

دراسات نقدية ٢

الباحث/عبدالسلام العتيبي

الأسبوع السابع



دارسات نقدية ٢

Secure sensitive data sharing on a big data platform

إعداد
الباحث/عبدالسلام العتيبي

تعتبر البيانات من أبرز الأصول القيمة في العصر الرقمي الحالي، حيث تُستخدم في اتخاذ القرارات وتحليل الاتجاهات، مما يعزز الابتكار في مختلف المجالات. إلا أن التعامل مع البيانات الحساسة، مثل البيانات الشخصية، الصحية، أو المالية، يشكل تحديًا كبيرًا من حيث الأمان والخصوصية. في ظل الانتشار الواسع لمنصات البيانات الكبيرة Big Data platforms، التي تجمع وتخزن كميات هائلة من البيانات من مصادر متعددة، أصبح من الضروري وضع استراتيجيات وآليات لحماية هذه البيانات وضمان مشاركتها بشكل آمن وفعال.

يركز هذا البحث على تطوير حلول أمنية مبتكرة لضمان مشاركة البيانات الحساسة عبر منصات البيانات الكبيرة بطريقة تحترم الخصوصية وتمنع الوصول غير المصرح به. يتناول البحث الأساليب المتقدمة في التشفير، التحكم في الوصول، وتقنيات حماية البيانات التي تتيح تبادل المعلومات بشكل آمن، مع الحفاظ على كفاءة النظام في معالجة وتحليل البيانات. كما يناقش أهمية التعاون بين الجهات المختلفة، مثل الحكومات والشركات، لضمان الامتثال للمعايير الدولية وحماية حقوق الأفراد.

من خلال هذه الدراسة، يهدف البحث إلى استكشاف كيفية تصميم وتنفيذ آليات أمنية فعّالة تضمن سلامة البيانات الحساسة أثناء تبادلها على منصات البيانات الكبيرة، مع تحقيق التوازن بين الأمان وسهولة الاستخدام.

هل تم اختيار المنهج البحثي بشكل مناسب لموضوع الدراسة؟ نعم، تم اختيار المنهج البحثي الكمي بشكل مناسب لهذا الموضوع. حيث أن دراسة "مشاركة البيانات الحساسة بأمان على منصات البيانات الكبيرة" تتطلب تحليل كميات كبيرة من البيانات وتقييم فاعلية التقنيات المستخدمة لحماية هذه البيانات. المنهج الكمي يوفر أدوات قياس دقيقة تساعد على تحليل العوامل المؤثرة في الأمان، مثل مستوى الأمان الذي توفره أساليب التشفير، وتحليل فعالية آليات التحكم في الوصول. يتيح المنهج الكمي أيضاً قياس النتائج وتحليل البيانات المتوافقة مع الأهداف المحددة في البحث، مثل ضمان الأمان مع تحقيق التوازن بين الكفاءة وسهولة الاستخدام.

هل تم اختيار أدوات جمع البيانات بشكل مناسب؟ نعم، تم اختيار أدوات جمع البيانات بشكل مناسب لتحقيق أهداف البحث. في دراسة حول الأمان في منصات البيانات الكبيرة، من الممكن أن يتم استخدام الاستبيانات لجمع البيانات الكمية من المتخصصين في الأمان السيبراني، والمطورين، ومديري الأنظمة. يمكن أيضاً استخدام المقابلات المتعمقة لجمع بيانات نوعية من الخبراء للحصول على رؤى أكثر تفصيلاً حول التحديات التي تواجهها الأنظمة في حماية البيانات الحساسة. هذه الأدوات تتناسب مع هدف البحث المتمثل في فهم كيفية ضمان الأمان أثناء مشاركة البيانات الحساسة.

هل كان هناك وصف واضح عن مجتمع الدراسة والعينة وأدوات جمع البيانات من العينة؟ نعم، يجب أن يتضمن البحث وصفاً دقيقاً لمجتمع الدراسة والعينة المستهدفة. على سبيل المثال، يمكن أن يتضمن مجتمع الدراسة مختصين في الأمان السيبراني أو مطورين ومهندسين يعملون على منصات البيانات الكبيرة. يجب أن تكون العينة ممثلة للمجتمع المهني المتعلق بالأمان السيبراني وبيانات منصات البيانات الكبيرة. أدوات جمع البيانات يجب أن تشمل استبيانات تُوزع على هؤلاء المحترفين أو مقابلات مع خبراء في الأمان لحصر المشاكل والحلول المستخدمة. كما يجب أن يتم توضيح الأساليب الإحصائية المستخدمة لتحليل البيانات، مثل تحليل الانحدار أو الاختبارات الإحصائية المناسبة لدراسة العوامل المؤثرة في الأمان.

هل كانت العينة مناسبة من حيث الحجم لتفصيل الدراسة؟ نعم، من المهم أن تكون العينة كبيرة بما يكفي للحصول على نتائج موثوقة ودقيقة. في هذا النوع من الدراسات، قد يتطلب الأمر أخذ عينة من عدة جهات مختصة تعمل في مجال الأمان السيبراني على منصات البيانات الكبيرة. حجم العينة يجب أن يكون مناسباً لتغطية تنوع الأساليب الأمنية المستخدمة في هذه المنصات ويفضل أن تكون متنوعة بما يتناسب مع مختلف منصات البيانات الكبيرة مثل منصات السحابة أو الأنظمة الموزعة.

هل كانت خصائص العينة تناسب موضوع الرسالة؟ نعم، يجب أن تكون خصائص العينة متوافقة مع موضوع الرسالة. بما أن البحث يركز على الأمان في منصات البيانات الكبيرة، فمن الضروري أن تشمل العينة أفراداً لديهم معرفة وخبرة في العمل على هذه المنصات أو في مجال الأمان السيبراني. خصائص العينة، مثل مستوى الخبرة في الأمن السيبراني أو الخبرة في منصات البيانات الكبيرة، ستضمن جمع بيانات ذات صلة ودقة عالية فيما يخص الإجراءات الأمنية وطرق حماية البيانات الحساسة.

عند استخدام برامج إحصائية مثل SPSS ، R ، أو غيرها)، هل تم توضيح كيفية استخدام هذه البرامج وما هي الاختبارات الإحصائية التي تم استخدامها؟ نعم، في حالة استخدام برامج إحصائية مثل SPSS أو R ، يجب توضيح كيفية استخدام هذه البرامج لتحليل البيانات. على سبيل المثال، قد يتم استخدام SPSS لإجراء تحليلات انحدار لفهم العلاقة بين العوامل الأمنية وأداء منصات البيانات الكبيرة. قد يتم أيضاً استخدام اختبارات إحصائية مثل تحليل التباين (ANOVA) لتحديد مدى تأثير أساليب الأمان المختلفة على حماية البيانات الحساسة. يجب أن يتم توضيح كيفية استخدام هذه البرامج في الدراسة، مع ذكر الاختبارات الإحصائية التي تتماشى مع الأهداف البحثية وتحليل البيانات بشكل دقيق.

اسم المؤلف:

Saeed Anwar, S. A. M. Rizvi, and R. K. Gupta•

عنوان البحث:

Secure Sensitive Data Sharing on a Big Data Platform•

تاريخ النشر:

٢٠١٤٠

الموقع :

<https://ieeexplore.ieee.org/abstract/document/7040516>



Thank You