Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Journal of University Studies for Inclusive Research

Vol.5, Issue 32 (2024), 14071- 14091

USRIJ Pvt. Ltd

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية

الاسم : حسن نايف مبارك الحجرف

المسمي الوظيفي : مدرب ب متخصص

الجهة : الهيئة العامة للتعليم التطبيقي

والتدريب المعهد العالي للاتصالات والملاحة

الملخص

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

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

المؤسسات والمنظمات. أوصت الدراسة بتعزيز البنية التحتية السيبرانية، وتدريب وتأهيل الموارد البشرية، وأخيراً التفاعل مع التحديات الأخلاقية والقانونية.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، المعهد الوطني للمعايير والتقنيات (NIST)، شبكات الاتصالات

Abstract

The study aimed to identify the areas and most prominent applications of artificial intelligence used to improve cybersecurity, and to indicate the challenges facing the application of artificial intelligence in cybersecurity. The research was based on a review and analysis of previous studies and research related to artificial intelligence technology and its role in enhancing cybersecurity. Data were collected by reviewing studies and research published in scientific journals, books, and official reports. The study found that artificial intelligence technologies contribute to improving the efficiency of cybersecurity strategies through threat prediction and rapid response. The study revealed an urgent need to train and qualify human resources to effectively understand and apply artificial intelligence techniques in the field of cybersecurity. The study indicated that there is a need to develop a legal and ethical framework that ensures the responsible and effective use of technology within institutions and organizations. The study recommended strengthening cyber infrastructure, training and qualifying human resources, and finally interacting with ethical and legal challenges.

Keywords: Artificial Intelligence (AI), Cybersecurity, National Institute of Standards and Technologies (NIST), Communications Networks

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

المقدمة

يُشار إلى مجموعة الأدوات والإجراءات والممارسات التي تحمي من الضرر والهجوم والوصول غير القانوني إلى الشبكات والأجهزة والبرامج والبيانات معًا باسم الأمان (Bhardwaj et al., 2022). إن النمو الهائل للأدوات والأنظمة والشبكات المترابطة يجعل الأمن السيبراني أكثر صعوبة. ويؤدي التقدم التكنولوجي في الاقتصاد الرقمي والبنية التحتية إلى تفاقم هذه المشكلة، مما يؤدي إلى زيادة ملحوظة في الهجمات السيبرانية التي تحمل عواقب وخيمة. علاوة على ذلك، يوثق الباحثون التطور المستمر للأعداء الذين لهم علاقات مع الدول القومية والمنظمات الإجرامية، بالإضافة إلى التعقيد المتزايد للهجمات السيبرانية التي تكتشف أساليب جديدة ومتطفلة لاستهداف حتى أكثر الأهداف ذكاءً (Chithaluru et al., 2023). ونتيجة لهذا التقدم، أصبحت الهجمات الإلكترونية أكثر تكرارًا وأكبر حجمًا وأكثر تأثيرًا. ونتيجة لذلك، لا بد من تنفيذ الأمن السيبراني القائم على الاستخبارات من أجل إدارة البيانات الضخمة وتوفير دفاع ديناميكي ضد الهجمات السيبرانية الناشئة. من خلال التحرك نحو التقييمات في الوقت الفعلي، والمراقبة المستمرة، والتحليل المبني على البيانات لتحديد الهجمات الإلكترونية والحماية منها واكتشافها والاستجابة لها وفهرستها من أجل منع وقوع حوادث أمنية في المستقبل، فإن المنظمات الاستشارية مثل المعهد الوطني للمعايير والتقنيات (NIST) يشجعون أيضًا على استخدام أساليب أكثر استباقية وتكيفًا (Umezawa et al., 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، حيث تم استخدامها لتحسين الأمن السيبراني في دول مختلفة (دحماني، ٢٠٢٣).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

١,١ المشكلة البحثية وتساؤلاتها

في ظل التطور المستمر للتكنولوجيا وانتشار استخدام الإنترنت والتقنيات الرقمية في كافة جوانب الحياة اليومية، يزداد التعرض للتهديدات السيبرانية بشكل مستمر. ومع تعقيد هذه التهديدات وتطورها، تنشأ حاجة ملحة لاستخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي لتحسين استراتيجيات الأمن السيبراني وحماية الأنظمة والبيانات الحيوية.

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:

١. ما المجالات التي تُستخدم فيها تقنية الذكاء الاصطناعي؟
٢. ما أبرز تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني؟
٣. ما التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني؟

١,٢ أهداف البحث

يهدف البحث الحالي لتحقيق الأهداف التالية:

١. التعرف علي المجالات التي تُستخدم فيها تقنية الذكاء الاصطناعي.
٢. الكشف عن أبرز تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني.
٣. توضيح التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

١,٣ مصطلحات البحث

أ. الذكاء الاصطناعي: الذكاء الاصطناعي هو فرع من فروع علوم الحاسوب يركز على تصميم وتطوير أنظمة وبرامج قادرة على تنفيذ مهام تشبه الذكاء البشري. يُستخدم في هذا المجال تقنيات وأدوات متقدمة تعتمد على القدرات الحسابية العالية للحواسيب وتكنولوجيا المعلومات، لإنشاء نماذج تتفاعل وتتعلم وتتخذ قرارات بشكل مشابه للبشر. تشمل فروع الذكاء الاصطناعي تصنيف الصور والصوت والترجمة الآلية، وكذلك التخطيط والاستنساخ. يُعد الذكاء الاصطناعي جزءًا أساسيًا من الابتكارات التكنولوجية الحديثة، ويُستخدم على نطاق واسع في مجالات مثل الروبوتات وتحليل البيانات الضخمة وتطوير تطبيقات الذكاء الاصطناعي لمختلف الصناعات (المصري، ٢٠٢٤).

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. يتضمن هذا المجال تحليل المخاطر وتصميم وتنفيذ إجراءات الأمان الضرورية لحماية البيانات والشبكات، والتعامل الفعال مع حوادث الأمن والتحقيق فيها للتعلم والتحسين المستمر. يُعتبر الأمن السيبراني عنصراً أساسياً للحفاظ على سرية المعلومات وضمان استمرارية العمليات الحاسوبية والاتصالات المرتبطة بها (المصري، ٢٠٢٤).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٢. 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. تم جمع البيانات من خلال مراجعة الدراسات والأبحاث المنشورة في المجلات العلمية والكتب والتقارير الرسمية. تمثلت أدوات الدراسة المستخدمة التقنيات النقدية والتحليلية لاستخلاص النتائج المتعلقة بتطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني.

٣. الدراسات السابقة

هدفت دراسة (Dambe et al., 2023) بعنوان "دور الذكاء الاصطناعي في تعزيز الأمن السيبراني والتدقيق الداخلي"، إلى استكشاف كيف يمكن للذكاء الاصطناعي تحسين الأمن السيبراني وممارسات التدقيق الداخلي. في وقتنا الحالي، تواجه المؤسسات عددًا متزايدًا من الهجمات السيبرانية المتطورة وتبحث بنشاط عن طرق جديدة لحماية معلوماتها وأنظمتها الحساسة. وقد برز الذكاء الاصطناعي كحل واعد لهذا التحدي، حيث يمكنه أتمتة عمليات الأمن السيبراني، وتحديد التهديدات والاستجابة لها في الوقت الفعلي، وتقديم رؤى حول نقاط الضعف المحتملة. بالإضافة إلى ذلك، يمتلك الذكاء الاصطناعي القدرة على تبسيط إجراءات التدقيق الداخلي، وتحسين الدقة، وزيادة الرؤية في عمليات المنظمة. 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.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

وضحت دراسة (Zeadally et al., 2020) بعنوان " تسخير قدرات الذكاء الاصطناعي لتحسين الأمن السيبراني" أنّ على مدى السنوات العشر الماضية، أصبح الأمن السيبراني مجالًا سريع التطور وظهر في الأخبار بشكل متكرر بسبب زيادة التهديدات والجهود المستمرة التي يبذلها المتسللون للتغلب على تطبيق القانون. بمرور الوقت، قام مجرمو الإنترنت بتحسين أساليبهم، على الرغم من أن دوافعهم الأولية للقيام بالهجمات الإلكترونية ظلت ثابتة إلى حد ما. إن قدرة أنظمة الأمن السيبراني التقليدية على تحديد وإيقاف عمليات الاختراق الجديدة آخذة في التضاؤل. إن التطورات التكنولوجية في مجال التشفير والذكاء الاصطناعي، وخاصة التعلم الآلي والتعلم العميق، لديها القدرة على تمكين المتخصصين في مجال الأمن السيبراني من مكافحة التهديدات الديناميكية التي يقدمها الخصوم. هنا، ندرس كيف يمكن للذكاء الاصطناعي أن يعزز حلول الأمن السيبراني من خلال الإشارة إلى مزاياه وعيوبه. نتحدث أيضًا عن الاتجاهات المحتملة للدراسة المستقبلية حيث يتم تطوير مناهج الذكاء الاصطناعي في الأمن السيبراني عبر مجموعة متنوعة من قطاعات التطبيقات.

هدفت دراسة (Alhayani et al., 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. وقد تم جمع البيانات من قبل الباحث من العاملين في قطاع تكنولوجيا المعلومات. استخدمت هذه الدراسة عينة مكونة من ٤٦٨ شخصًا، وأجرت التحليل العاملي التأكيدي، والصلاحية التمييزية، وتحليل النموذج الأساسي، وتقييم الفرضيات. وباستثناء النظام الخبير الذي لم يظهر أي علاقة ذات دلالة إحصائية بين الذكاء الاصطناعي والأمن السيبراني، فقد وجد أن القيم P لجميع المتغيرات ذات دلالة إحصائية. وكانت المشاكل الأساسية هي حجم العينة، وإمكانية الوصول، والمنطقة الجغرافية، وعدد أقل من المتغيرات.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

بيّنت دراسة (Tao et al., 2021) بعنوان " The future of artificial intelligence in cybersecurity: A comprehensive survey" أنه يساعد الذكاء الاصطناعي في مخطط سوق الأمن السيبراني المؤسسات في مراقبة الهجمات السيبرانية وتحديدها والكشف عنها وصدها من أجل الحفاظ على خصوصية بياناتها. إن زيادة الوعي العام، والتحسينات التكنولوجية، 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. إن الأنظمة السيبرانية ذات قدرات الذكاء الاصطناعي مدفوعة بارتفاع وتيرة ومستوى الهجمات السيبرانية. أدى العدد المتزايد من الهجمات الإلكترونية واسعة النطاق في جميع أنحاء العالم إلى جعل الشركات تدرك الحاجة إلى تأمين بياناتها. يتم تحفيز هؤلاء المجرمين الإلكترونيين من خلال المصالح الجماعية المتطرفة غير العلمانية، وسرقة المعلومات العابرة للحدود الوطنية، والتنافس بين المنافسين، والتحركات المتخذة لتحقيق مكاسب مالية وتشويه سمعة الآخرين. الغرض من معظم الهجمات الإلكترونية هو الربح.

وجدت دراسة (Li, 2018) بعنوان " الأمن السيبراني يلتقي بالذكاء الاصطناعي: استطلاع" أنّ الذكاء الاصطناعي والأمن السيبراني لديهما العديد من التفاعلات المختلفة متعددة التخصصات. فمن ناحية، يمكن تطبيق تكنولوجيا الذكاء الاصطناعي، مثل التعلم العميق، على الأمن السيبراني لبناء نماذج ذكية لتصنيف البرامج الضارة، واكتشاف التسلل، واستشعار التهديدات الذكية. ومع ذلك، ستواجه نماذج الذكاء الاصطناعي مجموعة متنوعة من التهديدات السيبرانية، مما سيعطل عملية التعلم وصنع القرار وأخذ العينات. لذلك، من أجل منع التعلم الآلي العدائي، والحفاظ على خصوصية التعلم الآلي، والتعلم الموحد الآمن، وما إلى ذلك، تتطلب نماذج الذكاء الاصطناعي تقنيات متخصصة في الدفاع والحماية في مجال الأمن السيبراني. نحن

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

ندرس العلاقة بين الذكاء الاصطناعي والأمن السيبراني بناءً على العاملين المذكورين أعلاه. أولاً، نقدم نظرة عامة على الجهود البحثية الحالية المتعلقة باستخدام الذكاء الاصطناعي لمواجهة الهجمات الإلكترونية، بما في ذلك استخدام كل من حلول التعلم العميق الراسخة وتقنيات التعلم الآلي التقليدية. بعد ذلك، سندرس الهجمات المضادة التي قد يكون الذكاء الاصطناعي عرضة لها، ونحلل سماتها، ونصنف استراتيجيات الحماية المناسبة. وأخيرًا، نلخص الأدبيات الحالية حول تطوير أنظمة الذكاء الاصطناعي الآمنة، مع التركيز على جوانب بناء شبكات عصبية مشفرة وتنفيذ التعلم العميق الموحد الآمن.

٤. الاطار النظري

٤,١ الذكاء الاصطناعي: مفهومه ومجالات استخدامه

٤,١,١ مفهوم الذكاء الاصطناعي

الذكاء الاصطناعي هو مجال يركز على تطوير الأنظمة والبرامج التي تحاكي الذكاء البشري في تحليل البيانات واتخاذ القرارات. يستخدم الذكاء الاصطناعي في مجموعة واسعة من المجالات مثل التجارة الإلكترونية، والطب، والتعليم، بالإضافة إلى مجالات أخرى متعددة (دحماني، ٢٠٢٣).

تكشف استعراض الأدبيات حول موضوع الذكاء الاصطناعي أن هناك العديد من التعاريف لمفاهيم تقنية الذكاء الاصطناعي قد تم نشرها، ليس فقط من قبل المنظمات والخبراء في هذا المجال، ولكن أيضًا من قبل الأفراد المهتمين بالتكنولوجيا (درار، ٢٠١٩).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٤,١,٢ مجالات استخدام الذكاء الاصطناعي

للذكاء الاصطناعي العديد من الاستخدامات (مركز البحوث والمعلومات، ٢٠٢١):

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، والروبوتات التي تعمل بشكل مستقل وتدير الآلات المستخدمة في مجموعة متنوعة من المهام، مثل العمل في المفاعلات النووية ومحطات الطاقة وإصلاح الكوابل وتمديدها تحت الأرض، واكتشاف المناجم وغيرها من المهام التي يتم فيها استبدال استخدام البشر بالتقنيات الذكية.

ب. يستخدم عمليات النمذجة الذكية الحاسوبية لدراسة كيفية تعرف الدماغ البشري على الوجوه والأصوات المألوفة، ومعالجة الصور، واستخراج البيانات المفيدة منها، وتحسين الذاكرة. يُطبق الأمر نفسه على تطوير الألعاب الإلكترونية مثل الشطرنج وألعاب الفيديو.

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، والفهم التلقائي للغة المكتوبة والمنطوقة، وترجمة اللغة في الوقت الفعلي بإجابات مبرمجة مسبقاً، ويتم جمع العديد من عمليات البحث في Google على أجهزة كمبيوتر متصلة بالإنترنت.

تتميز تقنية الذكاء الاصطناعي بالعديد من التطبيقات في مختلف المجالات، حيث تُستخدم في القطاعات العسكرية، المالية، الخدمية، والصناعية. كما يمكن الاستفادة منها في مجال التعليم من خلال المنصات

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

التعليمية والتطبيقات الرقمية المبرمجة. توفر التقنية الذكاء الاصطناعي فوائد كثيرة؛ ففي مجال الطب، يمكن أن يساعد الأطباء في تشخيص الأمراض وتوجيه العلاج بدقة أكبر، بينما في مجال التصنيع، يمكنه تحسين عمليات الإنتاج وزيادة الكفاءة. تُمكّن الروبوتات المجهزة بتقنيات الذكاء الاصطناعي من أداء المهام الروتينية بدقة وسرعة عالية. ومع ذلك، تواجه هذه التقنية بعض التحديات والقيود في المجالات التي تتطلب الإبداع والحدس البشري (دحماني، ٢٠٢٣).

٤,٢ الأمن السيبراني: مفهومه وأبعاده

٤,٢,١ مفهوم الأمن السيبراني

تُعرف الأمن السيبراني بأنه الحماية لشبكات الاتصالات وأنظمة المعلومات والبيانات، بما في ذلك الأجهزة المتصلة بالإنترنت. يتعلق الأمن السيبراني بالتدابير الوقائية والمعايير التي يجب اتباعها والامتثال لها لمواجهة التهديدات، والحد من الانتهاكات أو الوصول غير المصرح به (العتيبي، ٢٠٢٠).

وقد وصفه جبور (٢٠١٢) بأنه النشاط الذي يضمن حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، ويضمن القدرة على التعافي من الخسائر والأضرار الناتجة عن مخاطر وتهديدات محتملة، مما يسمح بإعادة الوضع الطبيعي في أسرع وقت ممكن.

٤,٢,٢ أبعاد الأمن السيبراني

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

يتضمن الأمن السيبراني أنظمة الأمن العسكري والاقتصادي والاجتماعي والسياسي والإنساني التي تهدف إلى الحفاظ على الاستقرار والأمان من جميع التهديدات السيبرانية. يتضمن الأمن المتكامل الجوانب التي تسهم في تعزيز نظام الأمن السيبراني، وتُعد من أهم أبعاده (مختار، ٢٠٢٣):

أ. البعد العسكري

يهدف الأمن السيبراني إلى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسهل تبادل المعلومات والأوامر. تطرح فكرة إنشاء ونشر شبكة للإنترنت والأهداف البعيدة، ولكنها تُعد نقطة ضعفاً، خاصة إذا لم تكن آمنة. يمكن أن يؤدي تدمير قواعد البيانات العسكرية أو الابتزاز عليها إلى تعطيل الاتصالات بين وحدات القيادة والوحدات العسكرية، بالإضافة إلى خطر فقدان السيطرة على بعض الأسلحة مثل الطائرات بدون طيار والصواريخ الموجهة والأقمار الصناعية.

ب. البعد الاقتصادي

نظراً لاستخدام أجهزة الكمبيوتر في تشغيل الصناعات وتطويرها ودفع الاقتصاد، ستكون الإنترنت أساساً للتجارة والتمويل والمعاملات المالية، حيث ترتبط جميعها ببعضها البعض من خلال شبكات الكمبيوتر لضمان الأمن السيبراني، وهو أمر يتعلق بشكل خاص بالقطاع المالي.

ج. البعد الاجتماعي

يوجد أكثر من ٤ مليار مستخدم للإنترنت حول العالم، حيث يستخدم أكثر من ٢,٦ مليار شخص مواقع الشبكات الاجتماعية. تتمتع مواقع التواصل الاجتماعي بأعلى معدلات التفاعل البشري، مما يتيح فرصاً واسعة

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

لمشاركة الأفكار والتجارب الناجحة، لكنها في المقابل تكشف أيضاً عن أخلاقيات الأفراد. صعوبة الرقابة على محتوى الإنترنت ليست مجرد خطر على المجتمعات، بل تعرض أيضاً المعلومات الشخصية لاستخدامات غير مشروعة من جهات خارجية، مما يهدد السلم الاجتماعي في البلدان، نتيجة فقدان الأمن السيبراني الاجتماعي.

د. البعد السياسي

بعيداً عن تسريبات الوثائق السرية والامتيازات التي غالباً ما تؤدي إلى أزمات دبلوماسية بين الدول، فإن التدخل السيبراني لروسيا في الانتخابات الأمريكية هو أهم دليل على الحاجة إلى الأمن السيبراني وأهميته في البعد السياسي.

هـ. البعد القانوني

يتطلب التطور التكنولوجي السريع الامتثال للتشريعات من خلال تحسين الأطر القانونية للتعامل مع الأنشطة القانونية وغير القانونية على الإنترنت، حيث تعتبر الجرائم الإلكترونية في الغالب جرائم سيبرانية. بعض الدول تفتقر إلى تشريعات صارمة للتعامل مع هذه الظواهر.

٤,٣ تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني

4.3.1 وظائف الذكاء الاصطناعي في الأمن السيبراني

يستخدم الذكاء الاصطناعي في تحسين الأمن السيبراني من خلال التطبيقات التاليه (حداوي وآخرون، ٢٠٢٣):

أ. التعامل مع بيانات ضخمة

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

يتم تنفيذ العديد من الأنشطة على خوادمنا، مما يعني نقل كميات كبيرة من البيانات بين عملائنا وبنيتنا التحتية يوميًا. 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.

ب. توقع التهديدات المستقبلية

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، مما يمكّن من الكشف المبكر عن الأنشطة الضارة. بفضل تحديد الإجراءات الوقائية والتهديدات المحتملة، يمكن تقليل الوقت المهدور والموارد البشرية، ويساعد في البقاء يقظًا من خلال اتخاذ خطوات لحماية المؤسسة.

ج. تقليل وقت اكتشاف التهديد

إكتشاف التهديدات بسرعة أمر حيوي للغاية، حيث أبلغت ٤٢% من المؤسسات عن زيادة في التهديدات الحساسة للوقت. في الوقت نفسه، يمكن للذكاء الاصطناعي فحص كميات هائلة من البيانات في وقت واحد للكشف عن التهديدات السيبرانية، مما يعزز الأمن بشكل كبير. وبحسب استطلاع، أفاد ٥٦% من المؤسسات بأنها تعاني من ضغط شديد بسبب تحليل تهديدات يشغل المحللين السيبرانيين، وأبلغ ٢٣% منهم أنهم غير قادرين على التحقق من التهديدات بشكل فعال.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

د. التقليل في التكاليف

يعاني العديد من المؤسسات من تأثيرات مالية جسيمة نتيجة انتهاكات البيانات كل عام، وهذا أمر لا يمكن تجاهله أو التوقف عن مواجهة المجرمين. وفقًا للدراسات، توضح الفروقات الكبيرة في توفير التكاليف بنسبة ٨٠% للمؤسسات التي تعتمد على تقنيات الذكاء الاصطناعي في أمنها السيبراني، حيث يتم تقديم خدمات بتكلفة ٢,٩ مليون دولار مقابل ٦,٧١ مليون دولار لمن لا يستخدمون هذه التقنيات.

من بين التقنيات البارزة في مجال الذكاء الاصطناعي، نجد ChatGPT، وعلى الرغم من المخاوف المتعلقة بالتحديات مثل التحيز العنصري ونقص المعايير الموثوقة، إلا أن لهذه التقنية فوائد هامة في ساحة أمن المعلومات. تسهم ChatGPT في زيادة الإنتاجية، ومساعدة المهندسين، وتدريب الموظفين، وتعزيز إنفاذ القانون. كما أن تطور ChatGPT يعمل على تعزيز قدرة الصناعة على كشف واستجابة الهجمات الإلكترونية في الوقت الفعلي، 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، فإنه يمثل خطوة هامة نحو تحسين الأمان والمرونة في الأنظمة التي تعتمد على الذكاء الاصطناعي.

٤,٤ تحديات تطبيق الذكاء الاصطناعي في الأمن السيبراني

يواجه الذكاء الاصطناعي عدة تحديات عند تطبيقه في الأمن السيبراني، من هذه التحديات ما يلي (الأمين، ٢٠٢٤):

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

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.

ب. تمثل الصناعات التكنولوجية الجديدة احتياجات جديدة للاستثمارات الكبيرة في مهارات الحوسبة والذاكرة ومراكز البيانات، وتساهم في بناء وصيانة التكنولوجيا الصناعية.

ج. دمج الذكاء الاصطناعي في السيبراني ليس للمنظمات، ولكن تحولات التحديات الرئيسية في جذب المواهب اللازمة، وحصر البيانات الأمنية، توظيف أدوات الذكاء الاصطناعي الأمثل.

د. تعد أدوات البحث عن البيانات هي الأسهل من حيث الرئيسية التي تواجه المنظمات في تطبيقات الذكاء الاصطناعي المتقدمة.

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، في حين تشهد مجرمو الإنترنت بمرونة لا محدودة في التأثير على التكنولوجيا.

٥. 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.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

تم استخدام منهجية شاملة تتضمن مراجعة الأدبيات لفهم النظريات والأساليب الحالية في مجال الأمن السيبراني وتطبيقات الذكاء الاصطناعي.

أبرز النتائج التي توصلت اليها الدراسة:

١. أظهرت الدراسة أن تقنيات الذكاء الاصطناعي تساهم في تحسين كفاءة استراتيجيات الأمن السيبراني عبر التنبؤ بالتهديدات والاستجابة السريعة.

٢. كشفت الدراسة عن حاجة ملحة لتدريب وتأهيل الموارد البشرية لفهم وتطبيق تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بشكل فعال.

٣. أوضحت الدراسة أن هناك حاجة لتطوير إطار قانوني وأخلاقي يضمن استخدام التكنولوجيا بشكل مسؤول وفعال داخل المؤسسات والمنظمات.

بناءً على النتائج المحققة، يجب على الجهات المعنية الاستثمار في تعزيز البنية التحتية التقنية وتطوير السياسات والإجراءات لتمكين تطبيق الذكاء الاصطناعي بشكل فعال في مجال الأمن السيبراني.

توصيات البحث:

١. تعزيز البنية التحتية السيبرانية: يجب على المؤسسات والمنظمات الاستثمار في تحسين البنية التحتية السيبرانية لتمكين تطبيق التقنيات المتقدمة مثل الذكاء الاصطناعي.

٢. تدريب وتأهيل الموارد البشرية: ينبغي تعزيز التدريب والتأهيل للمتخصصين في مجال الأمن السيبراني لفهم واستخدام التقنيات الحديثة بشكل فعال.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٣. التفاعل مع التحديات الأخلاقية والقانونية: يجب تطوير إطار عمل قانوني وأخلاقي يضمن استخدام الذكاء الاصطناعي في الأمن السيبراني بطريقة مسؤولة ومتوازنة.

الدراسات المستقبلية:

١. استكشاف تقنيات الذكاء الاصطناعي الجديدة لتحسين تحليل البيانات السيبرانية واستجابة أسرع للتهديدات.

٢. دراسة تأثير الذكاء الاصطناعي في تحسين تنبؤات الأمن السيبراني وتقليل الاستجابات الزائفة.

٣. تحليل التحديات الأمنية الناشئة المرتبطة بالتطبيقات الجديدة للذكاء الاصطناعي في الأمن السيبراني.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

المراجع

المراجع العربية

الأمين، دبار محمد، و جمال الدين، بابو. (٢٠٢٤). تداعيات الذكاء الاصطناعي على الأمن القومي. Journal of Private Law، ٢(١)، ١٠٠-١٢٢.

حداوي، أميرة هاتف، و مسلم، ضرغام علي، و محمد، صفاء تايه. (٢٠٢٣). القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات–دراسة تحليلة لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف. مجلة العلوم الإنسانية والطبيعية، ٥(١).

دحماني، محمد. (٢٠٢٣). الذكاء الاصناعي كألية لتعزيز الامن السيبراني. مجلة الفكر القانوني والسياسي، ٧(٢)، ٥٩٧-٦٠٨.

درار، خديجة محمد. أخلاقيات الذكاء الاصطناعي والروبوت: دراسة تحليلة. المجلة الدولية لعلوم المكتبات والمعلومات، ٦(٣)، ٢٣٧-٢٧١.

العتيبي، عبدالرحمن بجاد شارع. (٢٠٢٠). دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠ (رسالة ماجستير). جامعة نايف العربية للعوم الأمنية.

مختار، محمد. (٢٠٢٣). الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث، (٢)، ٦-٧.

مركز البحوث والمعلومات. (٢٠٢١). الذكاء الاصطناعي. السعودية. https://www.abhacci.org.sa/ar/Centers/ResearchCenter/EServices/SouthBulletins/

Documents/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1%20%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A.pdf

المصري، فرح محمد. (٢٠٢٤). دور الذكاء الاصطناعي في تحسين الأمن السيبراني. مجلة النخبة للدراسات والأبحاث، ٣(٢).

المراجع الأجنبية

Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)* (pp. 88-93). IEEE.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access, 8*, 23817-23837.

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings, 531*(10.1016).

Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies, 8*(28), e3-e3.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering, 19*(12), 1462-1474.

Bhardwaj, A., Alshehri, M. D., Kaushik, K., Alyamani, H. J., & Kumar, M. (2022). (Retracted) Secure framework against cyber attacks on cyber-physical robotic systems. *Journal of Electronic Imaging, 31*(6), 061802-061802.

Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2023). Computational-intelligence-inspired adaptive opportunistic clustering approach for industrial IoT networks. *IEEE Internet of Things Journal, 10*(9), 7884-7892.

Umezawa, Y., Umezawa, K., & Sato, H. (1995). Selectivity coefficients for ion-selective electrodes: Recommended methods for reporting KA, Bpot values (Technical Report). *Pure and applied chemistry, 67*(3), 507-518.