. 7th ACM Int. Conf. Web Search Data Mining*, New York, NY, USA, 2014, pp. 283–292.

[23] H. Wang, F. Zhang, M. Zhao, W. Li, X. Xie, and M. Guo, "Multi-task feature learning for knowledge graph enhanced recommendation," in *Proc. World Wide Web Conf. (WWW)*, San Francisco, CA, USA, 2019, pp. 2000–2010.

[24] C. Dwork, "Differential privacy: A survey of results," in *Proc. 5th Int. Conf. Theory Appl. Models Comput., (TAMC)*, Xi'an, China, 2008, pp. 1–19.

[25] S. K. Gupta, S. Rana, and S. Venkatesh, "Differentially private multi-task learning," in *Proc. IEEE Conf. Intell. Secur. Inform. (ISI)*, Tucson, AZ, USA, 2016, pp. 101–113.

[26] L. Xie, I. M. Baytas, K. Lin, and J. Zhou, "Privacy-preserving distributed multi-task learning with asynchronous updates," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Halifax, NS, Canada, Aug. 2017, pp. 1195–1204.

[27] A. D. Sarwate and K. Chaudhuri, "Signal processing and machine learning with differential privacy: Algorithms and challenges for continuous data," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 86–94, Sep. 2013.

[28] J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V. Shmatikov, "'You might also like': Privacy risks of collaborative filtering," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Oakland, CA, USA, May 2011, pp. 231–246.

[29] A. Friedman, S. Berkovsky, and M. A. Kaafar, "A differential privacy framework for matrix factorization recommender systems," *User Model. User-Adapted Interact.*, vol. 26, no. 5, pp. 425–458, Dec. 2016.

[30] X. Liu, A. Liu, X. Zhang, Z. Li, G. Liu, L. Zhao, and X. Zhou, "When differential privacy meets randomized perturbation: A hybrid approach for privacy-preserving recommender system," in *Database Systems for Advanced Applications*, S. Candan, L. Chen, T. B. Pedersen, L. Chang, and W. Hua, Eds. Suzhou, China: Springer, 2017, pp. 576–591.

[31] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. 3rd Theory Cryptogr. Conf. (TCC)*, S. Halevi and T. Rabin, Eds., New York, NY, USA, 2006, pp. 265–284.

[32] US Preventive Services Task Force, "Screening for colorectal cancer: Us preventive services task force recommendation statement," *Ann. Internal Med.*, vol. 149, no. 9, p. 627, 2008.

[33] X. Wang, X. He, Y. Cao, M. Liu, and T.-S. Chua, "KGAT: Knowledge graph attention network for recommendation," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Anchorage, AK, USA, Jul. 2019, pp. 950–958.

[34] H. Wang, F. Zhang, J. Wang, M. Zhao, W. Li, X. Xie, and M. Guo, "Exploring high-order user preference on the knowledge graph for recommender systems," *ACM Trans. Inf. Syst.*, vol. 37, no. 3, pp. 32:1–32:26, 2019.

[35] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, "Distributed representations of words and phrases and their compositionality," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 26, Oct. 2013, pp. 3111–3119.

[36] F. M. Harper and J. A. Konstan, "The movielens datasets: History and context," *ACM Trans. Interact. Intell. Syst.*, vol. 5, no. 4, p. 19, Jan. 2016.

[37] B. Rampton, *Crossing: Language and Ethnicity Among Adolescents*. Manchester, U.K.: St. Jerome Pub., 2005.

[38] E. Çano and M. Morisio, "Music mood dataset creation based on last.fm tags," in *Proc. Int. Conf. Artif. Intell. Appl.*, Vienna, Austria, 2017, pp. 1–12.

[39] T. Chai and R. R. Draxler, "Root mean square error (RMSE) or mean absolute error (MAE)?—Arguments against avoiding RMSE in the literature," *Geosci. Model Develop.*, vol. 7, no. 3, pp. 1247–1250, 2014.

[40] F. Liu, "Generalized Gaussian mechanism for differential privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 4, pp. 747–756, Apr. 2019.

[41] R. Devooght and H. Bersini, "Long and short-term recommendations with recurrent neural networks," in *Proc. 25th Conf. User Modeling, Adaptation Personalization (UMAP)*, Bratislava, Slovakia, Jul. 2017, pp. 13–21.

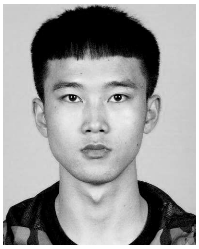
[42] Z. Jorgensen and T. Yu, "A privacy-preserving framework for personalized, social recommendations," in *Proc. 17th Int. Conf. Extending Database Technol. (EDBT)*, Athens, Greece, 2014, pp. 1–12.

BIN YU was born in 1964. He received the Ph.D. degree in computer software and theory from Northwest University, Xi'an, China, in 2003. He is currently a Full Professor with the School of Computer Science and Technology. His research interests include software theory, artificial intelligence, and information security.

CHENYU ZHOU was born in 1997. She received the B.E. degree in computer science and technology from Xidian University, Xi'an, China, in 2019, where she is currently pursuing the M.S. degree in computer science and technology. Her research interests include deep learning and privacy preserving.

CHEN ZHANG was born in 1981. She received the Ph.D. degree in computer application technology from Xidian University, Xi'an, China, in 2012. She is currently a Lecturer with the School of Computer Science and Technology. Her research interests include formal verification of software systems, model checking, and software theory.

GUODONG WANG was born in 1993. He is currently pursuing the M.S. degree in computer science and technology with Xidian University, Xi'an, China. His research interests include network representation learning and privacy preserving.



YIMING FAN was born in 1996. He is currently pursuing the M.S. degree in computer science and technology with Xidian University, Xi'an, China. His research interests include network representation learning and privacy preserving.

• • •