

قضايا بحثية ٣ – الأسبوع السادس

دراسة:

Protection of Big Data Privacy

إعداد الطالب/عبدالسلام العتيبي

٢٠٢٥



مشكلة البحث

شهد العالم في السنوات الأخيرة انفجارًا هائلًا في حجم البيانات الناتجة عن التفاعل مع الإنترنت، وتطبيقات الرعاية الصحية، ووسائل التواصل الاجتماعي، والمستشعرات الذكية، ما أفرز ما يُعرف بـ"البيانات الضخمة". وعلى الرغم من أن تحليل هذه البيانات يمنح المؤسسات فرصًا غير مسبوقة لاتخاذ قرارات استراتيجية دقيقة، إلا أن ذلك يصاحبه تهديد متزايد لخصوصية الأفراد. فقد أصبح بالإمكان، من خلال تقنيات التحليل الحديثة، استنتاج معلومات حساسة عن الأشخاص حتى وإن لم تُفصح البيانات عنها صراحة.

تتجلى المشكلة الرئيسية في أن معظم آليات حماية الخصوصية التقليدية، مثل التشفير البسيط أو التحكم بالوصول، لم تعد كافية في بيئة البيانات الضخمة التي تتسم بالتوزيع، والتنوع، والسرعة. ومع الاعتماد المتزايد على الحوسبة السحابية في تخزين البيانات ومعالجتها، تزداد احتمالية تسرب المعلومات أو إساءة استخدامها. إذن، تبرز الحاجة إلى إعادة النظر في الأساليب المتبعة حاليًا لحماية الخصوصية في ضوء التحديات التقنية الجديدة، مع الأخذ في الحسبان مراحل دورة حياة البيانات كاملة (من التوليد، إلى التخزين، فالمعالجة).

أهمية البحث

تكمن أهمية هذا البحث في عدة محاور رئيسية:

١. الأهمية النظرية؛ حيث يساهم في سد فجوة معرفية متزايدة في الأدبيات العلمية حول حماية الخصوصية في سياق البيانات الضخمة، من خلال استعراض شامل للتقنيات الحالية وتقييم فعاليتها وقيودها، مما يثري قاعدة المعرفة في هذا المجال سريع التطور.

٢. الأهمية التطبيقية؛ حيث يقدم البحث حلولاً عملية لصانعي القرار في المؤسسات والشركات التي تعتمد على البيانات في أنشطتها، كما يرشد المطورين والمهندسين إلى أفضل الممارسات التقنية لحماية خصوصية المستخدمين.

أهمية البحث

تكمّن أهمية هذا البحث في عدة محاور رئيسية:

٣. البعد القانوني والأخلاقي، حيث يعزز هذا البحث الوعي بمخاطر انتهاك الخصوصية، ويدفع باتجاه مواءمة تقنيات معالجة البيانات مع المبادئ القانونية والأخلاقية، خاصة مع غياب تشريعات واضحة في العديد من الدول حول حماية البيانات الشخصية في البيئة السحابية.

٤. الأهمية المستقبلية، حيث يقدم البحث تصورًا للاتجاهات المستقبلية في حماية خصوصية البيانات، ويسلط الضوء على التقنيات الناشئة مثل التشفير المتجانس والحوسبة متعددة الأطراف الآمنة.

أهداف البحث

يسعى البحث إلى تحقيق مجموعة من الأهداف المتكاملة تشمل ما يلي:

١. تحليل مراحل دورة حياة البيانات الضخمة وتحديد نقاط الضعف في كل مرحلة من حيث مخاطر الخصوصية.
٢. عرض ومقارنة تقنيات حماية الخصوصية المستخدمة في كل مرحلة (التوليد، التخزين، المعالجة) مثل: التشفير القائم على السمات (ABE)، التشفير القائم على الهوية (IBE)، تقنيات إخفاء الهوية (Anonymization)، وغيرها.
٣. تقييم التحديات العملية التي تواجه حماية الخصوصية في ظل الحوسبة السحابية متعددة المستأجرين (Multi-Tenancy) والتخزين المركزي.

أهداف البحث

يسعى البحث إلى تحقيق مجموعة من الأهداف المتكاملة تشمل ما يلي:

٤. اقتراح اتجاهات بحثية مستقبلية وتقنيات بديلة للتعامل مع القيود الحالية، مثل اعتماد أنظمة تخزين لا مركزية، أو تطوير آليات تشفير خفيفة وقابلة للتوسع.
٥. قياس العلاقة بين مستوى حماية الخصوصية ومدى الاستفادة من البيانات (Privacy-Utility Trade-off) وتقديم مقترحات متوازنة تحقق الأمان دون إهدار الفائدة التحليلية.

أهداف البحث

لتحقيق أهداف هذا البحث، سيتم اتباع منهجية علمية شاملة تجمع بين التحليل النظري والمقارنة التقنية:

١. المنهج الوصفي التحليلي؛ سيتم تحليل الوثائق العلمية والدراسات السابقة المتعلقة بحماية خصوصية البيانات الضخمة، وتوصيف آليات الحماية وتقييم أدائها من الناحية التقنية والوظيفية.
٢. منهج تحليل النظم؛ سيركز على تحليل دورة حياة البيانات الضخمة كاملة، وتحديد مواضع الخلل الأمنية المحتملة في كل مرحلة، مع ربطها بالبنية التحتية السحابية.
٣. المنهج المقارن؛ ستتم مقارنة فعالية أبرز تقنيات حماية الخصوصية المستخدمة حاليًا مثل التشفير، وتقنيات إخفاء الهوية، وحوكمة الوصول، من حيث الأمان، الكفاءة، قابلية التطبيق، والتكلفة.
٤. دراسة الحالات، سيستعرض عدد من الحوادث الأمنية البارزة التي حصل فيها تسريب لبيانات شخصية عبر منصات تعتمد على البيانات الضخمة (مثل تسريب استعلامات بحث AOL، أو تحليل بيانات Facebook)، بهدف فهم الثغرات وتحليل آليات الفشل.

الخاتمة

إن حماية خصوصية البيانات الضخمة تمثل تحديًا عالميًا معقدًا يتطلب حلولًا تقنية وتنظيمية مبتكرة. في ضوء النمو المطرد في الاعتماد على البيانات والتحليلات الذكية، يصبح هذا الموضوع أكثر إلحاحًا، خاصة مع الانتقال المتسارع إلى خدمات الحوسبة السحابية والذكاء الاصطناعي. تهدف هذه الدراسة إلى إرساء فهم عميق وممنهج للتقنيات المتوفرة، والكشف عن فجواتها، وتقديم إطار معرفي يساعد في رسم سياسات مستقبلية قائمة على التوازن بين الاستفادة من البيانات وحماية خصوصية الأفراد.

المرجع

Mehmood, A. (2016). Protection of Big Data Privacy.
Retrieved from

<https://ieeexplore.ieee.org/document/7460114>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

