نحو المزيد من الخصوصية في طرق تنقيب البيانات المستخدمة في أنظمة التوصيات

تهاني صالح النزاوي

بحث مقدم لنيل درجة الماجستير في العلوم

(تقنية المعلومات)

أسماء المشرفين على الرسالة

د / نرمين عويس د / ريم العتيبي

كلية الحاسبات وتقنية المعلومات

جامعة الملك عبد العزيز

المستخلص

مع استخدام الأجيال الجديدة من الهواتف الذكية المزودة بنظام تحديد المواقع العالمي (GPS)، تظهر أنظمة التوصية القائمة على الموقع في السوق، مما يتيح للمستخدمين الاقتراحات المناسبة أثناء زيارة أماكن التنقل الخاصة بهم بناءً على أذواق المستخدم. تحظى هذه الأنظمة بشعبية كبيرة، وفوائدها مهمة جدًا للمستخدمين، ولكن هناك العديد من مشكلات الخصوصية التي أصبحت مصدر قلق كبير في مجتمع البحث. في أنظمة التوصية المستندة إلى الموقع (LbRSs)، يكون المستخدم مقيدًا ببناء استعلامات تعتمد على الموقع الفعلي لطلب نقاط الاهتمام الأقرب (POIs). يمكن للمهاجم الخارجي تحليل الاستعلامات المرسلة أو تتبع الموقع الفعلي للمستخدم LbRS للكشف عن المعلومات

الشخصية. وبالتالي، فإن ضمان حماية عالية للخصوصية (بما في ذلك خصوصية الموقع وخصوصية الاستعلام) أمر أساسي.

في هذه الرسالة، نقدم مسحًا شاملاً لأنظمة التوصيات القائمة على الموقع ونحللها من خلال عرض خصوصية المستخدم. ثم نقترح نموذجًا يضمن حماية خصوصية عالية لمستخدمي LbRS. النموذج المقترح هو العمل من خلال ثلاثة مكونات رئيسية: يستخدم المكون الأول (selector_D) نهجًا جديدًا لحماية خصوصية الموقع، وهو أسلوب اختيار الموقع الوهمي الذكية (SDS). نهج SDS يولد موقع وهمي قوي لديه مقاومة عالية ضد هجوم الموقع الدلالي. يستخدم المكون الثاني (المشفر _ ID) نهجًا يستند إلى التشفير يضمن مستوى عالٍ من خصوصية الاستعلام مقابل هجوم استعلام أخذ العينات. يقوم المكون الأخير (constructor_Q) بإنشاء الاستعلام المحمي الذي يتم إرساله إلى خادم LbRS.

Towards a More Private Data Mining Approach for Recommender Systems

By

Tahani Saleh Al_Nazzawi

Dr. Nermin Hamza and Dr. Reem Alotaibi

ABSTRACT

With the use of new generations of Global Positioning System GPS-enabled smartphones, site-based recommendation systems appear on the market, giving users appropriate suggestions while moving places to visit based on user tastes. These systems are very popular, and their benefits are very interesting to users, but there are many privacy problems which have become a major concern in the research community. In location-based recommendation systems (LbRSs), the user is constrained to build queries that depend on the actual location to ask for the closer points of interest (POIs). An external attacker can analyze these queries or track the actual location of the LbRS user to reveal personal information. Consequently, ensuring high privacy protection (which is including location privacy and query privacy) is fundamental.

In this thesis, we provide an extensive survey of location-based recommendation systems and analyze them from a user privacy view. We then propose a model that guarantees high privacy protection for LbRS users. The proposed model has three main components: The first component ($\text{selector}_{\text{D}}$) uses a new location privacy protection approach, namely, the smart dummy selection (SDS) approach. The SDS approach generates a strong dummy location that has high resistance versus a semantic location attack. The second component ($\text{encryptor}_{\text{ID}}$) uses an encryption-based approach that guarantee a high level of query privacy versus a sampling query attack. The last component ($\text{constructor}_{\text{Q}}$) constructs the protected query that is sent to the LbRS server. Our proposed system is supported by a checkpoint technique to ensure a high availability quality attribute. Our proposed system yields competitive results compared to similar systems under various privacy and performance metrics.