

دراسات نقدية ٣ – الأسبوع السابع

تقرير نقدي حول المهمة السابعة: (تحليل المداخل النظرية)
لورقة بحثية في مجال التخصص
"تقنية المعلومات"

إعداد الطالب/
عبد السلام العتيبي

٢٠٢٥م



بيانات الدراسة (موضع النقد)

البيانات	المحتوى	المحتوى مترجم للعربية
عنوان الدراسة	Investigating Methods to Enhance Data Privacy in Business, Especially in sectors like Analytics and Finance	التحقيق في أساليب تعزيز خصوصية البيانات في الأعمال التجارية، وخاصة في قطاعات مثل التحليلات والتمويل
اسم المؤلف	Tanvir Rahman Akash, Dr. Dennis J. Lessard, Nayem Rahman, Md Shakil Islam	تنوير رحمن أكاش، د. دينيس جيه. ليسارد، نايم رحمن، محمد شاكيل إسلام
سنة النشر	٢٠٢٤	٢٠٢٤
جهة النشر	Journal of Computer Science and Technology Studies (منشور بواسطة AL-KINDI CENTER FOR	مجلة دراسات علوم الحاسوب والتكنولوجيا (منشور بواسطة مركز

مقدمة

تهدف هذه الورقة النقدية إلى تحليل الدراسة الموضحة بياناتها أعلاه. حيث سيتم التركيز بشكل خاص على عرض ومناقشة أحد المداخل النظرية المرتبطة بموضوع البحث، وتحليل مدى ملاءمتها للدراسة، مع تقديم أمثلة توضيحية من داخل الورقة لتعزيز الفهم، واختتام التقرير برؤية شاملة للتطوير المستقبلي.

عرض ومناقشة المدخل النظري تكنولوجيا تعزيز الخصوصية

(Privacy-Enhancing Technologies - PETs)

تُعد تكنولوجيا تعزيز الخصوصية (PETs) مدخلاً نظرياً محورياً في هذه الدراسة، حيث تمثل مجموعة من التقنيات المصممة لحماية خصوصية الأفراد مع السماح بمعالجة البيانات واستخدامها لأغراض تحليلية. تقدم الورقة ثلاث تقنيات رئيسية ضمن هذا المدخل:

١. الخصوصية التفاضلية (Differential Privacy): تهدف هذه التقنية إلى إضافة ضوضاء إحصائية إلى البيانات لضمان عدم الكشف عن المعلومات الخاصة بالأفراد عند إجراء التحليلات، مع الحفاظ على الفائدة الإجمالية للبيانات. وهذا يسمح للمؤسسات بالحصول على رؤى من البيانات دون المساس بخصوصية الأفراد.

تابع: عرض ومناقشة المدخل النظري تكنولوجيا تعزيز الخصوصية

(Privacy-Enhancing Technologies - PETs)

٢. إخفاء الهوية (Anonymization): تتضمن هذه العملية إزالة أو تعديل المعلومات التعريفية من مجموعة البيانات بحيث لا يمكن ربط البيانات بشخص معين. تطرح الدراسة هذه التقنية كأحد الأساليب الأساسية لتقليل مخاطر الخصوصية.

٣. التعلم الموحد (Federated Learning): يتيح هذا النهج تدريب نماذج التعلم الآلي على مجموعات بيانات موزعة عبر أجهزة متعددة دون الحاجة إلى نقل البيانات الخام إلى موقع مركزي. هذا يحافظ على خصوصية البيانات الفردية من خلال إبقاء البيانات على الجهاز المصدر.

تحليل مدى ملاءمة المدخل النظري (PETs) للدراسة

يُعد مدخل PETs ملائم جداً للدراسة، وذلك لعدة أسباب:

- **معالجة القضية البحثية الأساسية:** تتناول الدراسة بوضوح مخاوف خصوصية البيانات في القطاعات الحساسة مثل التحليلات والتمويل، وتقدم PETs حلولاً تقنية مباشرة لمعالجة هذه المخاوف. الورقة تؤكد أن PETs تسمح للشركات بتأمين البيانات الحساسة مع بقائها مفيدة للتحليل، وبالتالي تحقيق التوازن بين الابتكار والأمان.
- **التأصيل في السياق المعاصر:** تبرز الدراسة أهمية PETs في ظل تزايد استخدام المحتوى الذي ينشئه المستخدمون وتصادد الاهتمام بمجال حماية الهويات، حيث تصبح الحاجة ملحة لحماية الخصوصية. المدخل النظري لـ PETs يوفر استجابة مباشرة لتحديات الخصوصية في هذا السياق.
- **التكامل مع الأطر القانونية:** لا تكتفي الدراسة بعرض PETs كحلول تقنية بحتة، بل تربطها بشكل منهجي بالأطر القانونية مثل GDPR و CCPA. وهذا التكامل يعكس فهماً عميقاً بأن حماية الخصوصية تتطلب نهجاً شاملاً يجمع بين التقنيات والتشريعات. تُشير الدراسة إلى أن دمج PETs مع الأطر التنظيمية "يعمل كطريقة قابلة للتطبيق لزيادة حماية الخصوصية".

أمثلة توضيحية من واقع سياق الدراسة

- "الخصوصية التفاضلية على سبيل المثال تضمن أن تحليل البيانات لا يمكن أن يؤدي إلى انتهاك الخصوصية الفردية". وهذا يوضح كيف تساهم الخصوصية التفاضلية في الحفاظ على خصوصية الأفراد حتى عند إجراء تحليلات معمقة.
- "أدوات مثل تقليل البيانات، وإخفاء الهوية، والتعلم الموحد... كلها تهدف إلى تقليل مخاطر الخصوصية مع الحفاظ على فائدة البيانات للتحليل". وهذا الاقتباس يوضح كيف أن التقنيات المذكورة في المدخل النظري تعمل بشكل متكامل لتحقيق أهداف الدراسة.
- في مناقشة النتائج، تُشير الدراسة إلى أن "الخصوصية التفاضلية وإخفاء الهوية والتعلم الموحد هي الأساليب الواعدة التي تم تحديدها لتقليل مخاطر الخصوصية مع تحقيق تحليل فعال للبيانات". وهذا يؤكد بشكل مباشر على دور هذه التقنيات في سد الفجوات البحثية.
- تعزز الدراسة هذا المدخل بتقديم جدول تقييم للمخاطر قبل وبعد تطبيق الإجراءات الوقائية، مما يعزز المصداقية والمنهجية العلمية.



جوانب القوة في تناول المدخل النظري

- . **الوضوح والتركيز:** تحدد الدراسة بوضوح التقنيات التي تتدرج تحت مظلة PETs وتخصص قسماً لمناقشتها.
- . **التطبيق العملي:** لا تكتفي الدراسة بالشرح النظري، بل تقدم أمثلة على كيفية تطبيق هذه التقنيات، مثل استخدام تحليل أنواع المعاملات وتوزيع مبالغها ومقارنة الرصيد القديم والجديد لبيان الحاجة إلى PETs.
- . **التكامل التنظيمي:** الربط بين PETs والأطر القانونية (GDPR و CCPA) يُظهر فهماً شاملاً للتحديات والحلول في مجال خصوصية البيانات.
- . **الاعتراف بالقيود:** تدرك الدراسة أن تطبيق PETs قد يواجه تحديات، مثل التكلفة المالية ومتطلبات التغيير التنظيمي، وهذا يعكس واقعية في التحليل.

جوانب الضعف في تناول المدخل النظري

- **العمق النظري:** على الرغم من وضوح العرض، إلا أن الدراسة قد تستفيد من تعميق المناقشة النظرية لكل تقنية من تقنيات PETs، مثل استعراض الأسس الرياضية للخصوصية التفاضلية أو نماذج التعلم الموحد المختلفة.
- **نقص المقارنة النقدية:** لم تقدم الدراسة مقارنة نقدية متعمقة بين التقنيات المختلفة لـ PETs من حيث فعاليتها وتكاليفها ومدى تعقيد تطبيقها في سيناريوهات مختلفة. على سبيل المثال، متى تكون الخصوصية التفاضلية أكثر ملاءمة من إخفاء الهوية، والعكس صحيح؟
- **التحديات التطبيقية المفصلة:** بينما تُشير الدراسة إلى أن هناك فجوة تتطلب من الأفراد تكييف الممارسات، إلا أنها يمكن أن تتوسع في تفصيل التحديات العملية التي تواجه المؤسسات عند تطبيق هذه التقنيات، مثل متطلبات المهارات الفنية، والتحديات في دمجها مع الأنظمة الحالية.

رؤية شاملة للتطوير مستقبلاً

لتعزيز الدراسة بشكل أكبر، يمكن للباحثين المستقبليين التركيز على النقاط الرئيسية التالية المتعلقة بالمدخل النظري لـ تقنيات تعزيز الخصوصية (PETs):

١. توسيع نطاق PETs المدروسة: يشمل ذلك استكشاف تقنيات ناشئة مثل التشفير المتماثل (Homomorphic Encryption) وتقنية البلوك تشين (Blockchain)، مما سيثري المدخل النظري ويقدم حلولاً أكثر شمولاً لسيناريوهات الخصوصية المعقدة.

٢. تحليل التكلفة والفائدة (Cost-Benefit Analysis): إجراء تحليل كمي للتكاليف والفوائد المرتبطة بتطبيق أنواع مختلفة من PETs، خاصة بالنسبة للشركات الصغيرة والمتوسطة (SMEs)، لتوفير إرشادات عملية للمؤسسات حول أفضل السبل للاستثمار في حلول خصوصية البيانات.

٣. تطوير نماذج تقييم فعالية PETs ودمج الذكاء الاصطناعي: يتضمن ذلك وضع معايير وأطر لتقييم فعالية تقنيات الخصوصية المختلفة ونهج الامتثال. بالإضافة إلى ذلك، يُمكن استكشاف كيفية دمج خوارزميات الذكاء الاصطناعي والتعلم الآلي المتقدمة مع PETs لإنشاء آليات حماية بيانات استباقية.

خاتمة

تُعد الورقة البحثية "موضع التحليل والنقد" مساهمة قيمة في فهم طرق تعزيز خصوصية البيانات في القطاعات الحيوية مثل التحليلات والتمويل. فمن خلال التركيز على مدخل تكنولوجيا تعزيز الخصوصية (PETs) وربطها بالأطر التنظيمية، تقدم الدراسة إطاراً قوياً لضمان أمان البيانات. إلا أن هناك مجالاً للتطوير المستقبلي لتعميق الجوانب النظرية والتطبيقية، واستكشاف تقنيات جديدة، وتحليل التكاليف والفوائد، والنظر في العوامل الثقافية والتنظيمية. وإن دمج هذه التوصيات سيعزز من جدوى الأبحاث المستقبلية ويساهم في بناء بيئة رقمية أكثر أماناً وموثوقية للمستخدمين والمؤسسات على حد سواء.

المرجع

Akash, T. R., Lessard, D. J., Rahman, N., & Islam, M. S. (2024). Investigating Methods to Enhance Data Privacy in Business, Especially in sectors like Analytics and Finance. Journal of Computer Science and Technology Studies, 6(5), 143–151. <https://doi.org/10.32996/jcsts.2024.6.5.12>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

