

The dangers of artificial intelligence in breaching individuals' privacy

مخاطر الذكاء الاصطناعي في اختراق خصوصية الافراد

Abeer Ahmed Musleh

عبير احمد مصلح

ID:2021205764

مشروع تخرج ١

كلية الإدارة-جامعة ميدأوشن

إشراف

د.منى مصطفى العشري

عضو هيئة التدريس-كلية الإدارة-جامعة ميدأوشن

جدول المحتويات

1. الصفحة الرئيسية
2. الفهرس
3. المقدمة
4. المشكلة
5. الاهمية
6. ضحايا الذكاء الاصطناعي
7. الاسئلة
8. الاهداف الرئيسية
9. الاهداف الفرعية
10. الفرضيات
11. نموذج البصلة
12. منهجية البحث
13. طرق الحماية من مخاطر الذكاء الاصطناعي
14. الإطار النظري
15. دراسات سابقة
16. المراجع
17. توصيات

مخاطر الذكاء الاصطناعي: مقدمة

في عصر تسارع التطور التكنولوجي، أصبح الذكاء الاصطناعي واحدًا من أكثر المواضيع اهتمامًا ونقاشًا. يتيح الذكاء الاصطناعي إمكانيات هائلة للتحسينات في مختلف المجالات، مثل الطب، والصناعة، والتجارة، والترفيه. ومع ذلك، فإن هذا التقدم السريع يثير قلقًا بشأن المخاطر والتحديات التي قد تنجم عن تطبيقات الذكاء الاصطناعي مثل

فقدان الوظائف: يثير التطور السريع في مجال الذكاء الاصطناعي مخاوف من فقدان الوظائف البشرية. فتطبيقات الذكاء الاصطناعي قد تؤدي إلى الأتمتة في العديد من الصناعات، مما يقلل من الحاجة إلى العمالة البشرية ويؤثر على سوق العمل.

الخصوصية والأمان: يشكل استخدام الذكاء الاصطناعي تحديات كبيرة في ما يتعلق بالخصوصية والأمان، حيث يمكن أن تكون البيانات الشخصية والحساسة عرضة للاختراق والاستغلال

تطور غير مراقب: يمكن أن يؤدي التطور السريع في مجال الذكاء الاصطناعي إلى ظهور تطبيقات غير مراقبة، مما يزيد من المخاطر والتحديات التي يمكن أن تنشأ عنها

يجب على الجهات المعنية أن تدرك المخاطر المحتملة لتطبيقات الذكاء الاصطناعي وتتخذ التدابير اللازمة لتقليل هذه المخاطر وضمان استخدام التكنولوجيا بطريقة آمنة ومسؤولة

أتي الذكاء الاصطناعي كأحدث تطور في هذا السياق، مما يثير قضايا جديدة تتعلق بحماية خصوصية الأفراد. سيتم في هذا البحث استكشاف مخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد، وتسليط الضوء على أهمية التحذير من هذه المخاطر واتخاذ الإجراءات الوقائية المناسبة

التجميع الضخم للبيانات: يتيح الذكاء الاصطناعي جمع وتحليل كميات ضخمة من البيانات، مما يمكن أطرًا غير مخولة من الوصول إلى معلومات شخصية دقيقة حول الأفراد

تقنيات التعرف على الوجوه والصوت: قد تستخدم التقنيات المتقدمة للتعرف على الوجوه والصوت في انتهاك خصوصية الأفراد، حيث يمكن استخدامها للتجسس أو التحقق من هوية الأفراد بدون موافقتهم

نقص الأمان في التطبيقات والأجهزة: يمكن أن يؤدي نقص الأمان في التطبيقات والأجهزة التي تستخدم التكنولوجيا الذكية إلى تسرب معلومات الخصوصية، سواء عن طريق الاختراقات السيبرانية أو الثغرات في البرمجيات

إن حماية خصوصية الأفراد في عصر الذكاء الاصطناعي تتطلب توعية شاملة جب على الشركات والمؤسسات الالتزام .
بمعايير الأمان الصارمة وضمان أن تكون عمليات جمع واستخدام البيانات شفافة وموافق عليها من قبل الأفراد

النصائح حول كيفية التعامل مع مخاطر الذكاء الاصطناعي بحذر

-

التثقيف والوعي: يجب على الأفراد والمؤسسات أن يتعلموا عن مخاطر الذكاء الاصطناعي وكيفية التعامل معها بشكل آمن. يمكن ذلك من خلال حضور الدورات التعليمية، وقراءة المقالات، ومتابعة التطورات في هذا المجال

التحقق من الأمان: يجب على الشركات والمطورين التأكد من أمان التطبيقات والأنظمة الذكية، وتنفيذ التحديثات اللازمة لسد الثغرات الأمنية بشكل فوري

الشفافية : يجب على الشركات والمنظمات أن تكون شفافة في جمع البيانات واستخدامها، وتقديم المعلومات اللازمة للأفراد حول كيفية تخزين ومعالجة بياناتهم

باختصار، يمكن تقليل مخاطر الذكاء الاصطناعي من خلال التثقيف والتوعية، وتطوير السياسات والقوانين الصارمة، وتفعيل التدابير الأمنية، والتحافظ على الشفافية وممارسة الاستخدام المسؤول للتكنولوجيا الذكية

مشكلة البحث

تكمن أهمية التكنولوجيا الحديثة في توفير الجهد والوقت وتنمية المحيط الاقتصادي والاجتماعي للبلد، فمعالجة هذه التقنية الحديثة وما تقدمه من فوائد علمية في المجالات المعرفية والاقتصادية والإستراتيجية، تدفع المجتمعات النامية لمواكبة هذا التطور ولتحسين قدراتها العلمية، وتحقيقاً لأهدافها التنموية خاصة بتطبيق الذكاء الاصطناعي، وإن عدم توظيف التكنولوجيا في الاتجاه الايجابي يسبب لها الكثير من المخاطر في المجالات الاقتصادية ونستعرض مضمون الذكاء الاصطناعي وأهميته في عملية التنمية الاقتصادية والاجتماعية في الدول النامية وفي الأخير

من مخاطر الذكاء الاصطناعي

اليوم ومع التطور الهائل في مستوى التكنولوجيا وتطبيقاتها، فقد تحول الأمر إلى أخطار أخرى؛ روبوتات سيصل ذكاؤها إلى درجة تسمح لها بالتفوق على البشر، بخاصة مع قدرات الذكاء الاصطناعي، أو فيروسات حاسوبية مدمرة توقف الإنترنت عن العمل. الذكاء الاصطناعي هو الموضوعة الجديدة التي يدور الحديث حولها في كل المجالات، في أجهزة الهواتف الذكية، في الأجهزة المنزلية، في التلفزيونات، في الأسلحة، وأيضاً في السيارات الذكية، التي يفترض أن تنتشر قريباً في شوارع مدننا خلال 5 سنوات.. القلق الحقيقي، وفق بعض الخبراء، هو أنه وبحلول العام 2075، ستصل آلات مزودة بقدرات خاصة إلى مستويات ذكاء تفوق مستوى الإنسان تمكنها من اتخاذ قرارات بشكل ذاتي، من دون العودة إلى أي مرجعية بشرية. وعينت «غوغل» مؤخراً مجلساً للأخلاقيات والتعامل مع القضايا الخادعة المتعلقة بالذكاء الاصطناعي ومساعدة الشركة على مواجهة الانتقادات المتعلقة بصفتها في هذا المجال.

امثلة :

الاحتيال الأوتوماتيكي، أو إنشاء حسابات بريد إلكتروني مزيفة، ومواقع إلكترونية، وروابط إلكترونية لسرقة المعلومات. عمليات اختراق أسرع من خلال الكشف الآلي عن البرمجيات التي يمكن اختراقها. ممارسة الإقناع الشخصي، حيث يمكن استغلال المعلومات المتوفرة للعموم لاستهداف شخص بذاته والتأثير على رأيه.

لا يعني ذلك حالة من «الاستسلام لما يجري»، فالباحثون يعملون منذ الآن على وضع بعض الحلول الممكنة لهذه المشاكل.

ويبقى السؤال الى اي مدى ممكن اي يؤثر الذكاء الاصطناعي على المجتمع ومخاطره؟

اهمية البحث

إن حماية خصوصية الأفراد في عصر الذكاء الاصطناعي تتطلب توعية شاملة جب على الشركات والمؤسسات الالتزام .
بمعايير الأمان الصارمة وضمان أن تكون عمليات جمع واستخدام البيانات شفافة وموافق عليها من قبل الأفراد

خلال العقود الخمسة الماضية، كانت المخاطر التي دأب كثيرون على التحذير منها هي الانفجار السكاني، نقصان المصادر الطبيعية والمعادن، التلوث البيئي، واحتمال وقوع حرب نووية.. أما اليوم ومع التطور الهائل في مستوى التكنولوجيا وتطبيقاتها، فقد تحول الأمر إلى أخطار أخرى؛ روبوتات سيصل ذكاؤها إلى درجة تسمح لها بالتفوق على البشر، بخاصة مع قدرات الذكاء الاصطناعي، أو فيروسات حاسوبية مدمرة توقف الإنترنت عن العمل

الذكاء الاصطناعي هو الموضة الجديدة التي يدور الحديث حولها في كل المجالات، في أجهزة الهواتف الذكية، في الأجهزة المنزلية، في التلفزيونات، في الأسلحة، وأيضاً في السيارات الذكية، التي يفترض أن تنتشر قريباً في شوارع مدننا خلال 5 سنوات.. القلق الحقيقي، وفق بعض الخبراء، هو أنه وبحلول العام 2075، ستصل آلات مزودة بقدرات خاصة إلى مستويات ذكاء تفوق مستوى الإنسان تمكنها من اتخاذ قرارات بشكل ذاتي، من دون العودة إلى أي مرجعية بشرية. وعينت «غوغل» مؤخراً مجلساً للأخلاقيات والتعامل مع القضايا الخادعة المتعلقة بالذكاء الاصطناعي ومساعدة الشركة على مواجهة الانتقادات المتعلقة بصفتها في هذا المجال.

يعتبر إحدى أكثر التطورات التكنولوجية إثارة وتأثيراً في العصر الحالي، وله العديد من الأهمية (AI) الذكاء الاصطناعي البارزة

- التحسينات في الأداء والكفاءة: يمكن للذكاء الاصطناعي تحسين أداء العمليات والمهام في مجموعة متنوعة من المجالات مثل الطب، والصناعة، والخدمات المالية، وغيرها. يمكن للأنظمة الذكية تحسين كفاءة الإنتاجية وتقليل الأخطاء
- تطوير التطبيقات الذكية: يمكن للذكاء الاصطناعي تطوير تطبيقات ذكية تعمل على تلبية احتياجات المستخدمين بشكل أفضل، سواء في مجالات التجارة الإلكترونية، أو الرعاية الصحية، أو التعليم، أو غيرها
- دعم التفاعل البشري: يمكن للذكاء الاصطناعي تحسين تجربة المستخدم من خلال توفير خدمات تفاعلية مثل مساعدات الذكاء الصناعي والروبوتات الذكية
- بشكل عام، يمكن القول إن الذكاء الاصطناعي يعزز التقدم التكنولوجي ويفتح أبواباً جديدة للابتكار والتطور في مجموعة واسعة من المجالات، مما يعزز الإنتاجية ويحسن جودة الحياة بشكل عام

ضحايا الذكاء الاصطناعي في اختراق الحسابات

هناك العديد من الحوادث التي أظهرت تأثير الذكاء الاصطناعي على اختراق الحسابات الشخصية، وبعض الضحايا الشهيرة تشمل

ضحايا في حوادث الاحتيال الإلكتروني: يتم استخدام الذكاء الاصطناعي في تنفيذ عمليات الاحتيال الإلكتروني، ويكون الأفراد الذين يسقطون ضحية لهذه الاحتمالات هم من أبرز الضحايا

الشركات والمؤسسات: قد تتعرض الشركات والمؤسسات للاختراقات باستخدام التقنيات الذكية، مما يؤدي إلى فقدان البيانات الحساسة أو تسريبها وخرق الخصوصية

الأفراد الشهيرة والشخصيات العامة: يمكن أن تكون الشخصيات الشهيرة والعامة هدفًا للاختراق باستخدام تقنيات الذكاء الاصطناعي، سواء للوصول إلى معلوماتهم الشخصية أو لنشر الأخبار الزائفة

الأفراد العاديين: يمكن لأي شخص أن يتعرض للاختراقات باستخدام التقنيات الذكية، سواء من خلال اختراق حساباته الشخصية على وسائل التواصل الاجتماعي أو البريد الإلكتروني، أو اختراق أجهزته الشخصية

الجهات الحكومية: يمكن أن تكون الحكومات هدفًا للاختراقات باستخدام التقنيات الذكية، مما يؤدي إلى تسريب معلومات سرية أو تأثير عمليات الانتخابات أو تعطيل البنية التحتية للدولة

هذه الأمثلة تظهر كيف يمكن للذكاء الاصطناعي أن يؤثر على خصوصية الأفراد من مختلف الجوانب، وتحديدًا في اختراق الحسابات الشخصية وسرقة المعلومات الحساسة

الناشطين السياسيين: قد يكون الناشطون السياسيون هدفًا للاختراق باستخدام الذكاء الاصطناعي حيث يمكن استخدام تلك التقنيات لاختراق حساباتهم الشخصية للتجسس على نشاطاتهم السياسية أو لتشويه سمعتهم

المؤسسات الصحفية ووسائل الإعلام: قد تكون وسائل الإعلام والمؤسسات الصحفية هدفًا للاختراق باستخدام التقنيات الذكية، حيث يمكن للمهاجمين الوصول إلى المعلومات الحساسة أو تزوير الأخبار

المؤسسات المالية: يمكن أن تتعرض المؤسسات المالية للاختراقات باستخدام التقنيات الذكية، مما يؤدي إلى سرقة البيانات المالية الحساسة للعملاء أو تعريضها للتلاعب

اسئلة البحث الفرعية

ما هي الإجراءات التي يمكن اتخاذها لحماية خصوصية الأفراد؟

ما هي المخاطر الأمنية المرتبطة بالذكاء الاصطناعي؟

هل هناك أمثلة على قرارات خاطئة تم اتخاذها بواسطة الذكاء الاصطناعي؟

ما هي الإجراءات الواجب اتخاذها للحد من مخاطر الذكاء الاصطناعي؟

أهداف البحث:-هي

الهدف العام

تحديد المخاطر المحتملة المرتبطة بالذكاء الاصطناعي وتحديد النقاط الضعيفة في النظام

الأهداف الفرعية

تطوير السياسات والإجراءات: وضع سياسات وإجراءات تنظم استخدام الذكاء الاصطناعي وتحمي خصوصية الأفراد

التدريب والتوعية: توعية الموظفين والمستخدمين بمخاطر الذكاء الاصطناعي وتوفير التدريب اللازم

تحليل التأثيرات الاجتماعية: استكشاف كيف يؤثر الذكاء الاصطناعي على المجتمعات والثقافات، بما في ذلك التأثيرات على سوق العمل والتواصل الاجتماعي والتفاعلات الثقافية

تطوير تقنيات الحماية والأمان: البحث في تطوير تقنيات الحماية الجديدة التي يمكن أن تساعد في تقليل مخاطر الذكاء الاصطناعي وتحسين الأمان الرقمي

فرضيات البحث

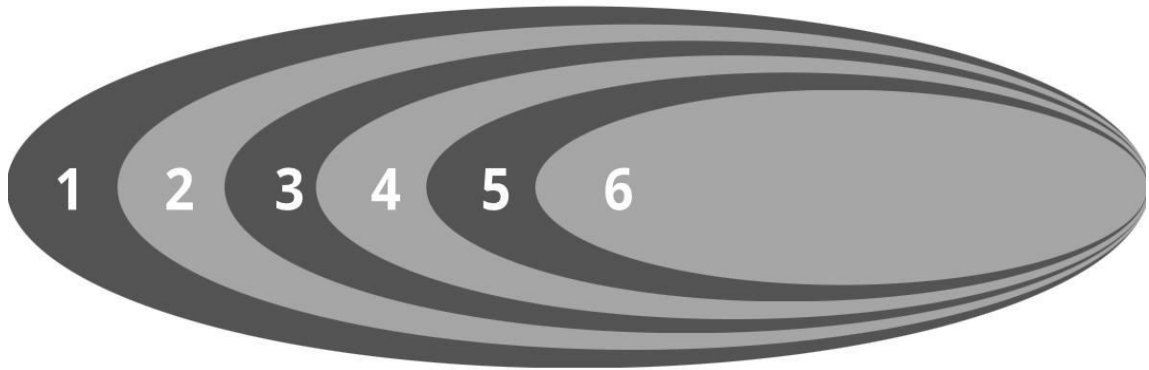
تأثير الذكاء الاصطناعي على سوق العمل

تطور التكنولوجيا واستخدام الذكاء الاصطناعي في مختلف الصناعات قد يؤدي إلى فقدان فرص العمل للعديد من الأشخاص في المهن التقليدية، مما قد يؤثر على سوق العمل بشكل عام

تهديد الذكاء الاصطناعي على الخصوصية الفردية هذه الفرضية تقترح أن استخدام تقنيات الذكاء الاصطناعي في جمع ومعالجة البيانات الشخصية يمكن أن يعرض خصوصية الأفراد للخطر، حيث يمكن أن يتم استغلال هذه البيانات بشكل غير قانوني أو غير مرغوب فيه.

خطر نقص الشفافية والمساءلة في تطبيقات الذكاء الاصطناعي هذه الفرضية تقترح أن نقص الشفافية والمساءلة في تطبيقات الذكاء الاصطناعي يمكن أن يؤدي إلى تبعات غير مرغوبة، مثل قرارات آلية غير مبررة أو انتهاكات لحقوق الإنسان، مما يجعل من الضروري وضع آليات رقابية فعالة لضمان استخدام الذكاء الاصطناعي بشكل أخلاقي ومسؤول.

نموذج البحث



1. الوضعية
2. الاستنتاجية
3. المسحية
4. الكمية
5. المقطعية
6. الاستبيانات

منهجية البحث

1-

فلسفة البحث: الاهتمام بالآثار السلبية الناتجة عن تقدم التكنولوجيا واستخدام الذكاء الاصطناعي. تتسم فلسفة مخاطر الذكاء الاصطناعي بتحليل عميق لتأثيرات هذه التكنولوجيا على الفرد والمجتمع بشكل عام، وتناقش القضايا الأخلاقية والاجتماعية التي قد تنشأ نتيجة لذلك.

حيث يتم التركيز على دراسة وتقدير التأثيرات السلبية المحتملة للاستخدام السيء أو غير الأخلاقي لتلك التكنولوجيا.

2-

منهج البحث: الطريقة التي يتم من خلالها تحليل وتقييم الآثار السلبية المحتملة لتطبيقات الذكاء الاصطناعي. يتمثل منهج مخاطر الذكاء الاصطناعي في عدة خطوات ومراحل تساعد على فهم وتقدير مدى تأثير هذه التكنولوجيا على الفرد والمجتمع إليك بعض عناصر منهج مخاطر الذكاء الاصطناعي

تحليل السياق: يتضمن هذه الخطوة دراسة السياق الاجتماعي والثقافي والقانوني الذي سيتم تطبيق تقنيات الذكاء الاصطناعي فيه، وفهم الصراعات والتحديات التي يمكن أن تنشأ نتيجة لذلك

تحديد المخاطر: تتمثل هذه الخطوة في تحديد وتصنيف المخاطر المحتملة التي قد تنشأ نتيجة لاستخدام تقنيات الذكاء الاصطناعي، مثل تهديدات الخصوصية أو ارتفاع معدلات البطالة بسبب التشغيل الآلي

تقييم المخاطر: يتم في هذه الخطوة تقييم مدى جدوى وتأثير المخاطر السابقة، وتحديد المخاطر ذات الأولوية العالية التي يجب التركيز عليها

تطوير استراتيجيات الحد من المخاطر: بناءً على التقييم السابق، يتم وضع استراتيجيات للحد من المخاطر وتقليل تأثيراتها، سواء كان ذلك من خلال تطوير أنظمة رقابية وأخلاقية أو تبني سياسات تنظيمية صارمة

رصد وتقييم النتائج: بعد تطبيق الاستراتيجيات المخططة، يجب على الباحثين والمهتمين بمخاطر الذكاء الاصطناعي متابعة النتائج وتقييم تأثيرها على المدى الطويل

باستخدام منهج مخاطر الذكاء الاصطناعي يمكن تحقيق فهم أعمق وأشمل لآثار تلك التكنولوجيا واتخاذ الإجراءات اللازمة للتصدي للمخاطر وضمان الاستفادة الأمثل منها في آن واحد

منهجية البحث

3-

استراتيجية البحث

استراتيجية مخاطر الذكاء الاصطناعي هي الخطة التي تقوم بها المؤسسات والحكومات والمجتمعات للتعامل مع المخاطر والتحديات التي قد تنشأ نتيجة لاستخدام تقنيات الذكاء الاصطناعي. إليك بعض عناصر استراتيجية مخاطر الذكاء الاصطناعي

وضع سياسات وأنظمة رقابة: يجب وضع سياسات وإطارات عمل تنظيمية قوية تحد من سلبية استخدام تقنيات الذكاء الاصطناعي، مثل حماية الخصوصية الشخصية ومراقبة استخدام البيانات

تعزيز الشفافية: ينبغي على المنظمات والشركات أن تكون شفافة فيما يتعلق بطريقة تطوير واستخدام تقنيات الذكاء الاصطناعي، وتوضيح النتائج المتوقعة والمخاطر المحتملة.

تدريب وتطوير المهارات: يجب تعزيز القدرات والمهارات الضرورية لفهم وتقييم تأثيرات تقنيات الذكاء الاصطناعي، وتحسين قدرة المجتمعات على التعامل معها.

التعاون والشراكات: من المهم تعزيز التعاون بين القطاعين العام والخاص والمجتمع المدني لتطوير استراتيجيات مشتركة للحد من مخاطر الذكاء الاصطناعي.

مراقبة وتقييم: يجب أن تكون هناك آليات مستمرة لرصد وتقييم تأثيرات تقنيات الذكاء الاصطناعي، وتعديل الاستراتيجيات والسياسات بناءً على النتائج.

التركيز على الأخلاقيات: يجب أن تكون الأخلاق والقيم الأخلاقية جزءاً أساسياً من استراتيجية مخاطر الذكاء الاصطناعي، ويجب على الجهات المعنية التصرف بنزاهة ومسؤولية في تطبيق تلك التكنولوجيا.

تعتبر هذه العناصر جزءاً من استراتيجية شاملة للتعامل مع المخاطر الناتجة عن استخدام التقنيات الذكاء الاصطناعي وضمان استفادة المجتمعات منها بشكل آمن ومسؤول.

منهجية البحث

4-

نوع البحث: بحث مخاطر الذكاء الاصطناعي يمكن أن يكون من نوعي أو كمي
البحث النوعي: يستخدم هذا النوع من البحث لفهم واستكشاف آراء وتجارب الأفراد والمجتمعات حول مخاطر الذكاء الاصطناعي. يعتمد هذا البحث على جمع البيانات من خلال مقابلات شخصية، مجموعات نقاش، استطلاعات رأي، وتحليل المضامين لفهم التحديات والمخاطر التي يمكن أن تنشأ.

البحث الكمي: يستخدم هذا النوع من البحث لقياس وتحليل البيانات الكمية التي تتعلق بمخاطر الذكاء الاصطناعي. يعتمد هذا البحث على أدوات إحصائية وتحليل البيانات للكشف عن العلاقات والانماط الموجودة في البيانات، مثل تحليل الانحدار والتحليل العاملي.

5-

الأفق الزمني: مخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد يعتمد على عدة عوامل، بما في ذلك حجم وتعقيد المشروع، الموارد المتاحة، والأهداف المحددة. إليك بعض الخطوات التي يمكن تضمينها في إفق زمني لمثل هذا المشروع

تحليل الوضع الحالي: يجب أولاً إجراء تقييم شامل للوضع الحالي لخصوصية الأفراد ومخاطر الذكاء الاصطناعي في اختراقها.

وضع استراتيجية وخطة عمل: بناءً على التحليل السابق، يتعين وضع استراتيجية وخطة عمل مفصلة تحدد الأهداف، والخطوات المطلوبة لتحقيقها، والموارد المطلوبة.

تنفيذ الخطة: يتم تنفيذ الخطة وتطبيق التقنيات الضرورية لحماية خصوصية الأفراد من الاختراقات المحتملة.

مراقبة وتقييم: يتم مراقبة نتائج التنفيذ بانتظام لضمان أن الإجراءات المتخذة فعالة وتلبي الاحتياجات.

التحسين المستمر: يجري تقييم وتحسين الإجراءات بانتظام بناءً على التحليل الجديد للمخاطر والتغيرات المحتملة.

بالنظر إلى أن مجال الذكاء الاصطناعي متطور بسرعة، فإن الإفق الزمني لمثل هذا المشروع قد يكون مستمرًا مع التركيز على التحسين المستمر لحماية خصوصية الأفراد. يجب أيضًا أن تتابع التغييرات التشريعية والتكنولوجية لضمان التعديلات اللازمة على الاستراتيجيات والسياسات.

طرق الحماية من الذكاء الاصطناعي

استخدام كلمات مرور قوية: استخدم كلمات مرور قوية ومعقدة لحساباتك الشخصية، وتأكد من تغييرها بانتظام.

"password" تجنب استخدام كلمات مرور سهلة الاختراق مثل "123456" أو

التحقق بخطوتين: قم بتفعيل خيار التحقق بخطوتين لحساباتك الشخصية، والذي يضيف طبقة إضافية من

الأمان عند تسجيل الدخول عبر تأكيد الهوية عن طريق رمز أو رسالة نصية إلى هاتفك المحمول.

تحديث البرامج والتطبيقات: تأكد من تحديث البرامج والتطبيقات الخاصة بك بانتظام، حيث يتم تضمين تحديثات

الأمان لسد الثغرات التي يمكن أن يستغلها القراصنة.

تقييد الوصول: قم بتقييد الوصول إلى حساباتك الشخصية للأشخاص الذين تثق بهم فقط، وتجنب مشاركة معلومات

الدخول مع الغرباء أو في رسائل غير مؤمنة.

استخدام أدوات الأمان المتقدمة: ابحث عن أدوات الأمان المتقدمة التي تقدمها الخدمات عبر الإنترنت، مثل الكشف عن الاحتيال ومراقبة النشاط غير المعتاد على الحساب.

التوعية والتدريب: قم بتعلم مزيد من المعرفة حول كيفية تحديد الرسائل الاحتيالية والاحتيال عبر الإنترنت، وتأكد من تدريب نفسك وأفراد عائلتك على الحفاظ على الأمان الرقمي.

باستخدام هذه الإجراءات، يمكنك تقليل مخاطر اختراق الحسابات الشخصية وحماية بياناتك الشخصية من التسريب أو الاستغلال.

طرق الحماية من الذكاء الاصطناعي

التحقق من الرسائل الاحتيالية والصفحات الوهمية: تحقق دائماً من مصدر الرسائل الإلكترونية وروابط الويب قبل النقر

عليها، وتجنب تقديم معلومات الدخول إلى الحسابات الشخصية عبر روابط غير معروفة أو رسائل احتيالية.

تنشيط الإشعارات للنشاط غير المعتاد: قم بتنشيط إشعارات الحسابات لتلقي تنبيهات حول أي نشاط غير معتاد، مثل

تسجيل الدخول من موقع غير معتاد أو جهاز غير معروف.

للاتصال بالإنترنت، حيث توفر طبقة VPN قم باستخدام شبكات الـ (VPN) استخدام الشبكات الافتراضية الخاصة

.الخاص بك IP إضافية من الأمان عند تشفير بيانات الاتصال وإخفاء عنوان

التحقق من إعدادات الخصوصية والأمان: تحقق وقم بتعديل إعدادات الخصوصية والأمان لحساباتك الشخصية على

.الشبكات الاجتماعية والخدمات عبر الإنترنت لضمان أعلى مستويات الحماية

استخدام برامج مضادة للفيروسات والبرمجيات الخبيثة: قم بتنصيب برامج مضادة للفيروسات والبرمجيات الخبيثة على

.أجهزتك وحافظ على تحديثها بانتظام للكشف والوقاية من التهديدات السيبرانية

تقييد الوصول إلى البيانات الشخصية: احرص على تقييد الوصول إلى بياناتك الشخصية ومشاركتها مع الأشخاص

.الذين تثق بهم فقط، وتجنب مشاركة المعلومات الحساسة عبر الإنترنت

الإطار النظري

مقدمة

بحث مخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد يعتبر موضوعاً مهماً ومعقداً يستحق الاهتمام، حيث يندرج ضمن مجال أمن المعلومات وحماية البيانات الشخصية. تتعدد المخاطر التي قد يتعرض لها الأفراد نتيجة لاستخدام التكنولوجيا وتطبيقات الذكاء الاصطناعي، وتشمل هذه المخاطر

1. اختراق البيانات الشخصية: ** تتيج التقنيات الذكية وتطبيقات الذكاء الاصطناعي جمع كميات ضخمة من البيانات ** . الشخصية، والتي يمكن أن تكون عرضة للاختراقات السيبرانية والوصول غير المشروع إليها

- تسرب البيانات:** قد يؤدي اختراق الأنظمة أو الاستخدام غير الصحيح للبيانات إلى تسربها، مما يؤدي إلى تعرض ** 2. معلومات شخصية حساسة للمخاطر والاستغلال.
- التعرض للاستهداف الإعلان:** يمكن أن يستخدم الذكاء الاصطناعي لتحليل سلوكيات الأفراد وتوجيه الإعلانات بشكل ** 3. متطور، مما يؤدي إلى انتهاك خصوصيتهم وتعرضهم للتنقيب الدقيق.
- التمييز والتحيز:** يمكن للتطبيقات الذكية أن تسهل التمييز والتحيز غير المقصود على أساس البيانات، مما يؤثر سلباً ** 4. على حقوق الأفراد والمساواة.
- التصنيف الخاطئ واتخاذ القرارات الخاطئة:** قد يؤدي تحليل البيانات بواسطة الذكاء الاصطناعي إلى التصنيف ** 5. الخاطئ للأفراد أو اتخاذ قرارات خاطئة تؤثر على حياتهم بشكل سلبي.
- لذلك، يتطلب بحث مخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد دراسة متعمقة للتحديات الأمنية والأخلاقية والقانونية التي قد تواجهها الأفراد في ظل تطور التكنولوجيا واستخداماتها المتزايدة. يتعين تطوير إطار قانونية وأخلاقية قوية لحماية خصوصية الأفراد وضمان استخدام التكنولوجيا الذكية بشكل آمن ومسؤول.

الإطار النظري

المتغير الاول

مخاطر الذكاء الاصطناعي

مخاطر الذكاء الاصطناعي تتنوع وتشمل عدة جوانب، من بينها

1. تهديدات أمنية واختراقات: ** قد تتعرض الأنظمة التي تعتمد على الذكاء الاصطناعي للاختراقات السيبرانية، مما ** 1. يعرض البيانات والمعلومات للسرقة أو التلاعب، ويسهم في تعريض الأفراد والمؤسسات للخطر
 2. تفاوت القدرات: ** قد تؤدي تطورات الذكاء الاصطناعي إلى زيادة التفاوت في القدرات بين الدول والشركات والأفراد، ** 2. مما يؤثر على العدالة الاجتماعية ويزيد من الفجوات الاقتصادية والاجتماعية
 3. فقدان الوظائف: ** يثير استخدام التكنولوجيا الذكية والروبوتات مخاوف من فقدان الوظائف للعمال البشريين، خاصة في ** 3. الصناعات التي يمكن أن تتميز بالتأأة التكنولوجية
 4. التحيز والتمييز: ** يمكن للنظم الذكية أن تكون مصدرًا للتحيز والتمييز بناءً على بيانات معينة أو نماذج تدريبية، مما ** 4. يؤثر على توزيع الفرص والمساواة
 5. فقدان السيطرة: ** قد تتسبب الأنظمة الذكية المعقدة في فقدان السيطرة على القرارات والعمليات، مما يزيد من التبعات ** 5. الخطيرة في حالة وقوع أخطاء أو تحكم ذاتي غير مرغوب فيه
 6. تهديدات أمن السلامة: ** يمكن أن يتسبب الاستخدام غير الآمن لتقنيات الذكاء الاصطناعي في تهديدات لأمن وسلامة ** 6. الأفراد، مثل استخدام التكنولوجيا في أنظمة المرور الذكية أو الرعاية الصحية دون اتخاذ الاحتياطات اللازمة
 7. التطور الأخلاقي: ** يطرح تقدم التكنولوجيا الذكية تحديات أخلاقية جديدة، مثل قضايا الخصوصية والمسؤولية والعدالة، ** 7. التي يجب معالجتها بشكل فعال لضمان استخدام التكنولوجيا بطريقة مسؤولة وأخلاقية
- تلك هي بعض المخاطر الشائعة للذكاء الاصطناعي، ومن المهم التعرف عليها ودراساتها بعناية لضمان تطوير واستخدام التكنولوجيا الذكية بشكل آمن وفعال

مخاطر الذكاء الصناعي

الاستبدال

يمكن أن يؤدي تطور الذكاء الصناعي إلى استبداده بالبشر وتحكمه في حياتهم

إنعدام التحكم

قد يتحكم الذكاء الصناعي بشكل غير متوقع في بعض الأحيان ما يؤدي إلى أضرار بالنظام الذي يعمل به

البطالة

قد يؤدي تطور الذكاء الصناعي إلى فقدان بعض الوظائف التي تعتمد على العمل اليدوي أو المهارات الأساسية

الأخطاء

يمكن أن يحدث خطأ في برمجة الذكاء الصناعي ما قد يؤدي إلى تداعيات سلبية على المجتمع

الخصوصية

يمكن للذكاء الصناعي أن يتحكم في بيانات الأفراد بشكل غير مشروع وينتهك الخصوصية

التمييز

يمكن للذكاء الصناعي أن يمارس التمييز الجنسي أو العرقي أو غيره

المتغير الثاني

خصوصية الأفراد هي حق أساسي وأساسي يتمتع به كل فرد لحماية معلوماته الشخصية والحفاظ على سرية حياته الخاصة. تشمل حقوق الخصوصية العديد من الجوانب، بما في ذلك

1. السيطرة على البيانات الشخصية: ** حق الفرد في التحكم في جمع واستخدام ومشاركة بياناته الشخصية، وفقاً لما يراه ** .
مناسباً
2. الحفاظ على السرية: ** حق الفرد في حماية بياناته الشخصية من الوصول غير المرغوب فيه من قبل الآخرين، سواء ** .
كانوا أفراداً أو مؤسسات
3. الحق في النسيان: ** حق الفرد في طلب حذف بياناته الشخصية بشكل دائم من نظم معالجة البيانات، في حالة عدم ** .
الحاجة إليها بعد الآن
4. الإبلاغ عن انتهاكات الخصوصية: ** حق الفرد في الإبلاغ عن أي انتهاكات لخصوصيته واستخدام غير مشروع لبياناته ** .
الشخصية
5. النقل المحمي للبيانات: ** حق الفرد في نقل بياناته الشخصية بشكل آمن ومحمي إلى أماكن أخرى، وذلك عند الانتقال من ** .
خدمة إلى أخرى أو من دولة إلى أخرى

يعتبر احترام خصوصية الأفراد أمراً بالغ الأهمية في العصر الرقمي الحديث، خاصة مع تزايد حجم جمع ومعالجة البيانات الشخصية. تطوير السياسات والتشريعات التي تحمي خصوصية الأفراد وتنظم استخدام بياناتهم يساهم في بناء بيئة رقمية آمنة وموثوقة.

الإطار النظري

العلاقة بين المتغيرات

هناك عدة علاقات بين مخاطر الذكاء الاصطناعي وخصوصية الأفراد، وهذه العلاقات تظهر كيف يمكن أن يتأثر حق الأفراد في الخصوصية نتيجة لتطبيقات الذكاء الاصطناعي. إليك بعض العلاقات الرئيسية بينهما

1. جمع البيانات الشخصية: **تتطلب تطبيقات الذكاء الاصطناعي جمع كميات كبيرة من البيانات الشخصية لتدريب ** 1. النماذج الذكية. وبما أن هذه البيانات تتضمن معلومات حساسة عن الأفراد، مثل المواقع والتفاصيل الطبية والعادات الشخصية، يمكن أن يؤدي جمعها بشكل غير مراقب أو غير مشروع إلى انتهاك خصوصية الأفراد.
 2. تحليل البيانات وتوقع السلوك: **يستخدم الذكاء الاصطناعي لتحليل البيانات الشخصية وتوقع سلوك الأفراد، مما قد يؤدي إلى انتهاك خصوصيتهم إذا تم استخدام هذه المعلومات بطرق غير مشروعة أو غير مرغوب فيها.
 3. التسويق المستهدف والإعلان: **يمكن لتقنيات الذكاء الاصطناعي أن تستخدم لتوجيه الإعلانات والتسويق المستهدف ** 3. بناءً على بيانات شخصية، مما يعرض خصوصية الأفراد للتعرض للرسائل غير مرغوب فيها والتتبع الدقيق لسلوكياتهم.
 4. التحليل السلوكي واتخاذ القرارات الآلية: **يمكن للأنظمة التي تعتمد على الذكاء الاصطناعي أن تحلل سلوك الأفراد ** 4. وتتخذ قرارات آلية بناءً عليه، مما يمكن أن يؤثر على خصوصية الأفراد إذا لم يتم احترام حقهم في السيطرة على بياناتهم الشخصية.
- بشكل عام، يمكن أن يؤدي استخدام التكنولوجيا الذكية بشكل غير مراقب أو غير مشروع إلى تعريض خصوصية الأفراد للخطر، لذا من الضروري تطوير سياسات وتشريعات تحمي خصوصية الأفراد وتضمن استخدام التكنولوجيا بشكل آمن ومسؤول.

دراسات سابقة

تختلف القضايا الأخلاقية المتعلقة بالبناء المستقبلي المحتمل للقدرات الفكرية العامة التي تتجاوز القادة

البشريين تمامًا عن أي مشاكل أخلاقية ناشئة في أنظمة المعلومات الحالية والمعلوماتية. لن يكون هؤلاء الخبراء مجرد تطور تكنولوجي آخر ؛ سيكون هذا الاختراع هو الأكثر أهمية على الإطلاق ، وسيؤدي إلى

التقدم المتفجر في جميع المجالات العلمية والتكنولوجية ، حيث ستم العملية الإلهية بكفاءة خارقة

للطبيعة. إلى الحد الذي تكون فيه الأخلاقيات هي السعي المعرفي ، يمكن للبشر بسهولة أن يتجاوز

لتحديد SuperTelligence البشر في جودة تفكيرهم الأخلاقي. ومع ذلك ، فإن الأمر متروك لمصممي

دوافعه الأصلية. منذ عملية الإلغاء ، قد تصبح قوية بطريقة لا جدال فيها بسبب تفوقها الفكري

والتقنيات التي يمكن أن تتطور ، من المهم توفيرها للدوافع البشرية. تستقر هذه الورقة في بعض القضايا الأخلاقية الفريدة في خلق الإلغاء ، وتناقش الدوافع التي يجب أن نقدمها لإعطاء الذكاء ، وتقديم بعض

الاعتبارات من التكلفة والفوائد المتعلقة بما إذا كان ينبغي تسريع تطوير الآلات الممتازة

هناك العديد من الدراسات التي تناولت موضوع مخاطر الذكاء الاجتماعي في اختراق خصوصية الأفراد. واحدة من هذه الدراسات هي دراسة أجرتها جامعة هارفارد في عام 2014، حيث توصلت الدراسة إلى أن استخدام وسائل التواصل الاجتماعي يمكن أن يؤدي إلى تقليل مستوى الخصوصية والأمان الشخصي للأفراد، ويزيد من احتمالية تعرضهم للاختراقات السلبية.

كما أجرت جامعة ستانفورد دراسة أخرى في عام 2018 حول تأثير شبكات التواصل الاجتماعي على الخصوصية، وخلصت الدراسة إلى أن الكثير من الأفراد يقومون بمشاركة معلومات شخصية دون النظر إلى العواقب، مما يجعلهم عرضة للاختراق والاستغلال.

بإجراء دراسة حول سلوكيات المستخدمين على وسائل Nielsen بالإضافة إلى ذلك، قامت شركة أبحاث السوق العالمية التواصل الاجتماعي، ووجدت أن العديد من الأشخاص يقومون بمشاركة معلومات حساسة دون التفكير في عواقب ذلك، مما يعرضهم لمخاطر الاختراق وانتهاك الخصوصية

هذه الدراسات تسلط الضوء على أهمية التوعية بمخاطر الذكاء الاجتماعي في اختراق خصوصية الأفراد، وضرورة اتخاذ إجراءات وقيد لحماية خصوصيتنا وأماننا الشخصي عند استخدام وسائل التواصل الاجتماعي والتكنولوجيا

دراسات سابقة

هناك العديد من الدراسات التي تناولت موضوع مخاطر الذكاء الاجتماعي في اختراق خصوصية الأفراد، ومن بين هذه الدراسات:

1. في عام 2019 وقامت بتحليل تأثير استخدام وسائل "Computers in Human Behavior" دراسة نُشرت في مجلة. التواصل الاجتماعي على خصوصية الأفراد. وجدت الدراسة أن الأشخاص الذين يتفاعلون بكثافة على وسائل التواصل الاجتماعي يكونون أكثر عرضة لمخاطر انتهاك الخصوصية

2. في عام 2018 حيث اتضح أن انتشار الهواتف الذكية ووسائل التواصل Kaspersky Lab دراسة أجرتها شركة. الاجتماعي قد زادت من مخاطر الاختراق وسرقة البيانات الشخصية

3. دراسة أجرتها جامعة كاليفورنيا في سانتا باربرا في عام 2020 تحذر من خطورة تسريب المعلومات الشخصية عبر وسائل التواصل الاجتماعي وتأثير ذلك على خصوصية الأفراد

تلك الدراسات تشير جميعاً إلى أهمية التوعية بمخاطر انتهاك الخصوصية واختراق البيانات الشخصية عبر وسائل التواصل الاجتماعي، وضرورة اتخاذ إجراءات احترازية للحفاظ على خصوصيتنا وتأمين بياناتنا الشخصية من التهديدات السلبية

دراسة أخرى أجرتها الباحثة الأمريكية ميشيل غيلادو في جامعة جورج ماسون، حيث نشرت دراسة في عام 2018 تحلل تأثير وسائل التواصل الاجتماعي على خصوصية الأفراد وكشفت عن مخاطر انتهاك الخصوصية من خلال منصات التواصل الاجتماعي الشهيرة

ووجدت الدراسة أن الأفراد الذين ينشرون معلومات شخصية على وسائل التواصل الاجتماعي قد يكونون عرضة للاختراق وانتهاك الخصوصية، خاصة إذا كانوا يتبعون عادات استخدام تقليدية لقفل الخصوصية أو لم يكونوا ملمين بأمور الأمان الرقمي.

تؤكد هذه الدراسة على أهمية توجيه الإنتباه إلى مخاطر نشر المعلومات الشخصية على وسائل التواصل الاجتماعي وضرورة الحفاظ على الخصوصية والأمان الرقمي من خلال ممارسات سليمة ووعي تقني

دراسات سابقة

إن موضوع المخاطر المحتملة والمتعلقة بالتقدم السريع لتقنيات الذكاء الاصطناعي أصبح من الموضوعات المهمة المتداولة

في الوقت الحاضر، وهي كغيرها من التقنيات والتكنولوجيا، تعد أنظمة وتقنيات مفيدة للغاية، لكن قد تظهر لها مخاطر

وأثار جسيمة لأسباب وعوامل عدة، منها الرغبة في النفوذ أو السيطرة، أو بسبب ضغوط تنافسية، أو غيرها من العوامل

الأخرى. ولعل من بين هذه المخاطر -على سبيل المثال- صعوبة تحقيق التحكم الكامل عليها، لكونها يمكن أن تتطور بشكل سريع وغير متوقع وتتجاوز التوقعات البشرية لها، وذلك قد يؤدي إلى حدوث أعمال أو قرارات غير مرغوب فيها أو ضارة

وخطيرة، كزراعة تقنيات الشرائح الإلكترونية الذكية في أدمغة البشر من شركة نيورالينك، والمخاوف والمخاطر من جراء

،ذلك، كما يمكن توظيف تقنيات الذكاء الاصطناعي في الأنشطة الإجرامية والخداعية، مثل الاحتيال الإلكتروني

والاختراقات السيبرانية، والتضليل الإعلامي، والتلاعب بالأسواق الاقتصادية، وغيرها من الأنشطة غير القانونية وغير

الأخلاقية، ما قد يصعد الجريمة ويعقد الجهود في مكافحتها. ومن الأمثلة أيضا، مع تزايد الكم الهائل من البيانات التي

،تتعامل معها أنظمة وتقنيات الذكاء الاصطناعي، يمكن أن تتعرض هذه البيانات للاختراق أو الاستغلال غير المشروع

وذلك سيشكل تهديدا واضحا للخصوصية والأمان. كما أن الاعتماد الكبير على الذكاء الاصطناعي في النظم الحيوية

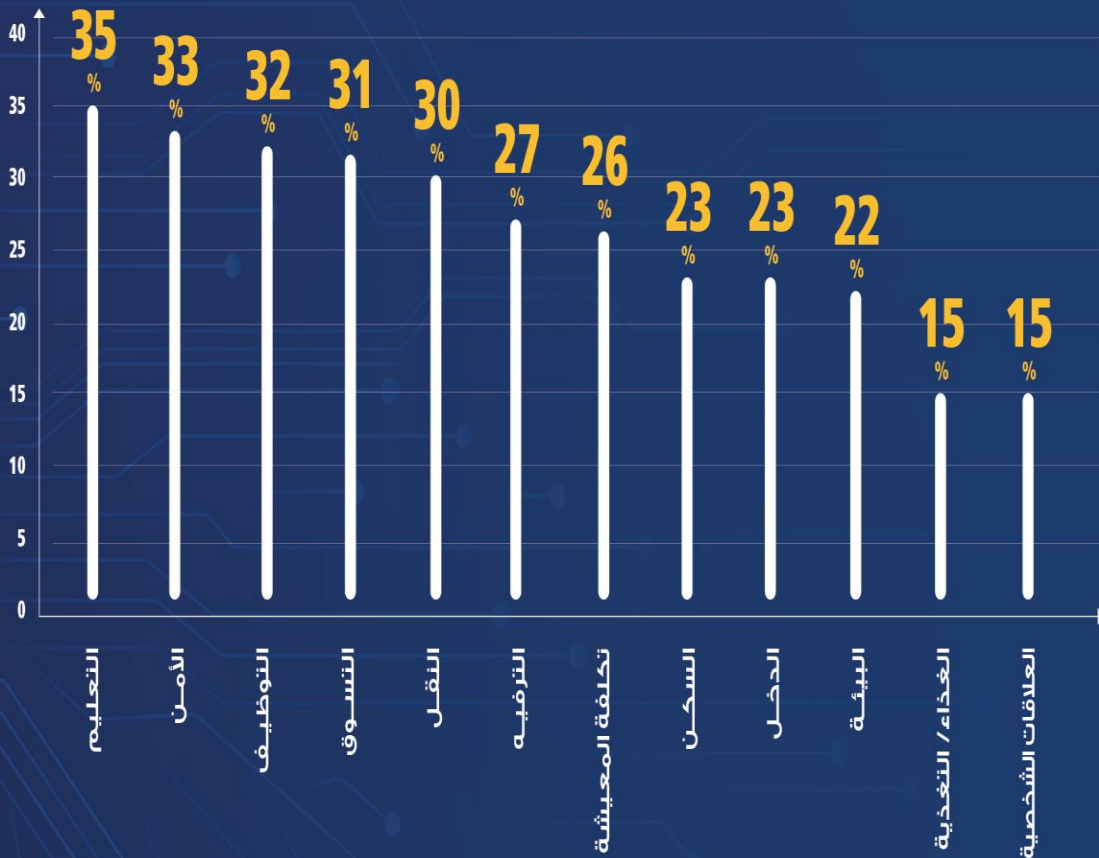
الحساسة يؤدي إلى تهديد الأمان والسلامة العامة، والاعتماد الزائد على هذه التقنيات قد يتسبب أيضا في تقليل

التحكم البشري في كثير من العمليات واتخاذ القرارات، وهذا بالتالي قد ينتج عنه كثير من الأخطاء أو الأعمال غير

.المرغوب فيها أو غير المتوقعة أو صعبة الحل

كيف سيغير الذكاء الاصطناعي حياتنا؟

نسبة المستجيبين يتوقعون أي من المجالات التالية سيحدث له أكبر تغيير
* من خلال استخدام الذكاء الاصطناعي في السنوات الثلاث إلى الخمس القادمة



* شارك في الاستطلاع 19504 بالغ عبر الإنترنت بين عمر 16 و74 سنة من 28 دولة
في الفترة من نوفمبر/تشرين الثاني إلى ديسمبر/كانون الأول 2021

تزايد الاهتمام بالذكاء الاصطناعي



غوغل ترندز

أداة تسمح بالتعرف على المواضيع التي يبحث عنها المستخدمون بكثرة عبر الإنترنت

الروبوت أميكا

من تصميم شركة «إنجنيرد آر تس» ليكون منصة بشرية لتطوير الذكاء الاصطناعي

في ختام بحث مخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد، يمكن التأكيد على أهمية فهم وتوعية المجتمع بالتحديات والمخاطر التي يمكن أن يتعرض لها الفرد نتيجة لتطبيقات الذكاء الاصطناعي. تظهر الدراسة والتحليلات أن استخدام التكنولوجيا الذكية بشكل غير مراقب أو غير مشروع قد يؤدي إلى انتهاك خصوصية الأفراد وتعرضهم للمخاطر الأمنية والقانونية.

لذا، يُرجى توفير الإطار القانوني والأخلاقي اللازم لضمان حماية خصوصية الأفراد وتقديم الإرشادات والتوجيهات للشركات والمؤسسات لضمان استخدام التكنولوجيا الذكية بطريقة مسؤولة وأمنة. ينبغي أيضاً تعزيز التعاون بين القطاعين العام والخاص لتطوير إطارات قانونية وتقنية تعزز الحماية الشخصية وتحد من مخاطر الاختراقات السيبرانية.

علاوة على ذلك، يجب أن تلعب التقنية دوراً محورياً في تعزيز الوعي بأهمية الخصوصية وضرورة احترامها، ويجب تشجيع المشاركة الفعالة والمسؤولة للأفراد في عملية تحديد سياسات الخصوصية وتشكيل المستقبل التكنولوجي.

بهذا الشكل، يمكننا تحقيق التوازن بين التقدم التكنولوجي وحماية خصوصية الأفراد، وبناء مجتمع رقمي آمن ومستدام يعزز الثقة والشفافية بين جميع الأطراف المعنية.

في النهاية، يجب أن ندرك أن الذكاء الاجتماعي قد يكون سلاحاً ذو حدين، حيث يمكن استخدامه للتفاعل الإيجابي مع الآخرين وبناء علاقات صحية، ولكنه أيضاً يمكن أن يُستغل لاختراق خصوصية الأفراد واستغلالها في أغراض سلبية.

لذلك، يجب على الأفراد أن يكونوا حذرين ويحافظوا على خصوصيتهم ومعلوماتهم الشخصية عن طريق تقديمها بحذر والتفكير جيداً قبل مشاركتها على الإنترنت، وكذلك يجب على منصات التواصل الاجتماعي وشركات التكنولوجيا اتخاذ إجراءات وسياسات صارمة لحماية خصوصية مستخدميها والحد من تعرضهم للاختراقات والاستغلال.

بهذه الطريقة، يمكننا الاستمتاع بفوائد الذكاء الاجتماعي دون المساس بخصوصيتنا وسلامتنا الشخصية، وبناء علاقات صحية وإيجابية مع الآخرين في عصر التكنولوجيا ووسائل التواصل الاجتماعي.

قائمة المراجع

المواقع صحيفة القبس

جريدة القبس جريدة يومية كويتية، تصدر عن دار القبس للصحافة والطباعة والنشر. يشرف عليها ويديرها مجلس إدارة Wikipedia مكون من المساهمين وعددهم خمسة أعضاء.

بن حمزة, & حورية. (2023). أهمية الذكاء الاصطناعي والتكنولوجيات الحديثة في تنمية المحيط السوسيو-اقتصادي

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines.

Journal of Information ..., 2023 - qscience.com. بيان فراس محمد النعانة, نشران ناصر طه -
qscience.com. اتجاهات مديري المكتبات نحو استخدام تطبيقات الذكاء الاصطناعي-الجامعات الأردنية

Nature Machine Intelligence, 1(9), 389-399.

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.

التغير القيمي لدى طلاب - journals.ekb.eg - أماني محمد شريف عبد السلام - مجلة كلية التربية (أسيوط), 2023
ekb.eg. جامعة أسيوط في ضوء بعض التغيرات المعاصرة

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.

يقدم Melanie Mitchell كتاب من تأليف - "Artificial Intelligence: A Guide for Thinking Humans"
نظرة شاملة وسلسلة حول مفهوم الذكاء الاصطناعي وتأثيره على المجتمع

David L. كتاب من تأليف - "Artificial Intelligence: Foundations of Computational Agents"
يقدم مفاهيم أساسية حول الذكاء الاصطناعي وتطبيقاتها العملية Alan K. Mackworth و Poole

Peter Norvig و Stuart Russell كتاب من تأليف - "Artificial Intelligence: A Modern Approach"
يعتبر من الكتب الكلاسيكية في مجال الذكاء الاصطناعي ويشمل تغطية شاملة للموضوع

قائمة المراجع

Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. In The Cambridge handbook of artificial intelligence (pp. 316-334). Cambridge University Press.

إستخدام تطبيقات الذكاء الاصطناعي . mfes.journals.ekb.eg - مها كمال حفى - مجلة كلية التربية (أسيوط), 2023
ekb.eg .في تحقيق أهداف التنمية المستدامة (رؤية مصر 2030) في مجال التعليم (Geo AI) الجغرافي

Dhshan, Y. I. (2020). *Criminal Liability for Artificial Intelligence Crimes*. YDhshan.

نحو . journals.ekb.eg - محمد الهادي, محمد - مجلة الجمعية المصرية لنظم المعلومات وتكنولوجيا, 2022
Ekb.eg .مجتمع رقمي مستدام

قناة العربية

قناة تلفزيونية

قناة العربية قناة فضائية إخبارية سعودية وجزء من مجموعة إم بي سي. تبث من العاصمة السعودية الرياض، وتهتم هذه القناة بالأخبار السياسية والرياضية والاقتصادية. تضم القناة إعلاميين عرب وسعوديين وغربيين، شأنها شأن معظم القنوات العربية والأجنبية الأخرى

يستكشف Nick Bostrom كتاب من تأليف - **"Superintelligence: Paths, Dangers, Strategies"**.
الآفاق المستقبلية للذكاء الاصطناعي والتحديات والاستراتيجيات المحتملة

19. **"Life 3.0: Being Human in the Age of Artificial Intelligence"** - كتاب من تأليف Max Tegmark
يناقش تأثيرات الذكاء الاصطناعي على المجتمع والبشرية بشكل عام ويطرح تساؤلات أخلاقية وفلسفية حول الموضوع.

20.

يقدم مفاهيم عميقة Aaron Courville و Yoshua Bengio و Ian Goodfellow كتاب من تأليف - **"Deep Learning"**.
حول تقنيات التعلم العميق في مجال الذكاء الاصطناعي.

الذكاء الاصطناعي

Chat GPT

AI Chatting

توصيات تخص البحث

تحليل أمثلة عملية: قم بدراسة حالات واقعية حدثت لأفراد أو منظمات نتيجة لاختراق خصوصيتهم باستخدام التقنيات الذكية. قدم تحليلاً للتأثيرات السلبية والتداعيات القانونية والأخلاقية

مقارنة السياسات والتشريعات: قم بمقارنة السياسات والتشريعات المتعلقة بحماية الخصوصية في مختلف الدول والقطاعات، وقارن كيفية التطبيق والفعالية في التعامل مع مخاطر الذكاء الاصطناعي

استقصاء الآثار النفسية والاجتماعية: قم بدراسة الآثار النفسية والاجتماعية لانتهاك خصوصية الأفراد باستخدام التقنيات الذكية، وكيف يؤثر ذلك على الثقة في التكنولوجيا والتفاعلات الاجتماعية

تطوير نماذج تنبؤية: قم بتطوير نماذج تنبؤية تقيم مخاطر اختراق خصوصية الأفراد باستخدام تقنيات الذكاء الاصطناعي، واستخدم البيانات التاريخية والمعلومات الإحصائية لتحديد العوامل المؤثرة

دراسة التدابير الوقائية والتعزيزية: قم بدراسة التدابير الوقائية التي يمكن اتخاذها لتقليل مخاطر اختراق خصوصية الأفراد، مثل تطوير أدوات الأمان وتعزيز التوعية والتدريب

تقييم تأثيرات التطور التكنولوجي: قم بتقييم تأثيرات التطور التكنولوجي المستقبلي على مخاطر اختراق خصوصية الأفراد، وتحليل كيفية التكيف مع التحديات المستقبلية

توصيات تخص البحث

دراسة التقنيات الحديثة للتحليل الضار: ابحث عن التقنيات الحديثة التي تستخدم في تحليل البيانات الشخصية بشكل ضار، مثل تعلم الآلة والتحليل النفسي والاجتماعي، ودرس كيفية تطوير إستراتيجيات للتصدي لهذا النوع من الاختراقات.

تقييم تأثير الأمان السيبراني: قم بتقييم التأثيرات المحتملة لانتهاكات الأمان السيبراني التي يمكن أن تسهم في اختراق خصوصية الأفراد، ودرس الإجراءات الوقائية والتدابير التي يمكن اتخاذها للحد من هذه التأثيرات.

،دراسة الأساليب الهندسية الاجتماعية: ابحث عن كيفية استخدام الهندسة الاجتماعية للاستيلاء على معلومات شخصية ودرس الطرق التي يمكن من خلالها توعية الأفراد بمخاطر الاحتيال والاختراق.

تحليل السياق القانوني والأخلاقي: قم بتحليل السياق القانوني والأخلاقي المحيط بمخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد، ودرس التدابير التشريعية والأخلاقية التي يجب اتخاذها لحماية الأفراد.

استكشاف التطورات الحالية والمستقبلية: ابحث عن أحدث التطورات في مجال الذكاء الاصطناعي وتأثيراتها المحتملة على خصوصية الأفراد، ودرس كيفية التكيف مع هذه التحديات في المستقبل.

تقييم الأدوات والتقنيات الوقائية: قم بتقييم الأدوات والتقنيات الوقائية المتاحة للأفراد والمؤسسات لحماية خصوصيتهم من مخاطر الذكاء الاصطناعي، ودرس فعاليتها وتكلفتها.

بيان اعتذار

نود أن نعبر عن اعتذارنا الصادق للقراء والباحثين عن مخاطر الذكاء الاصطناعي في اختراق

خصوصية الأفراد عن عدم توفير إحصائيات محددة في بحثنا. نعتزف بأن ذلك قد يقيد من دقة

وشمولية البحث. نحن ندرك أهمية الإحصائيات في تقديم دعم للمفاهيم والتحليلات، ونأمل في أن نكون قد قدمنا معلومات تثري المحتوى وتعمل على توجيه البحث في الاتجاه الصحيح

نود أن نشير إلى أن توفير الإحصائيات الموثوقة والمحدثة حول مخاطر الذكاء الاصطناعي يمثل تحديًا

في العديد من الأحيان نظرًا لطبيعة التطورات السريعة في هذا المجال ولصعوبة الوصول إلى البيانات الدقيقة.

نحن ملتزمون بالعمل على تحسين جودة البحث وتوفير المعلومات المفيدة للقراء والباحثين، وسنستمر في استكشاف مصادر متعددة وتوثيق المعلومات بشكل أفضل في المستقبل

شكرًا لتفهمكم ودعمكم

بيان شكر

نحن، فريق بحث مخاطر الذكاء الاصطناعي في اختراق خصوصية الأفراد، نود أن نعبر عن عميق

.شكرنا وامتناننا لدكتورة [د.منى مصطفى العشري] على توجيهاتها ودعمها المتواصل خلال إعداد بحثنا

نود أن نشمن جهودها الكبيرة في توجيهنا خلال مراحل البحث، وتقديمها للنصائح والتوجيهات القيمة التي ساهمت في تطوير وتحسين جودة البحث. تفانيها في مشاركة معرفتها وخبرتها كان له أثر كبير في إثراء محتوى البحث وزيادة فهمنا للموضوع.

نشكر الدكتورة [د.منى مصطفى العشري] على وقتها وجهودها، ونتطلع إلى الاستفادة من توجيهاتها في المستقبل.

،مع خالص الامتنان والتقدير

[الطالبة] عبير احمد حميد مصلح