مرحلتين في إطار الحفاظ على الخصوصية لخدمات تحديد المواقع

عبدالله بن عبدالعزيز بن سعود البليهي

بحث مقدم لنيل درجة دكتوراه الفلسفة
في علوم الحاسب

إشراف

د.فيجي ثايانانثان

كلية الحاسبات وتقنية المعلومات

جامعة الملك عبد العزيز

جدة – المملكة العربية السعودية

مرحلتين في إطار الحفاظ على الخصوصية لخدمات تحديد المواقع

عبدالله بن عبدالعزيز بن سعود البليهي

المستخلص

الهدف الرئيسي لهذا البحث هو توفير استعلامات الحفاظ على الخصوصية للخدمات المستندة إلى الموقع استنادًا إلى كل من التقنيات التالية المرشح وناقل الغموض وصفر المعرفة.

والمساهمة في تطوير مقياس الأداء الذي يمكن أن يحسب مجموع الكون والمعلومات المتبادلة لسلسلة من وظائف التجزئة (قبل أن يتم تحويلها بواسطة أ ، وكذلك بعد أن يتم تحويلها بواسطة أ. ومن ثم إنشاء محاكاة تحسب هذه التدابير.

وبالتالي عملنا على تصميم إطار عمل أ (يعتمد على دمج المرشح مع ناقل الغموض و المرشح مع صفر المعرفة) يقلل من تسرب المعلومات بمقدار ١ بت لكل استعلام (نظام المرشح خالص) مقابل ن بت لكل استعلامات أ (نظام المرشح + أ).

وكذلك تم إنشاء مقياس أداء تلقائي يمكن حسابه في تنفيذ محاكاة للخوارزمية المركبة التي توفر تقديرًا (احتماليًا) لقيمة ن. أظهر أنه يمكن تحقيق ن >> ١ للحصول على اختيار أ.

وفي نهاية البحث قمنا بتقييم الإطار المقترح للأمن وكفاءة الخصوصية.

في هذه الأطروحة نُقدم حلاً لمشكلة الهاش في المرشح عن طريق تطوير طريقة لإنشاء مجموعة عشوائية من وظائف التجزئة المتعامدة والحسنة بشكل تلقائي ؛ بناء على شرطين وهما:

"زيادة الانتروبيا (العشوائية)" و "تقليل المعلومات المتبادلة" ؛ وكلاهما يجعل من الصعب على الخصم تعلم أي شيء من دراسة الاستجابات المشفرة.

يتلخص تقسيم هذه الرسالة في سبعة فصول كالتالي:

- الفصل الأول (المقدمة): قدمنا خلفية للبحث والتحفيز في مجال الخوادم القائمة على المواقع ، والتحديات الحالية فيه ، والأهداف ، والمساهمة ، وتنظيم الأطروحة.
- الفصل الثاني: لقد قدمنا دراسة استقصائية للاتجاهات الحالية لتقنيات الخصوصية المستخدمة في حماية خصوصية الموقع للمستخدمين في الخوادم القائمة على الموقع. وكذلك أبرزنا كفاءة ونقص كل تقنية تمت مناقشتها في هذا الفصل. ولقد وجدنا أن المرشح يعاني من الدقة وسرية الاستعلام مما يؤدي إلى تسرب المعلومات ولكنه لا يزال فعالًا.
- الفصل الثالث: عرضنا بنية الخصوصية المقترحة ضمن أوصاف كل من دليل إثبات المعرفة الصفرية ، وناقل الغموض ، والمرشح ، وتلاها بيان المشكلة واقتراح الحل.
- الفصل الرابع: تناول هذا الفصل وصف الحل في بروتوكولين وهما دمج المرشح مع ناقل الغموض والمرشح مع صفر المعرفة ، وهما بروتوكولات مكونة تحاول معالجة أوجه القصور الأمنية التي توجد عادة في بيئات تطبيقات الخوادم القائمة على المواقع الحالية. على وجه الخصوص ، يقوم كل المرشح مع ناقل الغموض والمرشح مع صفر المعرفة بمعالجة أمان معلومات تخزين النسخ الاحتياطي ، أو أمان المعلومات المرئية

لمتنصت ، أو لوجود جسم ضار على جهاز مزود الخوادم القائمة على المواقع ، كما يوفر وسيلة للمستخدم لإجراء اختبارات التناسق على مزود الخوادم القائمة على المواقع. ويوفر كل مكون بشكل فردي زيادة في الأمان ، بينما يوفر نشر المكونات الثلاثة زيادة كبيرة جدًا في الأمان باستخدام أي من أساليب النقل.

- الفصل الخامس: يوفر هذا الفصل بحثًا شاملاً بشكل متزايد عن الحفاظ على الخصوصية في الخوادم القائمة على المواقع. بالإضافة إلى ذلك ، تقترح المرشح مع ناقل الغموض والمرشح مع صفر المعرفة تعزيز الأمن والحفاظ على الخصوصية. المرشح مع ناقل الغموض هي آلية أخرى ، ذات قيمة في قدرتها على معالجة المشاكل في الخوادم القائمة على المواقع. ومع ذلك ، تجدر الإشارة إلى أن هذه الآلية بالذات ليست مثالية ، وقد تحتوي بشكل جيد على خطر التسرب المحتمل.
- الفصل السادس: وفيه تم ذكر نتائج التجارب المقترحة ومناقشة هذه النتائج.
- الفصل السابع: يستعرض هذا الفصل الخاتمة وكذلك يعرض خطوتين جديدتين لتمديد العمل ومن الممكن دراستهما في العمل مستقبلا.

Two-Phase Privacy Preserving Framework for Location-based Services

Albelaihy, Abdullah Abdulaziz S

A thesis submitted for the requirements of the

Doctorate Philosophy Degree in Computer Science

Supervised By

Dr. Vijey Thayananthan

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY

KING ABDULAZIZ UNIVERSITY

JEDDAH – SAUDI ARABIA

Rajab 1440H – March 2019G

• ABSTRACT

- Location-based services have become ubiquitous, effectively penetrating all smartphones and GPS-enabled devices and providing tremendous value to customers. While LBSs have grown in popularity, they are not without flaws; specifically, the user of an LBS must reveal his or her location data in order to take full advantage of the service, thereby potentially risking their own privacy and security.
- Location-based services present an inherent challenge: that of finding the delicate balance between efficiency when answering queries and respecting user privacy. Inevitable security issues will most certainly arise since the server needs to be informed of the query location to provide accurate responses. In spite of the many advancements in security that have taken place in wireless communication, it is still possible for servers to become infected with malicious software. Of course, it is now possible to make sure queries do not generate any fake responses that may appear real to users. Actually, when a fake response is utilized, there are mechanisms that can be employed so that the user can identify the authenticity of the query, a number of techniques have been proposed in the literature in order to provide an optimal solution for privacy-preserving queries in LBS. This research firstly explored three well-known approaches used in privacy-preserving location-based services: Zero Knowledge Proof, Oblivious Transfer, and Bloom filter. Each has the goal of reducing information leakage and creating an automated performance measure. Of the three methods described above, bloom filters arguably have the best runtime performance. However, bloom filters suffer from two deficiencies: (a) they leak at most one bit of information per query, and (b) the hash functions Hk require careful design and security analysis so that they are orthogonal and independent. This

means that even if Hi is broken, for some i, nothing can be learned about any other Hj (secure), j = i. We proposed a novel, two-phase privacy preserving framework for LBS involving a combination of a bloom filter with a second technique, Zero-Knowledge Proof BL0K or Oblivious Transfer BLOT. While all three of these methods have proved useful in securing a user's private information, our proposed two-phase privacy approach should enhance privacy even further, protecting users from malicious attacks by exploiting the inherent capabilities of BLOT and BL0K in protecting from attacks, respectively. Towards this end, the research proposed **BL**oom Filter **O**blivious **T**ransfer (**BLOT**) and **BL**oom Filter **0 K**nowledge (**BL0K**), The usefulness of these methods have been shown for securing the private information of a user. Analysis of the results demonstrated that BLOT and BL0K performed decidedly better when it was compared to the referenced approaches, and it also enhanced entropy.