دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية هدفت الدراسة إلى التعرف على المجالات وأبرز تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني، وبيان التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني. اعتمد البحث على استعراض وتحليل الدراسات والأبحاث السابقة المتعلقة بتقنية الذكاء الاصطناعي ودورها في تعزيز الأمن السيبراني. تم جمع البيانات من خلال مراجعة الدراسات والأبحاث المنشورة في المجلات العلمية والكتب والتقارير الرسمية. توصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي تساهم في تحسين كفاءة استراتيجيات الأمن السيبراني عبر التنبؤ بالتهديدات والاستجابة السريعة. وكشفت الدراسة عن حاجة ملحة لتدريب وتأهيل الموارد البشرية لفهم وتطبيق تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بشكل فعال. وأوضحت الدراسة أن هناك حاجة لتطوير إطار قانوني وأخلاقي يضمن استخدام التكنولوجيا بشكل مسؤول وفعال داخل المؤسسات والمنظمات. أوصت الدراسة بتعزيز البنية التحتية السيبرانية، وأخيراً التفاعل مع التحديات الأخلاقية والقانونية. الكلمات المفتاحية: الذكاء الاصطناعي، المقدمة إن النمو الهائل للأدوات والأنظمة والشبكات المترابطة يجعل الأمن السيبراني أكثر صعوبة. ويؤدي التقدم التكنولوجي في الاقتصاد الرقمي والبنية التحتية إلى تفاقم هذه المشكلة، علاوة على ذلك، يوثق الباحثون التطور المستمر للأعداء الذين لهم علاقات مع الدول القومية والمنظمات الإجرامية، ونتيجة لذلك، لا بد من تنفيذ الأمن السيبراني القائم على الاستخبارات من أجل إدارة البيانات الضخمة وتوفير دفاع ديناميكي ضد الهجمات السيبرانية الناشئة. والمراقبة المستمرة، 1995). تمثل تقنية الذكاء الاصطناعي إنجازاً بارزاً في ثورة الصناعة الرابعة، بفضل تطبيقاتها الواسعة في مجالات مختلفة من الحياة. استُخدمت هذه التقنية في الاقتصاد والصناعة والخدمات والقطاع العسكري والسياسي، بالإضافة إلى دورها الكبير في تعزيز الأمن السيبراني. يعد هذا الأمر مرتبطاً بالشأن العام للأفراد والمجتمعات، 1.1 المشكلة البحثية وتساؤلاتها ومع تعقيد هذه التهديدات وتطورها، وبناءً علي ما سبق تتلخص مشكلة البحث في السؤال الرئيسي التالي: ما دور الذكاء الاصطناعي في تعزيز الأمان السيبراني؟ حيث تفرع من السؤال الرئيس مجموعة من الأسئلة الفرعية: 3. ما التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني؟ 1.2 أهداف البحث يهدف البحث الحالي لتحقيق الأهداف التالية: 3. توضيح التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني. 1.3 مصطلحات البحث تشمل فروع الذكاء الاصطناعي تصنيف الصور والصوت والترجمة الآلية، وكذلك التخطيط والاستنساخ. ويُستخدم على نطاق واسع في مجالات مثل الروبوتات وتحليل البيانات الضخمة وتطوير تطبيقات الذكاء الاصطناعي لمختلف الصناعات (المصري، 2024). ب. الأمن السيبراني: يُعد الأمن السيبراني مجالاً يهتم بحماية الأنظمة الحاسوبية والشبكات والمعلومات الرقمية من التهديدات الإلكترونية والهجمات السيبرانية. يهدف الأمن السيبراني إلى تأمين البيانات ومنع وكشف واستجابة للانتهاكات الأمنية والهجمات الإلكترونية التي تستهدف الأفراد والمؤسسات. 2024). 2. منهجية البحث استخدم المنهج الوصفي بالاعتماد على مراجعة الدراسات السابقة والأدب النظري المتعلق بموضوع الذكاء الاصطناعي والأمن السيبراني. يعتمد البحث على استعراض وتحليل الدراسات والأبحاث السابقة المتعلقة بتقنية الذكاء الاصطناعي ودورها في تعزيز الأمن السيبراني. تمثلت أدوات الدراسة المستخدمة التقنيات النقدية والتحليلية لاستخلاص النتائج المتعلقة بتطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني. 3. الدراسات السابقة 2023) بعنوان "دور الذكاء الاصطناعي في تعزيز الأمن السيبراني والتدقيق الداخلي"، في وقتنا الحالي، حيث يمكنه أتمتة عمليات الأمن السيبراني، وتحديد التهديدات والاستجابة لها في الوقت الفعلي، يمتلك الذكاء الاصطناعي القدرة على تبسيط إجراءات التدقيق الداخلي، وتحسين الدقة، تناقش هذه الورقة التقنيات المختلفة التي تعمل جنبًا إلى جنب مع الذكاء الاصطناعي لتحسين الأمن السيبراني وممارسات التدقيق الداخلي. تشير نتائج هذا البحث إلى أن الذكاء الاصطناعي هو أداة قوية يمكنها تعزيز الوضع الأمني للمؤسسة بشكل كبير وضمان الامتثال للمتطلبات التنظيمية. أصبح الأمن السيبراني مجالًا سريع التطور وظهر في الأخبار بشكل متكرر بسبب زيادة التهديدات والجهود المستمرة التي يبذلها المتسللون للتغلب على تطبيق القانون. قام مجرمو الإنترنت بتحسين أساليبهم، إن قدرة أنظمة الأمن السيبراني التقليدية على تحديد وإيقاف عمليات الاختراق الجديدة آخذة في التضاؤل. وخاصة التعلم الآلي والتعلم العميق، لديها القدرة على تمكين المتخصصين في مجال الأمن السيبراني من مكافحة التهديدات الديناميكية التي يقدمها الخصوم. نتحدث أيضًا عن الاتجاهات المحتملة للدراسة المستقبلية حيث يتم تطوير مناهج الذكاء الاصطناعي في الأمن السيبراني عبر مجموعة متنوعة من قطاعات التطبيقات. 2021) بعنوان "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry" إلى دراسة مدى فعالية تقنيات الذكاء الاصطناعي في التخفيف من مخاوف الأمن السيبراني في العراق. والصلاحية التمييزية، والمنطقة

الجغرافية، وزيادة أدوات الاستخبارات وإنفاذ القانون، وحجم المعلومات المجمعة من العديد من المصادر، كلها جعلت من الضروري استخدام حلول موثوقة ومعززة للأمن السيبراني في جميع الصناعات. أدى العدد المتزايد من الهجمات الإلكترونية واسعة النطاق في جميع أنحاء العالم إلى جعل الشركات تدرك الحاجة إلى تأمين بياناتها. وسرقة المعلومات العابرة للحدود الوطنية، والتحركات المتخذة لتحقيق مكاسب مالية وتشويه سمعة الآخرين. وجدت دراسة (Li, واكتشاف التسلل، والحفاظ على خصوصية التعلم الآلي، والتعلم الموحد الآمن، تتطلب نماذج الذكاء الاصطناعي تقنيات متخصصة في الدفاع والحماية في مجال الأمن السيبراني. نحن ندرس العلاقة بين الذكاء الاصطناعي والأمن السيبراني بناءً على العاملين المذكورين أعلاه. نقدم نظرة عامة على الجهود البحثية الحالية المتعلقة باستخدام الذكاء الاصطناعي لمواجهة الهجمات الإلكترونية، ونحلل سماتها، نلخص الأدبيات الحالية حول تطوير أنظمة الذكاء الاصطناعي الآمنة، 4. الاطار النظري 4.1 الذكاء الاصطناعي: مفهومه ومجالات استخدامه الذكاء الاصطناعي هو مجال يركز على تطوير الأنظمة والبرامج التي تحاكي الذكاء البشري في تحليل البيانات واتخاذ القرارات. والطب، والتعليم، بالإضافة إلى مجالات أخرى متعددة (دحماني، ليس فقط من قبل المنظمات والخبراء في هذا المجال، ولكن أيضًا من قبل الأفراد المهتمين بالتكنولوجيا (درار، 4.1. 2 مجالات استخدام الذكاء الاصطناعي للذكاء الاصطناعي العديد من الاستخدامات (مركز البحوث والمعلومات، 2021): أ. تستخدم تقنية الذكاء الاصطناعي في مجالات خدمية متنوعة مثل العسكرية والصناعية والتقنية والمالية والطبية والتعليمية. تشمل التطبيقات البارزة لهذه التقنية السيارات ذاتية القيادة والطائرات بدون طيار، ج. يمكن ممارسة المهارات الحركية والتحكم اللفظي وغير الخطي من خلال الأجهزة الذكية التي يمكنها أداء المهام العقلية مثل أبحاث التصميم الصناعي والتحكم في العمليات واتخاذ القرار. د. تستخدم لتعليم اللغة، المالية، والصناعية. توفر التقنية الذكاء الاصطناعي فوائد كثيرة؛ بينما في مجال التصنيع، 4.2 الأمن السيبراني: مفهومه وأبعاده 4.2. 1 مفهوم الأمن السيبراني والحد من الانتهاكات أو الوصول غير المصرح به (العتيبي، 2020). مما يسمح بإعادة الوضع الطبيعي في أسرع وقت ممكن. 4.2. وتُعد من أهم أبعاده (مختار، تطرح فكرة إنشاء ونشر شبكة للإنترنت والأهداف البعيدة، ولكنها تُعد نقطة ضعفاً، ب. البعد الاقتصادي نظراً لاستخدام أجهزة الكمبيوتر في تشغيل الصناعات وتطويرها ودفع الاقتصاد، حيث ترتبط جميعها ببعضها البعض من خلال شبكات الكمبيوتر لضمان الأمن السيبراني، ج. البعد الاجتماعي يوجد أكثر من 4 مليار مستخدم للإنترنت حول العالم، حيث يستخدم أكثر من 2. 6 مليار شخص مواقع الشبكات الاجتماعية. تتمتع مواقع التواصل الاجتماعي بأعلى معدلات التفاعل البشري، لكنها في المقابل تكشف أيضاً عن أخلاقيات الأفراد. صعوبة الرقابة على محتوى الإنترنت ليست مجرد خطر على المجتمعات، مما يهدد السلم الاجتماعي في البلدان، نتيجة فقدان الأمن السيبراني الاجتماعي. فإن التدخل السيبراني لروسيا في الانتخابات الأمريكية هو أهم دليل على الحاجة إلى الأمن السيبراني وأهميته في البعد السياسي. البعد القانوني يتطلب التطور التكنولوجي السريع الامتثال للتشريعات من خلال تحسين الأطر القانونية للتعامل مع الأنشطة القانونية وغير القانونية على الإنترنت، بعض الدول تفتقر إلى تشريعات صارمة للتعامل مع هذه الظواهر. 4.3 تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني 2023): أ. التعامل مع بيانات ضخمة تُظهر هذه العمليات التحديات التي يواجهها محللو الأمن السيبراني في التحقق من كل شيء وتقييم مخاطر محتملة. الذكاء الاصطناعي يعد الخيار المثلى لاكتشاف هذه التهديدات التي تنشأ خلال الأنشطة اليومية، بفضل قدرته على مراقبة حركة المرور وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة بشكل تلقائي. تعتبر كمية البيانات التي يتعامل معها محللو الأمن السيبراني تحديًا في التنبؤ بالتهديدات المستقبلية، إلا أن الذكاء الاصطناعي يستطيع معالجة حجم كبير من البيانات في وقت واحد، بفضل تحديد الإجراءات الوقائية والتهديدات المحتملة، إكتشاف التهديدات بسرعة أمر حيوي للغاية، أفاد 56% من المؤسسات بأنها تعاني من ضغط شديد بسبب تحليل تهديدات يشغل المحللين السيبرانيين، وأبلغ 23% منهم أنهم غير قادرين على التحقق من التهديدات بشكل فعال. يعاني العديد من المؤسسات من تأثيرات مالية جسيمة نتيجة انتهاكات البيانات كل عام، وهذا أمر لا يمكن تجاهله أو التوقف عن مواجهة المجرمين. حيث يتم تقديم خدمات بتكلفة 2. من بين التقنيات البارزة في مجال الذكاء الاصطناعي، ومساعدة المهندسين، وتدريب الموظفين، مما يعزز مرونة الأمن السيبراني بشكل عام. تقدم ChatGPT أيضًا ميزات تساعد الباحثين في مكافحة البرمجيات الضارة وتحليلها، وتسد الفجوات في المعرفة الأمنية، وتسهل تدريب الموظفين حول الأمن السيبراني. وعلى الرغم من التحديات التي قد تواجه استخدام ChatGPT، يواجه الذكاء الاصطناعي عدة تحديات عند تطبيقه في الأمن السيبراني، من هذه التحديات ما يلي (الأمين، 2024): أ. دمج الذكاء الاصطناعي في أنظمة السيبراني أمام العديد من كبار القادة والقيود، ومن أبرزها الحواجز التي تعتمد على القانون الجديد من قبل مجرمي

الإنترنت. ج. دمج الذكاء الاصطناعي في السيبراني ليس للمنظمات، ولكن تحولات التحديات الرئيسية في جذب المواهب اللازمة، وحصر البيانات الأمنية، توظيف أدوات الذكاء الاصطناعي الأمثل. هـ. استخدام مجرمي الانترنت للذكاء الاصطناعي يجعل سلاح ذو حدين، قادر على استخدامه للهجمات وكذلك كأداة دفاع قوية، مما يزيد من نجاح وفعالية تولي السيبرانية. و. المنظمات التي تدمج الذكاء الاصطناعي في أنظمتها السيبرانية للبيانات لقواعد وتتحد من نطاق استخدام التقنية، 5. الخاتمة هدفت الدراسة إلى استكشاف كيفية استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي في تعزيز استراتيجيات الأمن السيبراني. تم تحقيق هذا الهدف من خلال تحليل منهجي واسع للأدبيات المتاحة والأبحاث السابقة في مجال الأمن السيبراني والذكاء الاصطناعي. أبرز النتائج التي توصلت اليها الدراسة: 2. كشفت الدراسة عن حاجة ملحة لتدريب وتأهيل الموارد البشرية لفهم وتطبيق تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بشكل فعال. 3. أوضحت الدراسة أن هناك حاجة لتطوير إطار قانوني وأخلاقي يضمن استخدام التكنولوجيا بشكل مسؤول وفعال داخل المؤسسات والمنظمات. بناءً على النتائج المحققة، توصيات البحث: 1. تعزيز البنية التحتية السيبرانية: يجب على المؤسسات والمنظمات الاستثمار في تحسين البنية التحتية السيبرانية لتمكين تطبيق التقنيات المتقدمة مثل الذكاء الاصطناعي. 2. تدريب وتأهيل الموارد البشرية: ينبغي تعزيز التدريب والتأهيل للمتخصصين في مجال الأمن السيبراني لفهم واستخدام التقنيات الحديثة بشكل فعال.