الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي ٠08 ماي 1945٠ بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

Mémoire de Fin d'étude

Pour l'obtention du diplôme d'**ingénieur d'état**
Filière : **Informatique**
Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

Thème

PPREC: A Privacy Preserving Recommender System with Local Differential Privacy

---

Présenté par :

- Mohamed Naas

Soutenu le : **26/09/2021** Devant le jury composé de :

Mr BENDAOUAD Fayçal	Président
Mr BELFEDHAL Alaa Eddine	Encadreur
Mr AZZA Mohamed	Examinateur

Année Universitaire : 2020/2021

Abstract

Recommender systems plays an important role today and are widely applied to a wide range of domains. Similar to most machine learning algorithms, recommendation systems rely on users's data to train and to generate recommendations .Often, these data can be private and in case of a leakage, it could seriously cause harm to the users, making it a crucial mission to investigate privacy threats in recommender systems and implement defensive techniques to address them. In this work we highlight various recommendation systems types and techniques, then we present popular privacy preserving machine learning techniques. Moreover, we revisit the different proposed techniques to preserve privacy in literature. Furthermore, we propose **PPREC**, a privacy preserving recommendation engine using local differential privacy and matrix factorization. Finally, we put the proposed library on numerous tests and discussed the obtained results.

Key words : Recommender systems, privacy preserving machine learning, differential privacy, Node.js.

ملخص

تلعب أنظمة التوصية دورًا مهمًا اليوم ويتم تطبيقها على نطاق واسع في مجموعة واسعة من المجالات. على غرار معظم خوارزميات التعلم الآلي ، تعتمد أنظمة التوصية على بيانات المستخدمين للتدرب ولإصدار التوصيات ، و لكن في كثير من الأحيان ، يمكن أن تكون هذه البيانات خاصة وفي حالة حدوث تسرب ، يمكن أن تسبب ضررًا خطيرًا للمستخدمين مما يجعل التحقيق في تهديدات الخصوصية مهمة هامة و يجب تنفيذ تقنيات دفاعية لحل هته التهديدات.

في هذا العمل ، سنسلط الضوء على أنواع وتقنيات أنظمة التوصية المختلفة ، ثم نقدم تقنيات التعلم الآلي الاكثر شعبية للحفاظ على الخصوصية. سنعيد النظر في الأساليب المقترحة المختلفة للحفاظ على الخصوصية في الاوساط العلمية. علاوة على ذلك ، سنقترح نظام توصية محافظ على الخصوصية باستعمال الخصوصية التفاضلية المحلية . أخيرًا ، وضعنا المكتبة المقترحة على عدد االاختبارات ثم ناقشنا النتائج التي تم الحصول عليها.