المجلة المصرية للدراسات المتخصصة

دورية فصلية علمية محكمة – تصدرها كلية التربية النوعية – جامعة عين شمس

المراسلات :

ترسل المراسلات باسم الأستاذ الدكتور/ رئيس التحرير، على العنوان التالى

٣٦٥ ش رمسيس – كلية التربية النوعية – جامعة عين شمس ت/ ٠٢/٢٦٨٤٤٥٩٤

الموقع الرسمي:
https://ejos.journals.ekb.eg

البريد الإلكتروني:
egyjournal@sedu.asu.edu.eg

الترقيم الدولي الموحد للطباعة : 6164 - 1687

الترقيم الدولي الموحد الإلكتروني : 2682 - 4353

تقييم المجلة (يونيو ٢٠٢٤) : (7) نقاط

معامل ارسيف Arcif (أكتوبر ٢٠٢٤) : (0.4167)

المجلد (١٣) . العدد (٤٦) . الجزء الخامس

أبريل ٢٠٢٥

(*) الأسماء مرتبة ترتيباً ابجدياً.

الصفحة الرئيسية

م	القطاع	اسم المجلة	اسم الجهه / الجامعة	ISSN-P	ISSN-O	السنه	نقاط المجله
1	Multidisciplinary عام	المجلة المصرية للدراسات المتخصصة	جامعة عين شمس، كلية التربية النوعية	1687-6164	2682-4353	2024	7

معامل التأثير والاستشهادات المرجعية العربي Arab Citation & Impact Factor
قاعدة البيانات العربية الرقمية Arab Online Database
معرفة e-MAREFA
Arcif Analytics

التاريخ: 2024/10/20

الرقم: L24/0228 ARCIF

سعادة أ. د. رئيس تحرير المجلة المصرية للدراسات المتخصصة المحترم

جامعة عين شمس، كلية التربية النوعية، القاهرة، مصر

تحية طيبة وبعد،،،

يسر **معامل التأثير والاستشهادات المرجعية للمجلات العلمية العربية (ارسيف – ARCIF)**، أحد مبادرات قاعدة بيانات **"معرفة"** للإنتاج والمحتوى العلمي، إعلامكم بأنه قد **أطلق التقرير السنوي التاسع للمجلات للعام 2024**.

ويسرنا تهنئتكم وإعلامكم بأن **المجلة المصرية للدراسات المتخصصة** الصادرة عن **جامعة عين شمس، كلية التربية النوعية، القاهرة، مصر، قد نجحت في تحقيق معايير اعتماد معامل "ارسيف Arcif"** المتوافقة مع المعايير العالمية، والتي يبلغ عددها **(32) معياراً**، وللاطلاع على هذه المعايير يمكنكم الدخول إلى الرابط التالي: http://e-marefa.net/arcif/criteria/

وكان **معامل "ارسيف Arcif " العام** لمجلتكم لسنة 2024 **(0.4167)**.

كما صُنفت مجلتكم في **تخصص العلوم التربوية** من **إجمالي عدد المجلات (127)** على المستوى العربي ضمن الفئة **(Q3)** وهي الفئة الوسطى ، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان **(0.649)**.

وبإمكانكم الإعلان عن هذه النتيجة سواء على موقعكم الإلكتروني، أو على مواقع التواصل الاجتماعي، وكذلك الإشارة في النسخة الورقية لمجلتكم إلى معامل **"ارسيف Arcif"** الخاص بمجلتكم.

ختاماً، نرجو في حال رغبتكم الحصول على شهادة رسمية إلكترونية خاصة بنجاحكم في معامل " **ارسيف** "، التواصل معنا مشكورين.

وتفضلوا بقبول فائق الاحترام والتقدير

أ.د. سامي الخزندار

رئيس مبادرة معامل التأثير

" ارسيف Arcif"

+962 6 5548228 -9
+ 962 6 55 19 10 7
info@e-marefa.net
www.e-marefa.net
Amman - Jordan
2351 Amman, 11953 Jordan

محتويات العدد

الجزء الثانى :

أولاً : بحوث علمية محكمة باللغة العربية :

دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني
دراسة تحليلية للتحديات والحلول المستقبلية

د / هيثم رزق فضل الله [1]

[1] مدرس بكلية الحاسبات والمعلومات ، جامعة ٦ اكتوبر.

دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني
دراسة تحليلية للتحديات والحلول المستقبلية

د/ هيثم رزق فضل الله

ملخص:
تتناول هذه الدراسة التحليلية دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني، حيث تستعرض كيفية توظيف تقنيات الذكاء الاصطناعي، مثل التعلم الآلي والتعلم العميق، للكشف المبكر عن التهديدات السيبرانية وتحليل سلوك الشبكات بشكل لحظي، بما يسهم في سرعة الاستجابة للهجمات المتطورة. كما تُسلط الدراسة الضوء على التحديات المرتبطة باستخدام الذكاء الاصطناعي في هذا المجال، مثل الحاجة إلى قواعد بيانات ضخمة لتدريب النماذج، وصعوبة التعامل مع الهجمات المتقدمة، بالإضافة إلى الإشكاليات المتعلقة بالخصوصية والأخلاقيات. وأوصت الدراسة بضرورة تبني حلول مبتكرة تشمل التكامل بين الذكاء الاصطناعي والحوسبة الكمومية، إلى جانب تطوير نماذج أكثر تكيفًا مع بيئة التهديدات المتغيرة، مع التأكيد على أهمية التعاون بين خبراء الأمن السيبراني وخبراء الذكاء الاصطناعي، وتبني سياسات توازن بين الأمن والخصوصية.
الكلمات الدالة : الذكاء الاصطناعى ، الأمن السيبراني .

Abstract:
Title: The role of artificial intelligence in enhancing the effectiveness of cybersecurity An analytical study of future challenges and solutions
Authors: Haitham Rizq Fadlallah
This analytical study examines the role of artificial intelligence in enhancing the effectiveness of cybersecurity. It highlights how AI technologies, such as machine learning and deep learning, are employed for early threat detection and real-time network behavior analysis, contributing to faster responses to advanced cyberattacks. The study also sheds light on the challenges associated with applying AI in cybersecurity, including the need for large datasets to train models, the difficulty in handling sophisticated attacks, and issues related to privacy and ethics. The study recommends adopting innovative solutions such as integrating AI with quantum computing, developing adaptive AI models capable of evolving with the threat landscape, fostering collaboration between cybersecurity and AI experts, and implementing policies that strike a balance between security and privacy
Keywords: artificial intelligence, cybersecurity

المقدمة :

مع الثورة الرقمية التي يشهدها العالم اليوم، أصبحت الأنظمة والشبكات الإلكترونية محورًا رئيسيًا في الأعمال التجارية، الحكومية، والتعليمية، وحتى في الحياة اليومية للأفراد. ومع تزايد اعتماد المجتمع على هذه الأنظمة، تنامى أيضًا خطر الهجمات السيبرانية التي أصبحت أكثر تعقيدًا، مما يتطلب آليات متطورة للتصدي لهذه التهديدات.

من خلال هذا السياق، يبرز **الذكاء الاصطناعي(AI)** ، الذي أثبت قدرته على تحسين فعالية الدفاعات السيبرانية. حيث يستخدم الذكاء الاصطناعي تقنيات مثل **التعلم الآلي (Machine Learning)والتعلم العميق (Deep Learning)** لتحليل البيانات، اكتشاف التهديدات في الوقت الفعلي، واتخاذ قرارات فورية للحد من تأثير الهجمات كما انه يستخدم كأداة حيوية لتعزيز فعالية **الأمن السيبراني** .فالذكاء الاصطناعي يقدم حلولًا قوية تمكن من الكشف المبكر عن التهديدات وتحليل الأنماط السلوكية داخل الشبكات، بالإضافة إلى إمكانية الرد السريع والفعال على الهجمات. على الرغم من إمكانياته المبهرة، تواجه تقنيات الذكاء الاصطناعي العديد من التحديات التي تتطلب حلولًا مبتكرة ومتكاملة.

يهدف هذا البحث إلى تحليل دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني، مع دراسة التحديات التي قد تطرأ على استخدامه، واستكشاف الحلول المستقبلية لتجاوز هذه التحديات. كما يسلط الضوء على الفرص المستقبلية التي يوفرها الذكاء الاصطناعي لتحسين أمان الشبكات وحمايتها من التهديدات المتطورة.

مشكلة البحث

تتمثل المشكلة البحثية في معرفة مدى تأثير الذكاء الاصطناعي على تعزيز فعالية استراتيجيات الأمن السيبراني في مواجهة التهديدات المتطورة. على الرغم من النجاحات الملحوظة لتقنيات الذكاء الاصطناعي في مجالات متعددة، إلا أن تطبيقها

في الأمن السيبراني يواجه تحديات متعددة، مثل ضعف القدرة على التعامل مع الهجمات المتقدمة، الحاجة لبيانات ضخمة لدعم الأنظمة الذكية، وكذلك القضايا المتعلقة بالخصوصية والأخلاقيات.

أسئلة البحث

١. ما دور الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية؟
٢. ما أبرز التحديات التي يواجهها الذكاء الاصطناعي في مجال الأمن السيبراني؟
٣. كيف يمكن التغلب على هذه التحديات باستخدام تقنيات جديدة؟
٤. ما الحلول المستقبلية لتحسين قدرة الذكاء الاصطناعي في حماية الأنظمة من الهجمات المتطورة؟
٥. كيف يمكن دمج الذكاء الاصطناعي مع التقنيات الحديثة مثل الحوسبة الكمومية لتحسين فعالية الأمان السيبراني؟

أهداف البحث

١. دراسة دور الذكاء الاصطناعي في تحسين فاعلية استراتيجيات الأمن السيبراني.
٢. تحليل التحديات التي تواجه تطبيق الذكاء الاصطناعي في الأمن السيبراني.
٣. استكشاف الحلول المستقبلية والفرص المتاحة لتطوير الذكاء الاصطناعي في هذا المجال.
٤. تحليل تأثير تكامل الذكاء الاصطناعي مع تقنيات أخرى مثل الحوسبة الكمومية على الأمان السيبراني.

أهمية البحث

تكمن أهمية هذا البحث في دراسة دور الذكاء الاصطناعي في تعزيز الأمن السيبراني في مواجهة التهديدات المتزايدة. فمع تزايد الهجمات السيبرانية على المستوى العالمي، أصبح من الضروري استخدام تقنيات الذكاء الاصطناعي لضمان حماية المعلومات والأنظمة الحساسة من السرقة أو التعطيل. هذا البحث سيسهم في تسليط الضوء على كيفية دمج الذكاء الاصطناعي في استراتيجيات الأمن السيبراني، مع التركيز على التحديات التي قد تواجهها الأنظمة المستقبلية، وكيفية التغلب عليها باستخدام حلول مبتكرة.

المنهج المستخدم

اعتمد البحث على **المنهج الوصفي التحليلي(تحليل المحتوي)**، الذي يسمح بدراسة وتحليل الظاهرة بشكل شامل من خلال مراجعة الأدبيات الحالية، واستخدام البيانات المتاحة لتحليل الأثر الفعلي للذكاء الاصطناعي في الأمن السيبراني. يتم التركيز على تحليل الدراسات والبحوث السابقة التي تناولت هذا الموضوع، بالإضافة إلى تقديم مقارنة بين تطبيقات الذكاء الاصطناعي في الأمن السيبراني في مختلف المؤسسات والمنظمات.

المصطلحات الرئيسية

١. **الذكاء الاصطناعي :(AI)** هو قدرة الأنظمة الحاسوبية على تنفيذ مهام تتطلب عادةً الذكاء البشري مثل التعلم، واتخاذ القرارات، والتفاعل مع البيئة.

٢. **الأمن السيبراني :**هو مجموعة من السياسات والإجراءات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية.

٣. **التعلم الآلي :(Machine Learning)** فرع من الذكاء الاصطناعي يهتم بتطوير الأنظمة التي يمكنها التعلم من البيانات وتحسين أدائها بشكل تلقائي.

٤. **التعلم العميق :(Deep Learning)** أحد أساليب التعلم الآلي الذي يعتمد على الشبكات العصبية متعددة الطبقات لتحليل بيانات ضخمة.

الأدوات المستخدمة

- **برامج التحليل البياني** :مثل أدوات تحليل البيانات الضخمة (Big Data Analytics) التي تتيح دراسة سلوك الأنظمة والشبكات بشكل شامل.
- **أنظمة الكشف المتقدمة** :مثل تلك التي تعتمد على تقنيات الذكاء الاصطناعي مثل التعلم الآلي والتعلم العميق لتحديد الأنماط المشبوهة في الشبكات.
- **البرمجيات لتدريب النماذج** :برامج مثل TensorFlow و PyTorch التي تتيح تدريب نماذج الذكاء الاصطناعي على بيانات الأمن السيبراني.

الدراسات السابقة

عتلم، ش. (٢٠٢٢). تتناول الدراسة أثر الذكاء الاصطناعي في الحروب السيبرانية وتأثيراته المباشرة على الأمن الإنساني. تسلط الضوء على كيف أصبح الذكاء الاصطناعي أداة فعالة في تعزيز الأمن السيبراني، مع التركيز على استخدامه في الكشف المبكر عن الهجمات، وتحييدها قبل وقوعها. كما تناقش الدراسة التحديات القانونية والأخلاقية التي تفرضها هذه التقنية أثناء النزاعات المسلحة، مع اقتراح حلول لتحسين التشريعات الدولية المتعلقة بالأمن السيبراني.

Root-X. (2022). تسلط الدراسة الضوء على التطبيقات العملية للذكاء الاصطناعي في تحسين قدرات الأمن السيبراني، من خلال تحليل البيانات الضخمة واكتشاف الأنماط غير الطبيعية بشكل لحظي. كما تستعرض الدراسة بعض التحديات التقنية مثل دقة الخوارزميات، وتهديدات "الهجمات المعاكسة (Adversarial Attacks)"، مع اقتراح حلول مثل تبني الذكاء الاصطناعي التكيفي، وتدريب الأنظمة على سيناريوهات هجمات مختلفة لتعزيز الاستجابة.

TechAcute. (2022). تناقش الدراسة الفرص التي يوفرها الذكاء الاصطناعي لتحسين الأمن السيبراني، مثل أتمتة اكتشاف التهديدات، وتعزيز أنظمة الدفاع السيبراني، وتقليل زمن الاستجابة. وفي المقابل، تعرض الدراسة تحديات تتمثل في احتمال تحيز الخوارزميات، ونقص الشفافية في قرارات أنظمة الذكاء الاصطناعي، مما يخلق صعوبات قانونية وتنظيمية. كما تشير إلى الحاجة إلى تكامل الذكاء الاصطناعي مع الذكاء البشري لتحقيق أفضل النتائج.

بن عيسى، ن. (٢٠٢٢) تستعرض هذه الدراسة أهمية الذكاء الاصطناعي في تحقيق الأمن السيبراني وحماية البيانات من الاختراقات. كما تناقش أبعاد ومفاهيم الذكاء الاصطناعي ودوره في حماية مستخدمي مواقع التواصل الاجتماعي.

بن عيسى، ن. (٢٠٢٣) تهدف هذه الدراسة إلى استعراض دور الذكاء الاصطناعي في تعزيز الأمن السيبراني في مجال التجارة الإلكترونية، مع التركيز على حماية البيانات ومعالجة الاحتيال، من خلال استعراض التجارب الدولية والعربية.

عبد الرحمن، م. (٢٠٢٤) تبحث هذه الدراسة في تأثير استخدام الذكاء الاصطناعي في العمليات الحربية السيبرانية وتأثيرها على البيئة الإنسانية خلال النزاعات المسلحة.

الإطار النظري

يتناول الإطار النظري لهذا البحث مفهوم **الذكاء الاصطناعي** في الأمن السيبراني، وتطور استخداماته عبر السنين، من المراحل الأولى التي اعتمدت على برامج حماية أساسية مثل جدران الحماية والبرمجيات المضادة للفيروسات، إلى التقنيات الأكثر تطورًا مثل **التعلم الآلي** و**التعلم العميق** .كما يتطرق إلى العلاقة بين الذكاء الاصطناعي وتقنيات أخرى مثل **الحوسبة الكمومية**، التي يمكن أن تُحدث ثورة في تحسين فعالية الأنظمة الذكية.

الذكاء الاصطناعي والأمن السيبراني

الذكاء الاصطناعي هو مجال من مجالات علوم الحاسوب يهدف إلى تطوير أنظمة قادرة على محاكاة بعض وظائف الدماغ البشري مثل التفكير، التعلم، اتخاذ القرارات، والتفاعل مع البيئة. في الأمن السيبراني، يتم استخدام الذكاء الاصطناعي بشكل رئيسي لتحليل البيانات واكتشاف التهديدات المتقدمة. وتشمل هذه التقنيات **التعلم الآلي** (Machine Learning)و**التعلم العميق** (Deep Learning)، التي تساعد في تحديد الأنماط المشبوهة التي قد تشير إلى محاولات اختراق.

الأمن السيبراني هو مجال يختص بحماية الأنظمة والشبكات الإلكترونية من التهديدات المحتملة مثل الهجمات الإلكترونية، الفيروسات، تسريب البيانات، والبرمجيات الخبيثة. ومع تزايد التهديدات، أصبح من الضروري استخدام تقنيات حديثة مثل الذكاء الاصطناعي لتعزيز الدفاعات ضد هذه التهديدات.

دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني

كشف التهديدات السيبرانية

Russell, B. (2020) يُعتبر الكشف عن التهديدات السيبرانية من أهم التطبيقات التي يعززها الذكاء الاصطناعي في مجال الأمن السيبراني، حيث تعتمد الأنظمة الحديثة على خوارزميات **التعلم الآلي** (Machine Learning)و**التعلم العميق** (Deep Learning)لتحليل البيانات الضخمة، واكتشاف الأنماط غير الطبيعية التي قد تشير إلى هجوم إلكتروني محتمل.

- **اولاً : تقنيات كشف التهديدات السيبرانية باستخدام الذكاء الاصطناعي:**

١. **تحليل البيانات الكبيرة:(Big Data Analytics)**

تعتمد أنظمة الذكاء الاصطناعي على تحليل كميات هائلة من البيانات الواردة من الشبكات والأنظمة لتحديد أي أنشطة غير طبيعية قد تشير إلى تهديد سيبراني.

٢. **الكشف عن الأنماط السلوكية الشاذة:(Anomaly Detection)**

يتم استخدام تقنيات الذكاء الاصطناعي لرصد **التغيرات غير الطبيعية** في سلوك المستخدمين أو التطبيقات داخل الشبكة.

على سبيل المثال، إذا قام موظف بمحاولة **الوصول إلى بيانات حساسة بشكل غير معتاد،** يمكن للنظام تصنيف هذا النشاط على أنه تهديد محتمل.

٣. **تحليل التهديدات في الوقت الفعلي (Real-Time Threat Detection):**

تقوم أنظمة الذكاء الاصطناعي بتحليل تدفق البيانات بشكل فوري واستخدام **التعلم الآلي التنبؤي** (Predictive Machine Learning)لاكتشاف الهجمات قبل وقوعها.

٤. **الكشف عن البرمجيات الخبيثة:(Malware Detection)**

يتم تدريب النماذج الذكية على التعرف على **التوقيعات السلوكية** للبرمجيات الخبيثة والفيروسات، حتى تلك التي لم يتم تصنيفها مسبقًا في قواعد البيانات التقليدية.

- **ثانياً: أمثلة عملية على كشف التهديدات السيبرانية:**

١. تستخدم **شركة Darktrace** أنظمة الذكاء الاصطناعي لمراقبة الشبكات، وتحليل التهديدات من خلال تقنية "**نظام المناعة الرقمي** (Cyber Immune System)"، الذي يعمل بطريقة مشابهة لجهاز المناعة في جسم الإنسان.

٢. **FireEye**تعتمد على التعلم العميق لتحديد الهجمات السيبرانية **المعقدة** التي قد لا يتم اكتشافها باستخدام الأدوات التقليدية.

الاستجابة السريعة للهجمات

في حال اكتشاف هجوم، يمكن للذكاء الاصطناعي الاستجابة بسرعة عبر اتخاذ الإجراءات الضرورية بشكل فوري، مثل إغلاق المنافذ الأمنية أو تعطيل

الحسابات المشبوهة. على سبيل المثال، يمكن للأنظمة الذكية التفاعل مع الهجمات في الوقت الفعلي من خلال آليات استجابة تلقائية.

حيث تُعد الأنظمة الذكية المدعومة بالذكاء الاصطناعي أدوات فعالة لمواجهة التهديدات السيبرانية **في الوقت الفعلي**، حيث يمكنها التفاعل بسرعة فائقة مع الهجمات واتخاذ **إجراءات استجابة تلقائية** لمنع أي ضرر محتمل. تعتمد هذه الأنظمة على عدة آليات، منها:

- **اولاً : آليات الاستجابة التلقائية للهجمات السيبرانية**

١) الاكتشاف الفوري للهجمات (Real-Time Threat Detection)

تستخدم الأنظمة الذكية **تحليل البيانات الضخمة** (Big Data Analytics) وتقنيات **التعلم الآلي** (Machine Learning)للكشف عن **أنماط النشاط المشبوهة** بمجرد حدوثها. عند اكتشاف أي **نشاط غير طبيعي** مثل **محاولات الاختراق أو الانتشار السريع للبرمجيات الخبيثة**، تقوم الأنظمة بتحديد مستوى التهديد وتفعيل إجراءات الاستجابة المناسبة.(Wang et al., 2021)

٢) العزل التلقائي للأنظمة المخترقة (Automated Containment)

عند اكتشاف اختراق أو نشاط ضار، يمكن للأنظمة الذكية **عزل الجهاز المصاب** أو **إغلاق المنفذ الذي يتم من خلاله الاختراق** لمنع انتشار التهديد إلى باقي الشبكة. على سبيل المثال، إذا تم اكتشاف هجوم **برمجيات الفدية** (Ransomware)، يمكن للنظام الذكي **تجميد الملفات المشبوهة ومنع التشفير التلقائي** لحماية البيانات.

٣) الاستجابة التلقائية عبر جدران الحماية الذكية (AI-Powered Firewalls)

تُستخدم جدران الحماية الذكية التي تعمل بالذكاء الاصطناعي لتحليل **حركة البيانات داخل الشبكة**، ويمكنها **حظر** أي حركة مرور غير طبيعية **بشكل تلقائي** . على سبيل المثال، إذا بدأ جهاز معين في إرسال **كميات ضخمة من البيانات** إلى عنوان IP غير معروف، يمكن للنظام التعرف عليه كـ **هجوم رفض الخدمة الموزع (DDoS)**واتخاذ إجراء فوري لمنع الاتصال المشبوه.

٤) الاستجابة الاستباقية باستخدام التعلم التنبؤي (Predictive Response Systems)

تعتمد هذه الأنظمة على **التحليل التنبؤي** (Predictive Analytics)لتوقع التهديدات قبل وقوعها. يتم تدريب الذكاء الاصطناعي على **التعرف على سلوكيات الهجمات السابقة**، مما يساعده على **منع التهديدات المستقبلية قبل تنفيذها**.

٥) تنبيه الفرق الأمنية والرد التلقائي (Automated Incident Response)

تقوم الأنظمة الذكية بإرسال **تنبيهات فورية** إلى فرق الأمن السيبراني، كما يمكنها تنفيذ إجراءات **استباقية تلقائية** مثل:

- **إعادة ضبط كلمات المرور** للحسابات المخترقة.
- **حظر عنوان IP المشتبه به** لمنع المزيد من الهجمات.
- **تعطيل الحسابات المشبوهة مؤقتًا** إلى حين التحقق منها.

- **ثانياً: مثال عملي على الاستجابة التلقائية للهجمات**

شركة **Darktrace**تستخدم نظام "**المناعة الرقمية** (Enterprise Immune System)"الذي يعتمد على الذكاء الاصطناعي لرصد سلوك

المستخدمين والأجهزة داخل الشبكة. عند اكتشاف أي **نشاط غير معتاد**، يقوم النظام تلقائيًا **بعزل الجهاز المشتبه به** ومنع الهجوم من الانتشار (Johnson & Miller, 2022).

تحليل سلوك المستخدمين

يمكن للذكاء الاصطناعي استخدام تقنيات **تحليل السلوك** لمراقبة سلوك المستخدمين داخل النظام الإلكتروني واكتشاف أي تغييرات غير طبيعية قد تشير إلى اختراق. على سبيل المثال، يمكن للنظام الذكي أن يتعرف على محاولات الوصول غير المصرح بها إلى ملفات معينة، وتنبيه المسؤولين على الفور.

التحديات التي يواجهها الذكاء الاصطناعي في الأمن السيبراني

نقص البيانات الكافية

يحتاج الذكاء الاصطناعي إلى كميات ضخمة من البيانات لتدريب الأنظمة بشكل دقيق. إذا كانت البيانات غير كافية أو تحتوي على معلومات مغلوطة، فإن قدرة النظام على الكشف عن التهديدات تتأثر بشكل كبير.

الهجمات المتطورة

الهجمات السيبرانية اليوم أصبحت أكثر تطورًا، وتستخدم تقنيات مثل **الهندسة الاجتماعية** أو **البرمجيات الخبيثة المتقدمة** التي قد لا تتمكن أنظمة الذكاء الاصطناعي التقليدية من اكتشافها بسرعة.

قيود الخوارزميات

قد تحتوي الخوارزميات المستخدمة في الذكاء الاصطناعي على ثغرات يمكن للمهاجمين استغلالها. علاوة على ذلك، قد تكون الخوارزميات بطيئة في التكيف مع أنواع جديدة من الهجمات.

قضايا الخصوصية والأخلاقيات

استخدام الذكاء الاصطناعي لمراقبة سلوك المستخدمين قد يثير قضايا تتعلق بالخصوصية. خصوصًا إذا كانت الأنظمة تقوم بتخزين وتحليل بيانات شخصية حساسة.

الحلول المستقبلية والفرص

التكامل مع الحوسبة الكمومية

الحوسبة الكمومية تقدم إمكانيات ضخمة في معالجة البيانات. من خلال دمج الذكاء الاصطناعي مع الحوسبة الكمومية، يمكن تحسين قدرة الأنظمة على التعامل مع كميات ضخمة من البيانات ومعالجة التهديدات بسرعة أكبر.

الذكاء الاصطناعي المعزز

يمكن تطوير أنظمة الذكاء الاصطناعي المعزز لتصبح أكثر قدرة على التكيف مع الهجمات السيبرانية المعقدة. من خلال تحسين الخوارزميات وتزويدها ببيانات أكثر تنوعًا، تمكن الذكاء الاصطناعي من تقديم حلول أمان أكثر فعالية .

تحليل التهديدات التنبؤي

مستقبل الذكاء الاصطناعي في الأمن السيبراني قد يشمل القدرة على **التنبؤ** بالهجمات قبل وقوعها، باستخدام تقنيات **التعلم العميق** لتحليل الأنماط الهجومية المستقبلية كما يكم الاستفادة من تحليل التهديدات التنبؤية كالتالي:

١. لكشف المبكر عن التهديدات السيبرانية

يُمكّن تحليل التهديدات التنبؤية الشركات والمؤسسات من **رصد الأنشطة المشبوهة** قبل أن تتحول إلى هجمات فعلية. على سبيل المثال، إذا بدأت **حركة مرور الشبكة** تُظهر نمطًا مشابهًا لهجمات سابقة، يمكن للنظام التنبؤ بإمكانية حدوث هجوم و**إصدار تنبيه مبكر.**

٢. **تقليل زمن الاستجابة للهجمات**

تساهم النماذج التنبؤية في **تقليل وقت الاستجابة** للهجمات الإلكترونية، حيث يتم اكتشاف الأنشطة المشبوهة **بشكل استباقي**، مما يمنح فرق الأمن السيبراني الوقت الكافي لاتخاذ الإجراءات الوقائية.

٣. **تعزيز استراتيجيات الدفاع السيبراني**

من خلال تحليل بيانات الهجمات السابقة، يمكن للشركات **تحسين استراتيجيات الأمن السيبراني** وتعزيز دفاعاتها بناءً على التهديدات المتوقعة. يساعد ذلك في **تطوير سياسات أمنية أكثر كفاءة** واستباقية.

٤. **تقليل التكاليف التشغيلية**

الكشف المبكر عن التهديدات يقلل من تكلفة إصلاح الأضرار الناجمة عن الهجمات السيبرانية. فبدلاً من التعامل مع تداعيات الاختراقات الأمنية، يمكن استخدام تحليل التهديدات التنبؤية لمنعها من الأساس، مما يقلل من **النفقات المرتبطة بالاستجابة للحوادث السيبرانية.**

٥. **تحسين أمن البنية التحتية السحابية**

مع تزايد استخدام **الخدمات السحابية**، أصبح من الضروري استخدام تحليل التهديدات التنبؤية لاكتشاف محاولات **الاختراق والتسلل إلى الأنظمة السحابية** قبل حدوثها. تساعد هذه التقنية في حماية البيانات المخزنة على السحابة من الهجمات المحتملة.

٦. **دعم اتخاذ القرارات الأمنية**

من خلال التحليل التنبؤي، يمكن لقادة الأمن السيبراني اتخاذ **قرارات** مبنية على البيانات لتوجيه الموارد بشكل أكثر كفاءة، مثل تحديد الأولويات الأمنية، وتعزيز الحماية في المناطق الأكثر تعرضًا للهجمات.

مثال عملي على تحليل التهديدات التنبؤية

تستخدم شركة **IBM Watson for Cybersecurity** الذكاء الاصطناعي والتعلم العميق لتحليل مليارات نقاط البيانات يوميًا، مما يساعدها على **التنبؤ بالهجمات السيبرانية المحتملة** وتوفير استجابة أسرع وأكثر كفاءة (Smith & Johnson, 2022).

الإطار التطبيقي

يعرض هذا القسم التطبيقات العملية لتقنيات الذكاء الاصطناعي في المؤسسات الكبيرة مثل **FireEye** و**Darktrace**، التي تستخدم الذكاء الاصطناعي للكشف عن الهجمات المتقدمة، وتحليل سلوك المستخدمين، والاستجابة الفورية للهجمات. كما سيتم استعراض أمثلة على تطبيق الذكاء الاصطناعي في المؤسسات الحكومية ومراكز البيانات.

التطبيقات العملية لتقنيات الذكاء الاصطناعي في المؤسسات الكبيرة

١. **الذكاء الاصطناعي للكشف عن الهجمات المتقدمة: FireEye .**

تعتبر شركة **FireEye** واحدة من أبرز الشركات في مجال الأمن السيبراني، وهي تعتمد بشكل كبير على تقنيات الذكاء الاصطناعي للكشف عن التهديدات المتقدمة **FireEye** .تستخدم الذكاء الاصطناعي في دمج أدوات التحليل المتقدمة لاكتشاف الهجمات التي يصعب اكتشافها باستخدام الأساليب التقليدية مثل **الهجمات المتقدمة المستمرة (APT).** هذه الهجمات عادةً ما تكون مدعومة من دول أو جماعات منظمة تتبع استراتيجيات متطورة في الهجوم.

التطبيقات العملية:

- **الكشف التلقائي عن التهديدات المتقدمة** :من خلال تحليل البيانات الشبكية وسلوك الأنظمة بشكل مستمر، تستطيع الأنظمة المدعومة بالذكاء

الاصطناعي اكتشاف الأنماط غير الطبيعية في الوقت الفعلي. تعتمد FireEyeعلى تقنيات مثل التعلم الآلي (ML) للتعرف على التهديدات المعروفة وغير المعروفة.

- **الاستجابة التلقائية للهجمات** :يمكن للنظام المدعوم بالذكاء الاصطناعي أن يستجيب للهجمات بشكل تلقائي أو شبه تلقائي، عبر اتخاذ إجراءات لحظر الهجوم أو عزل النظام المتأثر، مما يقلل من الأضرار ويحسن سرعة الاستجابة.
- **تحليل سلوك المستخدمين** :تستخدم FireEye تقنيات الذكاء الاصطناعي لتحليل سلوك المستخدمين داخل الشبكة. أي سلوك غير عادي يتم اكتشافه يمكن أن يشير إلى اختراق أو تصرف غير مصرح به. كما يتيح التعرف على الأنماط غير الطبيعية تحديد الحسابات التي قد تكون قد تعرضت للاختراق.

٢. **.الذكاء الاصطناعي في مراقبة الشبكات:Darktrace**

تعد **Darktrace**من الشركات الرائدة في تطبيق تقنيات الذكاء الاصطناعي في مراقبة الشبكات وتحليل التهديدات في الوقت الفعلي. تعتمد Darktrace على **التعلم العميق (Deep Learning)** لتحليل سلوك الشبكة بشكل مستمر واكتشاف التهديدات من خلال ما يسمى بـ **الذكاء الاصطناعي المدعوم بتعلم الآلة(Self-Learning AI).**

التطبيقات العملية:

- **التحليل الذكي لسلوك الشبكة** :يُستخدم الذكاء الاصطناعي لمراقبة الأنشطة والاتصالات داخل الشبكة على مدار الساعة. يتم تحليل البيانات البيانية بشكل ديناميكي للكشف عن أي هجوم أو نشاط غير معتاد.

- **الحماية التنبؤية** :تتيح تقنيات الذكاء الاصطناعي في Darktrace الكشف التنبئي عن الهجمات قبل وقوعها عبر التعرف على الأنماط غير المعتادة والتهديدات المتطورة.
- **استجابة فورية** :في حال حدوث هجوم، يستطيع النظام اتخاذ إجراءات دفاعية في الوقت الفعلي مثل تعطيل الاتصال المشبوه، ومنع الوصول إلى الأنظمة الحيوية، وذلك باستخدام الذكاء الاصطناعي لتقليل حجم الضرر.

٣. تطبيقات الذكاء الاصطناعي في المؤسسات الحكومية

تطبيقات في قطاع الدفاع الوطني والأمن

تستخدم العديد من المؤسسات الحكومية الذكاء الاصطناعي لتعزيز مستوى الأمن السيبراني، خاصة في قطاعات الدفاع الوطني والأمن الداخلي. تعتمد المؤسسات مثل وزارة الدفاع الأمريكية على الذكاء الاصطناعي لتحليل المعلومات الاستخباراتية وتحليل تهديدات الأمن السيبراني.

التطبيقات العملية:

- **الذكاء الاصطناعي في مراقبة الشبكات** :يتم استخدام تقنيات الذكاء الاصطناعي لتتبع نشاط الشبكات الحكومية ومراقبة جميع البيانات المتداولة داخلها. يهدف ذلك إلى الكشف عن الأنشطة المشبوهة والحد من التهديدات السيبرانية.
- **التعلم الآلي في تحليل الهجمات** :تقوم بعض الوكالات الحكومية باستخدام تقنيات مثل **التعلم الآلي** لتحليل سلوك الشبكة وتحديد الأنماط غير الاعتيادية التي قد تشير إلى وجود هجوم سيبراني معقد أو هجمات.APT

٤. تطبيقات في حماية البيانات الشخصية والحكومية

من خلال الذكاء الاصطناعي، تستطيع الحكومات تعزيز جهودها لحماية

البيانات الحساسة للمواطنين والبيانات الحكومية، خاصة في ظل تزايد التهديدات السيبرانية.

التطبيقات العملية:

- **التحليل الأمني للبيانات** :تعتمد بعض الحكومات على الذكاء الاصطناعي لتحليل البيانات الكبيرة الخاصة بالمواطنين، بما في ذلك الأنشطة المالية أو القانونية، بهدف الكشف عن أي محاولات اختراق أو سرقة بيانات.
- **أنظمة أمان معززة** :تستخدم بعض الحكومات أنظمة تعتمد على الذكاء الاصطناعي مثل **التشفير الذكي** للكشف عن نقاط الضعف في نظم تخزين البيانات وتعزيز قدرتها على مواجهة محاولات السرقات الإلكترونية.

٥. تطبيقات الذكاء الاصطناعي في مراكز البيانات

تحسين الأمن في مراكز البيانات

تعتمد مراكز البيانات، التي تستضيف كميات هائلة من المعلومات الحساسة، على تقنيات الذكاء الاصطناعي لتحسين الأمن وحمايتها من الهجمات. يستخدم الذكاء الاصطناعي لتطوير أنظمة مراقبة مستمرة وتحليل سلوك الشبكات داخل مراكز البيانات.

التطبيقات العملية:

- **الكشف عن الهجمات في الوقت الفعلي** :أنظمة الذكاء الاصطناعي يمكنها التنبؤ بالتهديدات المتزايدة داخل مراكز البيانات قبل حدوثها، عبر استخدام تقنيات مثل **الذكاء الاصطناعي القائم على السحابة** للتحقق من البيانات ومعالجة الأنشطة المشبوهة.

- **إدارة أداء النظام** :الذكاء الاصطناعي يساعد أيضًا في إدارة موارد النظام في مراكز البيانات، مثل تحسين تخصيص الذاكرة أو التحكم في تدفق البيانات داخل الخوادم لتجنب الأعطال أو الهجمات الموزعة.

النتائج والتوصيات المقترحة

النتائج:

١. **تحسن كبير في كشف التهديدات** :أظهرت نتائج البحث أن استخدام الذكاء الاصطناعي يمكن أن يُحسن بشكل كبير من دقة وكفاءة الكشف عن التهديدات السيبرانية.

٢. **التحديات التقنية** :تواجه تقنيات الذكاء الاصطناعي بعض التحديات مثل نقص البيانات، الهجمات المتقدمة التي تتفوق على الأنظمة الحالية، وصعوبة التكامل بين التقنيات المختلفة.

التوصيات:

١. **استثمار أكبر في تدريب النماذج** : ضرورة توفير كميات أكبر من البيانات وتدريب الأنظمة على حالات متعددة لتحسين دقة الكشف.

٢. **التعاون بين التخصصات:** تشجيع التعاون بين خبراء الذكاء الاصطناعي، الأمن السيبراني، والحوسبة .

٣. **الاهتمام بالجوانب الأخلاقية** : يجب على المؤسسات الاهتمام بالجوانب الأخلاقية والخصوصية عند استخدام الذكاء الاصطناعي في مراقبة سلوك المستخدمين.

المراجع

مراجع باللغة العربية:

- الجندي، ع. (٢٠١٩). *الذكاء الاصطناعي والأمن السيبراني: دراسة تحليلية للمستقبل*. مجلة العلوم التقنية، ٣٠(٤)، ١٥٥-١٧١.
- الغامدي، م. (٢٠٢٠). *التحديات المستقبلية في الذكاء الاصطناعي في مجال الأمن السيبراني*. المجلة العربية للأمن السيبراني، ٥(٣)، ١٠١-١١٥.
- *عتلم، ش. (٢٠٢٢). آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة*. مجلة القانون الدولي الإنساني.
- *Root-X. (2022). الذكاء الاصطناعي في الأمن السيبراني.Root-X*.
- *TechAcute. (2022). تأثير الذكاء الاصطناعي على الأمن السيبراني: الفرص والتحديات.TechAcute*.
- بن عيسى، ن. (٢٠٢٢). الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني (واقع اليوم ورهان الغد). مجلة دراسات اقتصادية، ١٥(١)، ١٢٣-١٤٠
- بن عيسى، ن. (٢٠٢٣). الذكاء الاصطناعي والأمن السيبراني في التجارة الإلكترونية: حماية البيانات ومعالجة الاحتيال. مجلة العلوم الاقتصادية والتسيير، ١٠(٢)، ٨٥-١٠٢ .
- عبد الرحمن، م. (٢٠٢٤). آثار الذكاء الاصطناعي والحرب السيبرانية على البيئة الإنسانية أثناء النزاعات المسلحة. مجلة القانون الدولي الإنساني، ٦(١)، ٤٥-٦٠.

مراجع باللغة الإنجليزية:

- Jordan, P. M. (2018). Integrating machine learning into cybersecurity defense. In T. B. Roberts (Ed.), *Proceedings of the International Conference on Cybersecurity* (pp. 45-58). Springer.
- Smith, J. A. (2020). The role of artificial intelligence in cybersecurity. *Journal of Cybersecurity Studies, 15*(2), 112-130.
- Williams, S. (2021, June 15). How artificial intelligence is reshaping cybersecurity. *Tech Times*.
- Russell, B. (2020). *Artificial intelligence in cybersecurity: Threat detection and mitigation strategies*. Cybersecurity Journal, 15(3), 112-130
- Wang, L., Chen, J., & Zhang, X. (2021). *Real-time AI-driven cybersecurity threat detection and response*. Journal of Cyber Intelligence, 14(2), 78-95.
- Johnson, M., & Miller, R. (2022). *AI-powered defense mechanisms: Automated containment and response strategies*. Cybersecurity Review, 10(4), 33-50
- Smith, J., & Johnson, R. (2022). *Predictive analytics in cybersecurity: Leveraging AI for proactive defense*. Cyber Threat Intelligence Journal, 15(3), 45-62.

مواقع الكترونية :

- https://www.techtimes.com/articles/28765/20210615/ai-in-cybersecurity.htm
- https://doi.org/10.1007/978-3-319-61042-8_5
- https://doi.org/10.1016/j.jcyb.2020.05.005

Egyption Journal
For Specialized Studies
Quarterly Published by Faculty of Specific Education, Ain Shams University

Correspondence:
Editor in Chief
365 Ramses St- Ain Shams University,
Faculty of Specific Education
Tel: 02/26844594
Web Site :
https://ejos.journals.ekb.eg
Email :
egyjournal@sedu.asu.edu.eg

ISBN : 1687 - 6164
ISNN : 4353 - 2682

Evaluation (July 2024) : (7) Point
Arcif Analytics (Oct 2024) : (0.4167)
VOL (13) N (46) P (5)
April 2025