Deferentially Private Tagging Recommendation Based on Topic Model

Tianqing Zhu, Gang Li*, Wanlei Zhou, Ping Xiong, and Cao Yuan

School of Information Technology, Deakin University, Australia
School of Information, Zhongnan University of Economics and Law, China
School of Mathematics and Computer, Wuhan Polytechnic University, China
tianqing.e.zhu@gmail.com, {gang.li,wanlei.zhou}@deakin.edu.au,
pingxiong@znufe.edu.cn, yc@whpu.edu.cn

Abstract. *Tagging recommender system* allows Internet users to annotate resources with personalized tags and provides users the freedom to obtain recommendations. However, It is usually confronted with serious privacy concerns, because adversaries may re-identify a user and her/his sensitive tags with only a little background information. This paper proposes a privacy preserving tagging release algorithm, *PriTop*, which is designed to protect users under the notion of *differential privacy*. The proposed *PriTop* algorithm includes three privacy preserving operations: *Private Topic Model Generation* structures the uncontrolled tags, *Private Weight Perturbation* adds *Laplace* noise into the weights to hide the numbers of tags; while *Private Tag Selection* finally finds the most suitable replacement tags for the original tags. We present extensive experimental results on four real world datasets and results suggest the proposed *PriTop* algorithm can successfully retain the utility of the datasets while preserving privacy.

Keywords: Privacy Preserving, Differential Privacy, Recommendation, Tagging.

1 Introduction

The widespread success of social network web sites introduces a new concept called the *tagging recommender system* [9]. These social network web sites usually enable users to annotate resources with customized tags, which in turn facilitates the recommendation of resources. But the issue of privacy in the recommender process has generally been overlooked [11]. An adversary with background information may re-identify a particular user in a tagging dataset and obtain the user's historical tagging records [8]. How to preserve privacy in tagging recommender systems is an emerging issue that needs to be addressed.

Over the last decade, a variety of privacy preserving approaches have been proposed for traditional recommender systems [11]. For example, *cryptography* is used in the rating data for multi-party data sharing [15]. *Perturbation* adds noise

* Corresponding author.

V.S. Tseng et al. (Eds.): PAKDD 2014, Part I, LNAI 8443, pp. 557–568, 2014.

to the users' ratings before rating prediction [12], and *obfuscation* replaces a certain percentage of ratings with random values [1]. However, these approaches can hardly be applied in tagging recommender systems due to the semantic property of tags. To overcome the deficiency, the *tag suppression* method has recently been proposed to protect a user's privacy by modeling users' profiles and eliminating selected sensitive tags [11]. However, this method only releases an incomplete dataset that significantly affects the recommendation performance. Moreover, most existing approaches suffer from one common weakness: the privacy notions are weak and hard to prove theoretically, thus impairing the credibility of the final results. Accordingly, a more rigid privacy notion is needed.

Recently, *differential privacy* provides a strict privacy guarantee for individuals [6]. It applies a randomized mechanism suitable for both numeric and non-numeric values and has been proven effective in recommender systems [16,17]. This paper introduces *differential privacy* into tagging recommender systems, with the aim of preventing re-identification of users and avoiding the association of sensitive tags (e.g., healthcare tags) with a particular user. However, although these characteristics make *differential privacy* a promising method for tagging recommendation, there remain some barriers: First, the naive *differential privacy* mechanism only focuses on releasing statistical information that can barely retain the structure of the tagging dataset. this naive mechanism lists all the tags, counts the number and adds noise to the statistical output, but ignores the relationship among users, resources and tags. This simple statistical information is inadequate for recommendations; Second, Differential privacy introduces a large amount of noise due to the sparsity of the tagging dataset. For a dataset with millions of tags, the mechanism will result in a large magnitude of noise.

Both barriers imply the naive *differential privacy* mechanism can not be simply applied in tagging recommender systems. To overcome the first barrier, we generate a synthetic dataset retaining the relationship among tags, resources and users rather than releasing statistical information. The second barrier can be addressed by shrinking the randomized domain, because the noise will decrease when the randomized range is limited. The topic model method is a possible way to structure tags into groups and limit the randomized domain. Therefore, we propose a tailored *differential privacy* mechanism that optimizes the performance of recommendation with a fixed level of privacy. The contributions can be summarized as follows:

- We maintain an acceptable utility of the tagging dataset by designing a practical private tagging release algorithm, *PriTop*, with a rigid privacy guarantee.
- In *PriTop*, a novel private topic model-based method is proposed to structure the tags and to shrink the randomized domain. The effectiveness of the proposed method is verified by extensive experiments on real-world datasets.
- With *differential privacy* composition properties, a theoretical privacy and utility analysis confirms an improved trade-off between privacy and utility.

2 Preliminaries and Related Work

Let G be a dataset to be protected, two datasets G and G' are *neighboring datasets* if they differ in only one record. *Differential privacy* provides a randomization mechanism $\mathcal{M}$ to mask the difference between the *neighboring datasets* [6]. We use $\widehat{G}$ to represent the synthetic dataset after applying $\mathcal{M}$.

In tagging recommendation, dataset G contains users $U = \{u_1, u_2, \cdots\}$, resources $R = \{r_1, r_2, \cdots\}$ and tags $T = \{t_1, t_2, \cdots\}$. For a particular user $u_a \in U$ and a resource $r_b \in R$, $T(u_a, r_b)$ represents all tags flagged by the u_a on r_b, and use $T(u_a)$ to denote all tags utilized by u_a. The recommended tags for u_a on a given resource r are represented by $T^p(u_a, r)$. A user u_a's profile $P(u_a) =< T(u_a), W(u_a) >$ is usually modeled by his tagging records, including tag's names $T(u_a) = \{t_1, ..., t_{|T(u_a)|}\}$ and weights $W(u_a) = \{w_1, ..., w_{|T(u_a)|}\}$ [11].

Differential privacy acquires the intuition that releasing an aggregated report should not reveal too much information about any individual in the dataset [6].

Definition 1 (ϵ-*Differential Privacy*). *A randomized mechanism $\mathcal{M}$ gives* ϵ-differential privacy *if for every set of outcomes Ω, $\mathcal{M}$ satisfies: $Pr[\mathcal{M}(G) \in \Omega] \leq \exp(\epsilon) \cdot Pr[\mathcal{M}(G') \in \Omega]$, where ϵ is the privacy budget.*

$\mathcal{M}$ is associated with the *sensitivity* [7], which measures the maximal change of the query f when removing one record from G.

Definition 2 (*Sensitivity*). *For $f : G \to \mathbb{R}$, the* sensitivity *of f is defined as $\Delta f = \max_{G,G'} ||f(G) - f(G')||_1$,*

Two mechanisms are utilized in *differential privacy*: the *Laplace* mechanism and the *Exponential* mechanism. The *Laplace* mechanism is suitable for numeric output and adds controlled noise to the outcome of a query [7]:

Definition 3 (*Laplace* Mechanism). *Given a function $f : G \to \mathbb{R}^d$, the mechanism, $\mathcal{M}(R) = f(R) + Laplace(\frac{\Delta f}{\epsilon})^d$, provides the* ϵ-differential privacy.

The *Exponential* mechanism focuses on non-numeric queries and pairs with an application dependent *score function* $q(G, \psi)$, which represents how good an output scheme ψ is for dataset G:

Definition 4 (*Exponential* Mechanism). *[10] An Exponential mechanism $\mathcal{M}$ is* ϵ-differential privacy *if: $\mathcal{M}(G) = \{return\ \psi \propto \exp(\frac{\epsilon q(G,\psi)}{2\Delta q})\}$.*

Privacy violations in recommender systems have been well studied since 2001. The first study concerned with this issue was undertaken by Ramakrishnan et al. [13]. They claimed users who rated items across disjointed domains could face a privacy risk through statistical database queries. Recently, Calandrino et al. [4] presented a more serious privacy violation. By observing temporal changes in the public outputs of a recommender system, they inferred a particular user's historical rating and behavior with background information.

Several traditional privacy preserving methods have been employed in CF, including *cryptographic* [5,15], *perturbation* [12] and *obfuscation* [1]. *Cryptographic*

is suitable for multiple parties but induces extra computational cost [5,15]; *Obfuscation* is easy to understand and to implement, but the utility will decrease significantly [1]. *Perturbation* preserves high level of privacy by adding noise to the original dataset, but the magnitude of noise is hard to control [12].

The privacy in tagging recommendation systems is more complicated due to its unique structure and semantic content. Parra-Arnau et al. [11] proposed the *tag suppression* by eliminating sensitive tags from users' profile. They applied a clustering method to structure tags and suppressed the less represented ones. This approach only releases an incomplete dataset, and sensitive tags are subjective. When publicly sharing the dataset, users still have the potential to be identified. The privacy issue in tagging recommender systems remains largely unexplored, and we attempt to fill this void in this paper.

3 Private Tagging Release

In a tagging dataset G, users' profile is represented as $\mathbf{P} = \{P(u_1), ..., P(u_{|U|})\}$. *Differential privacy* assumes all tags have probabilities to appear in $P(u_a)$. Suppose tags in $P(u_a)$ are represented by $T(u) = \{t_1, ..., t_{|T|}\}$ and weights are denoted as $W(u_a) = \{w_1, ..., w_{|T|}\}$, where $w_i = 0$ indicates that t_i is unused. *Differential privacy* will add noise to the weight $W(u_a)$ and release a noisy profile $\widehat{P}(u_a) =< T(u_a), \widehat{W}(u_a) >$. However, this process will introduce large noise because lots of weights will change from zero to a positive value. To reduce the noise is to shrink the randomized domain, which refers to the diminished number of zero weights in the profile. Accordingly, we structure the tags into K *topics* $Z = \{z_1, ...z_K\}$ and define a *topic-based* profile $P_z(u_a) =< T_z(u_a), W_z(u_a) >$, where $T_z(u_a) = \{T_{z_1}(u_a), ..., T_{z_K}(u_a)\}$ represents tags in each topic and $W_z(u_a) = \{w_{z_1}(u_a), ..., w_{z_K}(u_a)\}$ is the frequency of tags. Compared to $W(u_a)$, $W_z(u_a)$ is less sparse. The total noise added will significantly diminish.

In this section, we propose a ***Pri**vate **Top**ic-based Tagging Release* (PriTop) algorithm to publish users' profiles by masking their exact tags and weights under *differential privacy*. As described in Alg. 1, three private operations are involved: *Private Topic Model Generation* creates multiple private topics by masking the topic distribution on tags. *Topic Weight Perturbation* masks the weights of tags to prevent inferring how many tags a user has annotated on a topic. *Private Tag Selection* uses privately selected tags replace the original tags.

3.1 Private Topic Model Generation

This operation categorizes tags into topics to eliminate the randomization domain. We introduce *differential privacy* to *Latent Dirichlet Allocation* (LDA) [2] to generate a private LDA model, which is constructed in three steps: *LDA Model Construction*, *Private Model Generation* and *Topic-based Profile Generation*.

LDA Model Construction. The first step constructs the LDA model by *Gibbs Sampling* [14]. In this model, a resource is considered as a document and a tag is

Algorithm 1. *Private Topic-based Tagging Release (PriTop)* Algorithm

Require: G, privacy parameter ϵ, K.
Ensure: $\widehat{G}$
1. Divided privacy budget into $\epsilon/2$, $\epsilon/4$ and $\epsilon/4$;
2. *Private Topic Generation*: create topic-based user profiles $P(u_a)$ based on the private topic model with $\epsilon/2$ privacy budget;
for each user u_a **do**
3. *Topic Weight Perturbation*: add *Laplace* noise to the weights with $\epsilon/4$;
for each topic z_k in $P(u_a)$ **do**
4. *Private Tag Selection*: Select tags according to the $\widehat{W}(u_a)$ with $\epsilon/4$;
end for
end for
5. Output $\widehat{G}$ for tagging recommendations;

interpreted as a word. Let $Z = \{z_1, ...z_K\}$ be a group of topics, Eq. 1 represents a standard LDA model to specify the distribution over tag t.

$$Pr(t|r) = \sum_{l=1}^{K} Pr(t|z_l)Pr(z_l|r) \tag{1}$$

where $Pr(t|z_l)$ is the probability of tag t under a topic z_l and $Pr(z_l|r)$ is the probability of sampling a tag from topic z in the resource r.

To estimate topic-tag distribution $Pr(t|z)$ and the resource-topic distribution $Pr(z|r)$ in Eq. 1, *Gibbs Sampling* iterates multiple times over each tag t of resource r and samples the new topic z for the tag based on the posterior probability $Pr(z|t_i, r, Z_{-i})$ by Eq. 2 until the model converges.

$$Pr(z|t_i, r, Z_{-i}) \propto \frac{C_{tK}^{TK} + \beta}{\sum_{t_i}^{|T|} C_{t_iK}^{TK} + |T|\beta} \frac{C_{rk}^{RK} + \alpha}{\sum_{K=1}^{K} C_{r_iK}^{RK} + K\alpha} \tag{2}$$

where C^{TK} is the count of topic-tag assignments and C^{RK} counts the resource-topic assignments. Z_{-i} represents topic-tag assignment and resource-topic assignment except the current z for t_i. α and β are parameters of Dirichlet priors. Simultaneously, the evaluation on $Pr(t|z)$ and $Pr(z|r)$ is formulated as follows:

$$Pr(t|z) = \frac{C_{tk}^{TK} + \beta}{\sum_{t_i}^{|T|} C_{t_iK}^{TK} + |T|\beta}, Pr(z|r) = \frac{C_{rK}^{RK} + \alpha}{\sum_{k=1}^{K} C_{r_iK}^{RK} + K\alpha}$$

After converging, the LDA model is generated by $Pr(z|t, r)$, $P(t|z)$ and $P(z|r)$.

Private Model Generation. The second step adds *Laplace* noise to the final counts in the LDA model. There are four difference counts in Eq. 2. If we changed the topic assignment on current t_i, the C_{tK}^{TK} will decrease by 1 and $\sum_{t_i}^{|T|} C_{t_iK}^{TK}$ will increase by one. Similarly, if the C_{rK}^{RK} decreases by 1, the $\sum_{K=1}^{K} C_{r_iK}^{RK}$ will

increase by 1 accordingly. So we sample two groups of *Laplace* noise and add them to four count parameters. The new $\widehat{Pr}(z|t,r)$ is evaluated by Eq. 3:

$$\widehat{Pr}(z|t,r) \propto \frac{C_{tK}^{TK} + \eta_1 + \beta}{\sum_{t_i}^{|T|} C_{t_iK}^{TK} - \eta_1 + |T|\beta} \frac{C_{rK}^{RK} + \eta_2 + \alpha}{\sum_{K=1}^{K} C_{r_ik}^{RK} - \eta_2 + K\alpha} \tag{3}$$

where η_1 and η_2 are both sampled from $Laplace(\frac{2}{\epsilon})$ with the *sensitivity* as 1.

Topic-based Profile Generation. The third step creates topic-based user profiles. For each user with tags $T(u_a) = \{t_1, ..., t_{|T(u_a)|}\}$ and related resources $R(u_a) = \{r_1, ..., r_{|R(u_a)|}\}$, each tag can be assigned to a particular topic $z_l \in Z$ according to the $\widehat{Pr}(z|t,r)$. So the user profile can be represented by a topic-based $P_z(u_a) =< T_z(u_a), W_z(u_a) >$ with the weight $W_z(u_a) = \{w_1(u_a), ..., w_K(u_a)\}$.

3.2 Topic Weight Perturbation

After generating $P_z(u_a)$, we will add *Laplace* noise to mask the weights of tags in each topic: $\widehat{W}_z(u_a) = W_z(u_a) + Laplace(\frac{4}{\epsilon})^K$. Noise implies the revision of the list $T_z(u_a)$. Positive noise indicates new tags being added, while negative one indicates tags being deleted from the list. For positive noise in the topic z_l, the operation will choose the tags with the highest probability in the current topic z_j according to the $Pr(t|z)$. For negative noise, the operation will delete the tag with the lowest probability in the current topic z_l.

$$\widetilde{T}_{z_l}(u_a) = T_{z_l}(u_a) + t_{new}, \widetilde{T}_{z_l}(u_a) = T_{z_l}(u_a) - t_{delete} \tag{4}$$

where $t_{new} = \max_{i=1}^{|T|} Pr(t_i|z_l)$ and $t_{delete} = \min_{i=1}^{|T|} Pr(t_i|z_l)$.

After perturbation, we use $\widetilde{P}_z(u_a) =< \widetilde{T}_z(u_a), \widehat{W}_z(u_a) >$ to represent the noisy topic-based user profile. However, the $\widetilde{P}_z(u_a)$ still has the high probability to be re-identified because it retains a major part of the original tags. The next operation will replace all tags in $\widetilde{T}(u_a)$ to preserve privacy.

3.3 Private Tag Selection

Private Tag Selection adopts the *Exponential* mechanism to privately select tags from a list of candidates. Specifically, for a particular tag t_i, the operation first locates the topic z_l to which it belongs and all tags in $\hat{T}_{z_l}(u_a)$ are then included in a candidate list I. Each tag in I is associated with a probability based on a *score function* and the *sensitivity* of the function. The selection of tags is performed based on the allocated probabilities.

The *score function* is defined as the *Jensen-shannon* (JS) divergence between $Pr(z|t_i = t_i)$ and $Pr(z|t_i = t_j)$. Because the JS divergence is bounded by 1, the score function q for a target tag t_i is defined as $q_i(I, t_j) = (1 - D_{JS}(Pr_i||Pr_j))$, where $t_j \in I$ are the candidate tags for replacement and D_{JS} refers to JS divergence. The *sensitivity* for q is measured by the maximal distance of two

tags, which is 1. Based on the *score function* and *sensitivity*, the probability arranged to each tags t_j is computed by Eq. 5 with the privacy budget $\frac{\epsilon}{4}$.

$$Pr_{t_j \in I}(t_j) = \exp\left(\frac{\epsilon \cdot q_i(I, t_j)}{8}\right) / \sum_{j \in z_l} \exp\left(\frac{\epsilon \cdot q_i(I, t_j)}{8}\right). \quad (5)$$

where z_l is the topic in which t_j belongs to.

4 Algorithm Analysis

4.1 Privacy Analysis

To analyze the privacy guarantee, we apply two composition properties of differential privacy [10]. The *sequential composition* accumulates ϵ of each step when a series of private analysis is performed *sequentially* on a dataset. The *parallel composition* ensures the maximal ϵ when each private step is applied on disjointed subsets of the dataset. The *PriTop* algorithm contains three private operations and the ϵ is consequently divided into three pieces: $\frac{\epsilon}{2}$, $\frac{\epsilon}{4}$ and $\frac{\epsilon}{4}$, respectively.

- *Private Topic Model Generation* is performed on the whole dataset with the $\frac{\epsilon}{2}$. According to *sequential composition*, it preserves $\frac{\epsilon}{2}$-*differential privacy.*
- *Topic Weight Perturbation* preserves $\frac{\epsilon}{4}-$*differential privacy* for each user. As a user's profile is independent, according to *parallel composition*, it preserves $\frac{\epsilon}{4}$-*differential privacy.*
- *Private Tag Selection* processes the *Exponential* mechanism successively. For a user u, each selection is performed on the individual tags, according to *sequential composition*, each user guarantees $\frac{\epsilon}{4}$-*differential privacy.* Similar to the *Topic Weight Perturbation*, every user can be considered as subsets. Thus, the *Private Tag Selection* guarantees $\frac{\epsilon}{4}$-*differential privacy.*

Consequently, the proposed *PriTop* algorithm preserves ϵ-*differential privacy.*

4.2 Utility Analysis

Given a target user u_a, the utility level of the proposed *PriTop* algorithm is highly dependent on the distance between $P(u_a)$ and $\widehat{P}(u_a)$, which is referred to as *semantic loss* [11]: $SLoss = \frac{1}{|U|}\sum_{u \in U}(\frac{\sum_{t \in P(u_a)} d(t,\widehat{t})}{\max d \cdot |T(u)|})$, where $\widehat{t}$ is the new tag replacing the tag t. If we consider each private step as a query f, we then apply a utility definition in *differential privacy* suggested by Blum et al [3]. Accordingly, we demonstrate the *SLoss* is bounded by a certain value α with a high probability.

Definition 5 ((α,δ)-usefulness). *A mechanism $\mathcal{M}$ is (α,δ)-useful for a set of query F, if with probability $1-\delta$, for every query $f \in F$ and every dataset G, for $\widehat{G} = \mathcal{M}(G)$, we have $\max_{f \in F} |f(\widehat{G}) - f(G)| \leq \alpha$, where F is a group of queries.*

Theorem 41 *For any user $u \in U$, for all $\delta > 0$, with probability at least $1 - \delta$, the $SLoss_1$ of the user in the perturbation is less than α. When $|T(u)| \geq \frac{K \cdot \exp(\frac{-\epsilon\alpha_a}{4})}{\delta}$, the perturbation operation is satisfied with (α, δ)-useful.*

Proof. The perturbation adds *Laplace* noise with $\epsilon/4$ to the weight. According to the property of *Laplace*(b): $Pr(|\gamma| > t) = \exp(-\frac{t}{b})$, we have $Pr(SLoss_1 > \alpha_a) = \frac{K \cdot d(t_{ai}, \widehat{t}_{ai})}{\max d|T(u_a)|} \exp(-\frac{\epsilon\alpha_a}{4})$. As the perturbation step adds new tags or delete tags, the $d(t_{ai}, \widehat{t}_{ai})$ will be less than 1, we obtain the evaluation on the $SLoss_1$: $Pr(SLoss_1 < \alpha_a) \leq 1 - \frac{K \cdot \exp(-\frac{\epsilon\alpha_a}{4})}{|T(u_a)|}$. Let $1 - \frac{K \cdot \exp(-\frac{\epsilon\alpha_a}{4})}{|T(u_a)|} \geq 1 - \delta$, Thus $|T(u_a)| \geq \frac{K \cdot \exp(\frac{-\epsilon\alpha_a}{4})}{\delta}$. The average semantic loss for all the users is less than the maximal value, $\alpha = \max_{u_a \in U} \alpha_a$, we have $|T(u)| \geq \frac{K \cdot \exp(\frac{-\epsilon\alpha}{4})}{\delta}$.

The theorem 41 reveals the *semantic loss* of perturbation depends on the number of tags a user has. More tags results in a lower *semantic loss*.

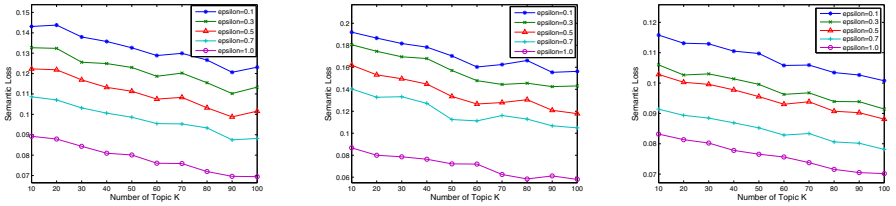
Theorem 42 *For any user $u \in U$, for all $\delta > 0$, with probability at least $1 - \delta$, the $SLoss_2$ of the user in the private selection is less than α. When $Q \leq \frac{\exp(\frac{\epsilon}{8})}{1 - \delta\alpha}$, where Q is the normalization factor that depends on the topic that $t \in T(u)$ belongs to, the private selection operation is satisfied with (α, δ)-useful.*

Proof. According to Marlkov's inequality, we get $Pr(SLoss_2 > \alpha_a) \leq \frac{E(SLoss_2)}{\alpha_a}$. For each tag t_{ai} in $\widehat{P}_a$, the probability of 'unchange' in the private selection is proportional to $\frac{\exp(\frac{\epsilon}{8})}{Q_i}$, where Q_i is the normalization factor depending on the topic t_{ai} belongs to. We then obtain $E(SLoss_2) = \sum_{t_i \in T(u_a)} \frac{d(t_{ai}, \widehat{t}_{ai})}{\max d|T(u_a)|}(1 - \frac{\exp(\frac{\epsilon}{8})}{Q_i})$ and estimate $SLoss_2$ as $Pr(SLoss_2 > \alpha_a) \leq \frac{\sum_{t_i \in T(u_a)} d(t_{ai}, \widehat{t}_{ai})(1 - \frac{\exp(\frac{\epsilon}{8})}{Q_i})}{|T(u_a)|\alpha_a}$. When $d(t_{ai}, \widehat{t}_{ai}) = 1$ and $Q = \max Q_i$, it is simplified as $Pr(SLoss_2 \leq \alpha_a) \geq 1 - \frac{1 - \frac{1}{Q}\exp(\frac{\epsilon}{8})}{\alpha_a}$. Let $1 - \frac{1 - \frac{1}{Q}\exp(\frac{\epsilon}{8})}{\alpha_a} \geq 1 - \delta$, $Q \leq \frac{\exp(\frac{\epsilon}{8})}{1 - \delta\alpha_a}$. Similar to the proof of theorem 41, We obtain $Q \leq \frac{\exp(\frac{\epsilon}{8})}{1 - \delta\alpha}$, where $Q_i = \sum_{j \in z_l} \exp\left(\frac{\epsilon \cdot d(t_i, t_j)}{8}\right)$.

The theorem 42 shows the *semantic loss* of private selection mainly depends on the ϵ and Q_i, which measures by the total distance inside topic z to which t_i belongs. The shorter distance leads to a smaller Q_i and less *semantic loss*.

5 Experiment and Analysis

We conduct experiment on three datasets: *Del.icio.us*, *MovieLens* and *Last.fm*. *Del.icio.us* dataset was retrieved from the *Del.icio.us* website by the *Distributed Artificial Intelligence Laboratory* (DAI-Labor), and includes around 132 million resources and 950,000 users. We extracted a subset with 3,000 users, 34,212 bookmarks and 12,183 tags. *MovieLens* and *Last.fm* datasets were obtained from *HetRec 2011*. All datasets are structured as triples (*user*, *resource*, *tag*), and filtered by removing added tags like "imported", "public", etc.



(a) *Semantic Loss* in *Del.icio.us* (b) *Semantic Loss* in *MovieLens* (c) *Semantic Loss* in *Last.fm*

Fig. 1. *Semantic Loss* on Different Datasets

5.1 Semantic Loss Analysis

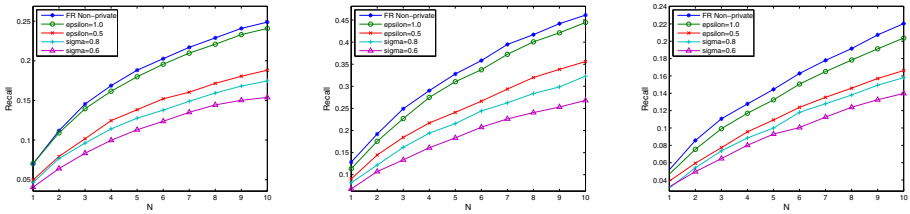
To maintain consistency with previous research, we compare the *semantic loss* of *PriTop* with *tag suppression* [11]. For the *PriTop* algorithm, we selected $\epsilon = 0.1, 0.3, 0.5, 0.7$ and 1.0 to represent different privacy levels and the number of topic K varies from 10 to 100 with a step of 10. In *tag suppression* [11], the *semantic loss* exhibits a linear relationship with the *eliminate parameter* σ. When we choose the representative value $\sigma = 0.8$, the *sematic loss* is 0.2.

It can be observed from Fig. 1 that the *semantic loss* of the *PriTop* algorithm in a variety of datasets was less than 0.2 with different privacy budgets, which indicates that *PriTop* outperforms *tag suppression* on all configurations. Specifically, the *PriTop* obtains a considerably lower *semantic loss* when $\epsilon = 1$. For example, in Fig. 1a, when $K = 90$ and $\epsilon = 1$, the *semantic loss* is 0.0767, which is 62% lower than *tag suppression* with $SLoss = 0.2$. This trend is retained when K equals other values and in other figures, such as Fig. 1b and 1c. All figures show that *PriTop* obtains a stable *semantic loss* at a lower level, and retains more utility than *tag suppression*. This is because *PriTop* retains the relationship between tags and resources, and makes the profiles of users meaningful.

5.2 Performance of Tagging Recommendation

To investigates the effectiveness of *PriTop* in the context of tagging recommendations, we apply a state-of-the-art tagging recommender system, *FolkRank* [9], to measure the degradation of privacy preserving recommendations. We use *Recall* to quantify the performance and N is the number of recommended tags. The following experiments compare the *PriTop* with *tag suppression* with N varies from 1 to 10. For *PriTop*, we chose $K = 100$, and test the performance when $\epsilon = 1$ and 0.5. For *tag suppression*, we fix $\sigma = 0.8$ and 0.6, corresponding to suppression rates of 0.2 and 0.4, respectively.

Fig. 2 presents the recall of recommendation results. It is observed that the proposed *PriTop* algorithm significantly outperforms the *tag suppression* method on both privacy budgets. Specifically, as shown in Fig. 2a, when $N = 1$, *PriTop* achieves a *recall* at 0.0704 with the $\epsilon = 1$ which outperforms the result from the *tag suppression* with $\sigma = 0.6$, 0.0407, by 42.19%. This trend is retained

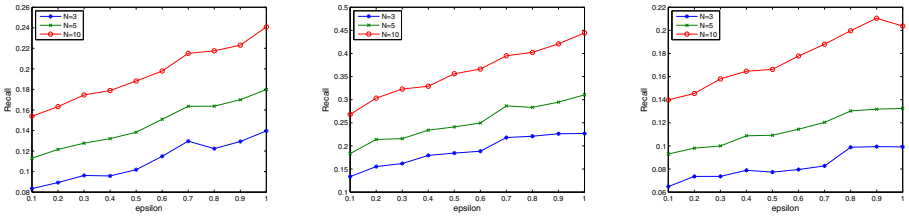


(a) *Del.icio.us* (b) *MovieLens* (c) *Last.fm*

Fig. 2. *FolkRank* Recall Result

as the increasing of N. When $N = 5$, *PriTop* achieves a *recall* at 0.1799 with the $\epsilon = 1$ which outperforms the result from the *tag suppression* by 37.19% when $\sigma = 0.6$, 0.113. When N reaches 10, the *PriTop* still retains 36.09% higher on *recall* than *tag suppression*. Even we choose the lower privacy budget with $\epsilon = 0.5$ and a higher *eliminate* parameter $sigma = 0.8$, the improvement is still significant. The *PriTop* has a *recall* of 0.1382, which is also 7.67% higher than *tag suppression* with a *recall* of 0.1276. The improvement of *PriTop* is more obvious when $N = 10$. It achieves *recalls* of 0.1882 and 0.2408 when $\epsilon = 1$ and $\epsilon = 0.5$, respectively. But *tag suppression* only achieves *recalls* of 0.1538 and 0.1881 with $\sigma = 0.6$ and $\sigma = 0.8$. Similar trends can also be observed in Fig. 2b and 2c. In the *MovieLens* dataset, when $N = 10$ and $\epsilon = 1.0$, the recall of *PriTop* is 0.4445, which is 27.33% higher than *tag suppression* with $\sigma = 0.8$. With the same configuration, *PriTop* is 22.43% and 25.22% higher than *tag suppression* in *Last.fm* and *Bibsonomy* datasets. The experimental results show the *PriTop* algorithm outperforms *tag suppression* in variety of N, which implies that *PriTop* can retain more useful information for recommendations than simply deleting the tags. In addition, the performance of *PriTop* is very close to the *non-private* baseline. For example in Fig. 2a, when $\epsilon = 1$, the *recall* of the *De.licio.us* dataset is 0.2408, which is only 3.00% lower than the non-private recommender result. Other datasets show the same trend. As shown in Fig. 2b and 2c, with the same configuration, the *PriTop* result is 3.62% lower than the non-private result on the *MovieLens* dataset, and 7.58% lower on the *Last.fm* dataset. The results indicate that *PriTop* algorithm achieves the privacy preserving objective while retaining a high accuracy of recommendations.

To show the statistical effectiveness of *PriTop*, we apply a paired t test (with a 95% confidence) to examine the difference on the performance of *PriTop* with $\epsilon = 1.0$ and *tag suppression* with $\sigma = 0.2$. The statistics for results are shown in Table 1. All t values are greater than 6 and all p values are less than 0.0001, thus indicating improvement on *recall* are statistically significant.



(a) *Del.icio.us* (b) *MovieLens* (c) *Last.fm*

Fig. 3. Impact of Privacy Budget in *FolkRank* Recall Result

Table 1. Paired-t-test betwee *PriTop* and *Tag Suppression*

		df	*t*	*p*-value
De.licio.us	Recall	9	11.3276	< 0.0001
MovieLens	Recall	9	9.0957	< 0.0001
Last.fm	Recall	9	10.7546	< 0.0001

5.3 Impact of Privacy Budget

In the context of *differential privacy*, the lower ϵ represents a higher privacy level. To achieve a comprehensive examination of *PriTop*, we evaluate the performance of recommendation under diverse privacy levels.

Fig. 3 shows the *recall* on the three datasets. It presents the recommendation performance achieved by *PriTop* when the privacy budget ϵ varies from 0.1 to 1 with a step of 0.1. It is clear the *recall* of tag recommendations is significantly affected by the required privacy budget. The *recall* increases as ϵ increases. For example, as plotted in Fig. 3a on the *Del.icio.us* dataset, when $N = 10$, *PriTop* achieves a *recall* at 0.1538 with $\epsilon = 0.1$ and 0.2408 with $\epsilon = 1$. The reason is the privacy and utility issues are two opposite components of the datasets. We have to sacrifice the utility to obtain the privacy, therefore our purpose is to obtain an optimal utility when fixing the privacy at an acceptable level.

As a summary, results on a real tagging recommender system confirm the practical effectiveness of the *PriTop* algorithm.

6 Conclusions

Privacy preserving is one of the most important aspects in recommender systems. However, when we introduce the *differential privacy*, the solution fails to retain the relationship among users, resources and tags; and introduces a large volume of noise, which significantly affects the recommendation performance.

This paper proposes an effective privacy tagging release algorithm *PriTop* with the following contributions: 1) We propose a private tagging release algorithm to protect users from being re-identified in a tagging dataset. 2) A

private topic model is designed to reduce the magnitude of noise by shrinking the randomization domain. 3) A better trade-off between privacy and utility is obtained by taking the advantage of the differentially private composition properties. These contributions provide a practical way to apply a rigid privacy notion to a tagging recommender system without high utility costs.

References

1. Berkovsky, S., Eytani, Y., Kuflik, T., Ricci, F.: Enhancing privacy and preserving accuracy of a distributed collaborative filtering. In: RecSys (2007)
2. Blei, D.M., Ng, A.Y., Jordan, M.I.: Latent dirichlet allocation. The Journal of Machine Learning Research 3, 993–1022 (2003)
3. Blum, A., Ligett, K., Roth, A.: A learning theory approach to non-interactive database privacy. In: STOC, pp. 609–618 (2008)
4. Calandrino, J.A., Kilzer, A., Narayanan, A., Felten, E.W., Shmatikov, V.: "You might also like:" privacy risks of collaborative filtering. In: SP (2011)
5. Canny, J.: Collaborative filtering with privacy. In: S&P 2002, pp. 45–57. IEEE (2002)
6. Dwork, C.: A firm foundation for private data analysis. Commun. ACM 54(1), 86–95 (2011)
7. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 265–284. Springer, Heidelberg (2006)
8. Fung, B.C.M., Wang, K., Chen, R., Yu, P.S.: Privacy-preserving data publishing: A survey of recent developments. ACM Comput. Surv. (2010)
9. Jäschke, R., Marinho, L., Hotho, A., Schmidt-Thieme, L., Stumme, G.: Tag recommendations in folksonomies. In: Kok, J.N., Koronacki, J., Lopez de Mantaras, R., Matwin, S., Mladenič, D., Skowron, A. (eds.) PKDD 2007. LNCS (LNAI), vol. 4702, pp. 506–514. Springer, Heidelberg (2007)
10. McSherry, F., Talwar, K.: Mechanism design via differential privacy. In: FOCS 2007, pp. 94–103 (2007)
11. Parra-Arnau, J., Perego, A., Ferrari, E., Forne, J., Rebollo-Monedero, D.: Privacy-preserving enhanced collaborative tagging. IEEE Transactions on Knowledge and Data Engineering 99(PrePrints), 1 (2013)
12. Polat, H., Du, W.: ICDM, pp. 625–628 (November 2003)
13. Ramakrishnan, N., Keller, B.J., Mirza, B.J., Grama, A.Y., Karypis, G.: Privacy risks in recommender systems. IEEE Internet Computing 5(6), 54–62 (2001)
14. Steyvers, M., Griffiths, T.: Probabilistic topic models. In: Handbook of Latent Semantic Analysis, vol. 427(7), pp. 424–440 (2007)
15. Zhan, J., Hsieh, C.-L., Wang, I.-C., Hsu, T.S., Liau, C.-J., Wang, D.-W.: Privacy-preserving collaborative recommender systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C 40(4), 472–476 (2010)
16. Zhu, T., Li, G., Ren, Y., Zhou, W., Xiong, P.: Differential privacy for neighborhood-based collaborative filtering. In: ASONAM (2013)
17. Zhu, T., Li, G., Ren, Y., Zhou, W., Xiong, P.: Privacy preserving for tagging recommender systems. In: The 2013 IEEE/WIC/ACM International Conference on Web Intelligence (2013)