الاختراق السيبراني والتهديد الامني في مجال الذكاء الاصطناعي

الأستاذ الدكتور مهندس/ هشام نبيه المهدي
رئيس لجنة السلامة والصحة المهنية
أستاذ تكنولوجيا المعلومات
كلية الحاسبات والذكاء الاصطناعي جامعة القاهرة
الوكيل السابق لشئون خدمة المجتمع وتنمية البيئة
ehesham.cu.edu.eg

القاهرة مايو 2024

1- التحيز في صنع القرار

في حال استخدام أنظمة الذكاء الاصطناعي القائمة على مجموعات البيانات التي تحتوي على معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني؛ فقد يؤدي ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.ر وعلى سبيل المثال، إذا اتخذ الذكاء الاصطناعي قرارًا قائم على المدخلات المتحيزة؛ فقد ينتج عن ذلك منع المستخدمين الشرعيين من الوصول إلى أنظمة الشركة.

2- الافتقار إلى القابلية للتفسير والشفافية

تتسم الخوارزميات المستخدمة لاتخاذ قرارات بشأن التهديدات الأمنية بعدم الشفافية في كل الأوقات، وهو ما يصعب من تفسير قرارات الذكاء الاصطناعي السيئة ويُفقد القدرة على تحسينها، وبالتالي يتأثر أمن المنظمة بالسلب.

3- الاستخدام الضار للخوارزميات

على الرغم من أن خوارزميات الذكاء الاصطناعي تعمل على البحث في البيانات واكتشاف الأنماط بسرعة؛ إلا أن الجهات الضارة تستطيع استخدامها في الوصول إلى المعلومات الحساسة أو مهاجمة البنية التحتية.

كما يمكن للمهاجمين السيبرانيين أيضًا الاستفادة من الذكاء الاصطناعي في شن هجمات أكثر تعقيدًا من خلال التعلم من البيانات لفهم الأهداف ونقاط الضعف المحتملة بشكل أفضل.

4- إساءة استخدام الذكاء الاصطناعي

قد يضر الذكاء الاصطناعي بالأمن السيبراني عندما يُستخدم في أغراض ضارة مثل إنشاء أخبار مزيفة أو نشر دعاية سلبية.

5- انتهاك خصوصية البيانات

هناك العديد من المخاوف المُثارة بشأن خصوصية البيانات التي تعالجها وتحللها تطبيقات الذكاء الاصطناعي في الأمن، إذ أن تلك التطبيقات قادرة على التعرف على تلك البيانات، وهو ما يفرض ضرورة الامتثال للوائح الخصوصية من خلال الفحص القانوني قبل نشر أنظمة الذكاء الاصطناعي. وختامًا، فإن استخدام الذكاء الاصطناعي في مجال الأمن السيبراني بات ضرورة لا غنى عنها، حتى تعزز المؤسسات من أداء أمن تكنولوجيا المعلومات، في ظل الزيادة غير المسبوقة للهجمات الإلكترونية خلال السنوات الأخيرة.

كيف يمكن لتحليل البيانات في نظم الذكاء الاصطناعي أن يتسبب في انتهاك الخصوصية؟

انتهاك الخصوصية :يمكن لأنظمة الذكاء الاصطناعي جمع وتحليل كميات كبيرة من البيانات الشخصية، مما قد يؤدي إلى انتهاك الخصوصية .المعلومات المضللة :يمكن استخدام تقنيات الذكاء الاصطناعي لإنشاء معلومات مضللة،

ما هي أفضل الممارسات لتوفير حماية البيانات والخصوصية في نظم الذكاء الاصطناعي؟

تعد حماية البيانات جانبًا مهمًا لتطبيقات الذكاء الاصطناعي (AI). تقوم نماذج الذكاء الاصطناعي بتحليل كميات هائلة من البيانات لوضع تنبؤات وقرارات وتوصيات. ويضمن الحفاظ على خصوصية وأمن هذه البيانات مصداقية وموثوقية أنظمة الذكاء الاصطناعي، ويمنع الوصول غير المصرح به إلى المعلومات الحساسة، ويساعد على تجنب العواقب القانونية المحتملة. بعض الأسباب التي تجعل حماية البيانات أمرًا بالغ الأهمية في تطبيقات الذكاء الاصطناعي هي:

الثقة والموثوقية: يساعد ضمان خصوصية وأمن البيانات المستخدمة في أنظمة الذكاء الاصطناعي على بناء ثقة المستخدم ومصداقية النظام. من الأرجح أن يتفاعل المستخدمون مع تطبيقات الذكاء الاصطناعي ويعتمدون عليها عندما يكونون واثقين من حماية معلوماتهم الشخصية والحساسة.

الامتثال القانوني: تتطلب لوائح حماية البيانات المختلفة، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي وقانون خصوصية المستهلك في كاليفورنيا (CCPA) في الولايات المتحدة، من الشركات حماية بيانات المستخدم من الوصول والاستخدام غير المصرح به. يمكن أن يؤدي عدم الامتثال لهذه اللوائح إلى فرض غرامات باهظة والإضرار بسمعة الشركة. منع خروقات البيانات: يمكن أن يكون لخروقات البيانات عواقب وخيمة، بما في ذلك الخسائر المالية والإضرار بالسمعة والمشكلات القانونية. يساعد ضمان حماية البيانات في تطبيقات الذكاء الاصطناعي على تقليل مخاطر اختراق البيانات ويقلل من تأثير حوادث الأمن السيبراني.

ما هي الحلول التي يمكن اتخاذها للوقاية من تسرب البيانات واختراق النظم في نظم الذكاء الاصطناعي؟

حلول الأمن السيبراني

التخطيط الاستيراتيجي تطوير استراتيجية الأعمال

الابتكار المؤسسي تأسيس وتشغيل مركز الابتكار المؤسسي

التخصيص تصميم وتطوير إستراتيجيات التخصيص

التميز المؤسسي تصميم إطار التميز المؤسسي

الحوكمة والمخاطر والامتثال و استمرارية الاعمال إدارة الحوكمة المؤسسية

ما هي التحديات الأخلاقية التي تواجه جمع البيانات واستخدامها في تطبيقات الذكاء الاصطناعي؟

قد يتعجب البعض من حقيقة أنه يوجد نحو 39 تحدياً أخلاقياً واقتصادياً للذكاء الاصطناعي حول العالم. وأبرز تلك التحديات هي: –تكلفة الابتكار في هذا المجال.حهخ

–انعدام الثقة الكاملة في الذكاء الاصطناعي من قبل الكثيرين. –نقص في جودة البيانات. –اختفاء بعض الوظائف –.الضرر على السلامة الجسدية للبشر احيانا عند التعامل مع الروبوتات.

–قلة الخصوصية خاصة حين استخدام بيانات المجالات الصحية والأمنية وغيرها.

–الظهور المفاجئ للذكاء الاصطناعي وضرورة تبنيه بشكل سريع.

–التحديات الأمنية ذات الصلة. –مشكلات عدم النزاهة وتحيز البيانات في بعض الأحيان.

–انعدام الشفافية. –إمكانية الاستخدام الإجرامي والضار.

–فقدان الحرية والاستقلالية الفردية نتيجة رقابة الآلة المستمرة.

–عدم السماح بوصول أنظمة الذكاء الاصطناعي إلى العديد من الخدمات العامة والحكومية.

–الحد من التواصل البشري خاصة في المجال الصحي. –عدم وجود المساءلة والمسؤولية.

–التأثير السلبي على البيئة. – فقدان الإنسان للقرار. –عدم وصول البشر إلى المعلومات بسهولة.

–زيادة استخدام تكنولوجيات الذكاء الاصطناعي غير الموثوق بها في مجال إنفاذ القانون.

واليوم، توجد آليات تقنية متطورة للذكاء الاصطناعي تعمل على جمع وتحليل البيانات المختلفة، في أنظمة ذكية ترتبط بكافة مجالات الحياة، بدءاً من معلومات الأفراد الشخصية والعائلية، والمعلومات الصحية والبنكية، ووصولاً إلى معلومات التسوق الخاصة بالأفراد ، واستخدام السيارات ذاتية القيادة. وكذلك توجد البيانات الضخمة التي تتوفر من خلال شبكات الانترنت والأنظمة المختلفة في المؤسسات والهيئات الحكومية والمصانع والقطاع الخاص، وأيضا تلك الخاصة بالطاقة والموارد، والتي تُستخدم في تغذية انظمة الذكاء الاصطناعي للتعلم والتحليل والتنبؤ المستقبلي في المجالات الاقتصادية والاجتماعية والصحية والعلمية المختلفة. وكذلك، أصبحت هناك مصادر كثيرة من الممكن خلالها الحصول على تلك البيانات واستخدامها سواء بطرق قانونية وأخلاقية، او غيرها. كما أنه لا يوجد حالياً بنية تحتية قانونية لازمة لضمان التطور الأخلاقي للتكنولوجيا الخاصة بالذكاء الاصطناعي. ولذلك، تعتبر أخلاقيات علم البيانات والذكاء الاصطناعي هي النصوص والتشريعات التي تمكننا من معرفة ما هو الصواب وما هو الخطأ خلال التعامل مع تلك التقنية. وبالمقام الأول، أصبح هناك اهتمام بالعديد من العناصر المهمة التي تساعد في عمل تلك التشريعات، مثل حوكمة البيانات المغذية للأنظمة الذكية وتحديد ملكيتها، وتصنيفها، وخصوصيتها، وصلاحية الوصول والاستفادة منها، وكذلك حماية تلك البيانات وأمنها. ويوجد عنصر هام آخر في مجال أخلاقيات الذكاء الاصطناعي، وهو ضرورة أن تكون البيانات، المُستخدمة في تغذية الآلات الذكية، ذات جودة عالية ويمكن الوثوق والاعتماد عليها. ومؤخرا، فقد اعتمدت جميع الدول الأعضاء في اليونسكو، وعددهم 193 دولة، اتفاقاً عالمياً تاريخياً يحدد المبادئ والأخلاقيات والقيم "المشتركة" اللازمة لضمان تطوير الذكاء الاصطناعي بصورة سليمة، ومن أجل وضع قواعد للذكاء الاصطناعي تعود بالنفع على البشرية. ويهدف هذا الاتفاق إلى توجيه بناء البنية التحتية القانونية اللازمة لضمان التطور الأخلاقي لهذه التكنولوجيا، وضمان الشفافية والأهلية وتحكم الأفراد في بياناتهم الشخصية. كما تحظر الاتفاقية استخدام أنظمة الذكاء الاصطناعي في التقييم الاجتماعي أو المراقبة الجماعية.

مقدمة:

يستمرّ الذكاء الاصطناعي في تغيير وتطوير عدد لا يحصى من الصناعات والمجالات، وليس الأمن السيبراني استثناءً. وبينما نستمرّ في التكيّف مع الطابع الرقمي المتنامي لعصرنا هذا، فكان من الأهمية أن نفهم كيف يمكن للذكاء الاصطناعي تعزيز جهود الأمن السيبراني ، حتى يكون وجودنا وتجاربنا عبر الإنترنت أكثر أمانًا وأمانًا. لنبدأ بتعرفات الذكاء الاصطناعي والأمن السيبراني.

الذكاء الاصطناعي

هو أحد أفرع علوم الحاسب الذي يهتم باستخدام أجهزة الحاسوب لحل المهام التي لم يكن من الممكن حلها سابقًا إلا من خلال تطبيق الذكاء البشري. وهناك تعريفان للذكاء الاصطناعي: عند عدم الأخذ في الاعتبار علم النفس أو الأخذ في الاعتبار علم النفس عند عدم الأخذ في الاعتبار علم النفس فإن الذكاء الاصطناعي هو دراسة تقنيات حل المشكلات الصعبة بشكل كبير في وقت متعدد الحدود من خلال استغلال المعرفة حول مجال المشكلة. أما عند الأخذ في الاعتبار علم النفس: فإن الذكاء الاصطناعي هو دراسة كيفية عمل الحواس البشرية ومحاولة محاكاة طريقة عملها باستخدام برمجيات خاصة مع التمثيل الجيد للمعرفة التي تساعد في عملها..الهدف الرئيس للذكاء الاصطناعي هو: محاكاة الأداء البشري .في رحلة تعليم الماكينة لعبة الشطرنج استطعنا نقل كل القواعد والخطط للماكينة فلما قامت الماكينة بملاعبة أبطال اللعبة للشطرنج ونقلنا طريقة وافكار أبطال اللعبة للماكينة وجدنا ان لبعض أولئك الأبطال نقلة غريبة أو تضحية غير مبررة ولم يستطيعوا وضعها كقواعد، ولكن تلك النقلة أو التضحية كانت السبب بعد نقلتين ثلاثة بالفوز بالمباراة.تعامل الذكاء الاصطناعي مع تجميع البيانات وتصنيفها ومعالجتها وتصفيتها وإدارتها.

الأمن السيبراني

الأمن السيبراني هي العملية التي تهدف إلى حماية أنظمة وشبكات الكمبيوتر المتصلة بالإنترنت من الهجمات الرقمية والاختراقات أو التدمير أو التعطيل أو التعطيل . يتضمن الأمن السيبراني العديد من نقاط البيانات التي يمكن استخدامها للذكاء الاصطناعي.

ما علاقة الذكاء الاصطناعي بالامن السيبراني؟

هناك علاقة وثيقة بين الذكاء الاصطناعي والأمن الالكتروني أو السيبراني، إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب.
فبعد تزايد الجرائم الإلكترونية مثل سرقة البيانات والتصيد الاحتيالي؛ لجأت المنظمات إلى عدة وسائل لمكافحة تلك التهديدات، فاستعانت بفرق الأمن السيبراني المؤهلة المجهزة بأحدث التقنيات ومنها تقنية الذكاء الاصطناعي، التي تساعد على الكشف السريع عن الأنشطة الضارة ومواجهتها وتحمي الشبكات من الهجمات الإلكترونية.
ويعمل الذكاء الاصطناعي في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي، تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات، وأتمتة آليات الاستجابة، مما يعزز من البنية التحتية لأمن الشركات.

فوائد لاستخدام الذكاء الاصطناعي في الأمن السيبراني:

تتمثل فوائد استخدام أدوات وأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي فيما يلي:

1- التعامل مع البيانات الضخمة

يجد موظفو الأمن السيبراني صعوبة كبيرة في مراجعة جميع الأنشطة يدويًا بحثًا عن التهديدات المحتملة، وهنا تتجلى فائدة الذكاء الاصطناعي الذي يقوم تلقائيًا بمسح وتحديد التهديدات ويسهل من عملية الكشف عنها ويعزز من الحماية ضدها.

2- تقليل العمليات المزدوجة

من أهم فوائد استخدام الذكاء الاصطناعي في المجال الأمني، قدرته على الكشف عن التهديدات الأمنية الأساسية بانتظام ومنعها، إضافة إلى دوره في التحليل الشامل لتحديد الثغرات الأمنية المحتملة، وهو ما يمكّن الشركات من تنفيذ أفضل ممارسات أمن الشبكة دون التعرض لخطر الخطأ البشري أو الملل الذي يصيب موظفي فرق الأمن السيبراني.

3- تسريع أوقات الكشف والاستجابة

عند قيام الشركات بدمج الذكاء الاصطناعي مع الأمن السيبراني؛ فهي تضمن الكشف السريع عن التهديدات الأمنية والاستجابة لها، لأن الذكاء الاصطناعي يقوم بمسح النظام بالكامل ويحدد التهديدات مبكرًا، ويسهل من المهام الأمنية.

4- محاربة الروبوتات الضارة. هناك الكثير من الروبوتات التي تُستخدم في الأنشطة الضارة مثل نشر البرامج الضارة سرقة البيانات، ويمتلك الذكاء الاصطناعي القدرة على تحديد أنماط تلك الروبوتات والتعرف عليها وحظرها.

5- تأمين المصادقة

يوفر الذكاء الاصطناعي العديد من الأدوات مثل ماسحات بصمات الأصابع والتعرف على الوجه، يوفر الذكاء الاصطناعي العديد من الأدوات مثل ماسحات بصمات الأصابع والتعرف على الوجه، وهي الأدوات المطلوبة لتأمين المصادقة أثناء محاولات تسجيل الدخول على المواقع التي تحتوي على معلومات حساسة وتتطلب طبقة أمان إضافية للحماية.
وتساعد تلك الأدوات على اكتشاف محاولات تسجيل الدخول الاحتيالية والهجمات الإلكترونية التي تهدف إلى سرقة البيانات.

6- تحسين الدقة والكفاءة توفر أنظمة الأمن السيبراني القائمة على الذكاء الاصطناعي دقة وكفاءة أفضل مقارنة بالحلول الأمنية التقليدية، كما تمتلك خوارزميات الذكاء الاصطناعي القدرة على التعرف على الأنماط التي لا تستطيع العين البشرية اكتشافها، وهو ما يزيد من دقة اكتشاف الأنشطة الضارة.

استخدام تعليم الآلة في الأمن السيبراني:

تتعدد طرق استخدام التعلم الآلي في تعزيز الأمن السيبراني، وهي كما يلي:

1- أتمتة مهام الأمان: يساعد التعلم الآلي على تحسين الأمن السيبراني من خلال أتمتة المهام المتكررة، مثل المراقبة والاستجابة للتنبيهات الأمنية، وبالتالي يكون هناك المزيد من الوقت للفرق الأمنية للتركيز على المهام الأكثر تعقيدًا.

2- تعزيز الكشف عن التهديدات

يُستخدم التعلم الآلي في تحديد الأنماط في البيانات التي قد تشير إلى تهديد محتمل، إذ تحلل هذه التقنية مجموعات كبيرة من البيانات، ومن ثم تستطيع الكشف عن الحالات الشاذة التي يمكن أن تكون مؤشرًا على هجوم أو احتيال، وهو ما يزيد من احتمالية التصدي لتلك التهديدات بسرعة أكبر.

3- تعزيز الكشف عن البرامج الضارة

من خلال التعلم الآلي، يمكن تحليل كميات هائلة من البيانات والتي تتيح اكتشاف البرامج الضارة الجديدة وغير المعروفة بسرعة وإزالتها من الأنظمة.

4- اكتشاف برامج الفدية

برامج الفدية هي أحد البرامج الضارة التي تشفر ملفات الضحية، وترهن فك هذا التشفير بدفع فدية، ومن خلال التعلم الآلي تستطيع الروبوتات اكتشاف برامج الفدية قبل أن تقوم بتشفير ملفات الضحية، كما يمكنها التعرف على النشاط الضار وإيقافه.

5- الحماية من التصيد الاحتيالي

المقصود بالتصيد الاحتيالي رسائل البريد الإلكتروني التي يتلقاها الضحية ويظن أن مصدرها موثوق، وعند فتحها يفاجئ بسرقة هويته أو اختراق بياناته.
ويساعد التعلم الآلي على تحديد رسائل البريد الإلكتروني غير المرغوب فيها وتصفيتها، واكتشاف رسائل التصيد فيها وحظرها قبل وصولها إلى المستخدم.

6- الكشف الاستباقي عن التهديدات

غالبًا ما تعمل تدابير الأمن السيبراني التقليدية بطريقة تفاعلية، وتستجيب للتهديدات بعد حدوثها. ومع ذلك، يمكن للذكاء الاصطناعي تحديد الأنماط والشذوذ في البيانات التي يمكن أن تشير إلى هجوم إلكتروني محتمل ، مما يتيح الكشف الاستباقي عن التهديدات.
يمكن للتعلم الآليّ، وهو متفرّع عن الذكاء الاصطناعي، تحليل كميات هائلة من البيانات، وتعلّم التنبؤ بالتهديدات واكتشافها قبل إلحاق الضرر بالأجهزة أو الأشخاص.

7- تحسين الاستجابة للحوادث

في حالة وقوع هجوم إلكتروني، فإن الاستجابة السريعة أمر بالغ الأهمية. يمكن أن يساعد الذكاء الاصطناعي في تقصير أوقات الاستجابة من خلال تحديد مصدر الاختراق ومداها بسرعة، مما يسمح للفِرَق بالتصرّف بسرعة وتخفيف الضّرر المحتمل.يتطور مجال الأمان الرقمي بسرعة شديدة بالتزامن مع اعتماد البشر أكثر وأكثر على الأدوات الرقمية، ممّا يزيد من مخاطر انتهاك خصوصيتها وبياناتهم، لذلك متابعة كل ما هو جديد سواء من جهة الأدوات والآليات التي تساعد علي حماية الخصوصية من جهة، او أخبار الاختراقات والجرائم الرقمية من جهة اخرى، من خلال الأخبار والأبحاث والنشرات المتخصصة، هو عمل شبه يومي تقريبا سواء بالنسبة لي أو لفريق العمل.

8- تقليل أعباء وتكاليف تكنولوجيا المعلومات

تساعد قدرات أتمتة التعلم الآلي على تقلي ل الوقت الذي يستغرقه توزيع التحديثات الأمنية واستكمال اختبارات الاختراق وأجهزة المراقبة، وهو ما يوفر الوقت لدى فرق تكنولوجيا المعلومات للتركيز على قضايا الأمان الأكثر إلحاحًا.

9- تسجيل مخاطر الشبكة

تُستخدم خوارزميات التعلم الآلي في تحليل مجموعات بيانات الهجمات الإلكترونية السابقة وتحديد مناطق الشبكات التي شاركت في هجمات معينة، وهو ما يمكّن من تحديد تأثير الهجوم فيما يتعلق بمنطقة شبكة معينة، وبالتالي تستطيع المنظمات تقليل فرص التعرض لهجمات أخرى.

تحديات الأمن السيبراني في عصر الذكاء الاصطناعي:

على الرغم من الفوائد المتعددة التي يحققها استخدام الذكاء الاصطناعي في مجال الأمن السيبراني؛ إلا أن هناك عدة تحديات ومخاطر تواجه هذا الاستخدام وهي: