العدد (24) سبتمبر 2023 عدد خاص

دور الذكاء الاصطناعي فى الأمن السيبرانى

إعداد

اد عادل عبد السميع احمد عوض

ملخص البحث

يتناول البحث استخدام تقنيات التعلم العميق في تحسين قدرات الأمن السيبراني، وذلك من خلال تحليل البيانات بشكل فعال وتحديد الأنماط والتهديدات بدقة وسرعة، وتطوير نماذج تنبؤية دقيقة لإدارة المخاطر. ومع ذلك، فإن استخدام التعلم العميق يواجه تحديات مثل الحاجة إلى كميات كبيرة من البيانات عالية الجودة والتحديات المتعلقة بالتفسير والشفافية للنماذج المعقدة. يجب على الممارسين في مجال الأمن السيبراني مراقبة التطورات الحديثة وتحديد التحديات المحتملة وتطوير استراتيجيات فعالة لحماية الشبكات والأنظمة من الهجمات الإلكترونية.

يمكن استخدام التعلم العميق في العديد من مجالات الأمن السيبراني، مثل تحليل سجلات الشبكة والتعرف على الهجمات المستهدفة وتصنيفها وتنبؤ بالهجمات المستقبلية. كما يمكن استخدام التعلم العميق لتحليل البرامج الضارة والكشف عنها وإزالتها من الأنظمة.

مع ذلك، فإن استخدام التعلم العميق يتطلب مهارات تقنية عالية وخبرة في مجال الأمن السيبراني. يجب على المؤسسات التي ترغب في استخدام التعلم العميق في أمن السيبراني أن تستثمر في تدريب موظفيها على هذه التقنية وتوفير الموارد اللازمة لتحليل البيانات بشكل فعال.

بصفة عامة، فإن استخدام التعلم العميق في أمن السيبراني يعد تطورًا مهمًا في مجال الأمن السيبراني، حيث يمكن استخدامه لتحسين تحليل البيانات وتحديد الأنماط والتهديدات بدقة وسرعة وتطوير نماذج تنبؤية دقيقة لإدارة المخاطر.

في النهاية، يجب على المؤسسات المهتمة بتحسين أمنها السيبراني أن تستكشف إمكانية استخدام التعلم العميق في عملياتها، وتحديد المجالات التي يمكن استخدامها فيها بشكل فعال، وتوفير الموارد اللازمة لتطبيقها بشكل صحيح وفعال.

تمهيد

لأن الجرائم بصفة عامة والجرائم الالكترونية بصفة خاصة لها خطورة على أمن واستقرار البشر، بل وتهدد كل مناحى الحياة الإجتماعية، ونظراً لأن القراصنة أكثر انتشاراً من أى وقت مضى، أصبحت هذه الجرائم تمثل تهديداً مستمراً للتقدم فى مجال تكنولوجيا المعلومات.

إن الحماية الالكترونية تتطلب تقنيات الذكاء الاصطناعى جديدة وفاعله، ومن المسلم به أن الأمن السبيرانى يحركه الذكاء الاصطناعى والذى بدوره يؤدى دوراً مهماً فى إدارة الأمن السبيرانى، وستعمل تقنية الذكاء الاصطناعى على تحسين أدوات الأمن السبيرانى.

مساعدة الذكاء الاصطناعى المؤسسات فى مواجهة التهديدات الالكترونية

يساعد مخطط الذكاء الاصطناعي في سوق الأمن السيبراني المؤسسات في مراعاة التهديدات الإلكترونية واكتشافها والإبلاغ عنها ومواجهتها للحفاظ على سرية المعلومات. طالب الوعي المتزايد بين الناس، والتقدم في تكنولوجيا المعلومات، ورفع درجات حلول عمل الاستخبارات والشرطة، وزيادة حجم المعرفة التي تم جمعها من عديد من المصادر، باستخدام حلول موثوقة ومحسنة للأمن السيبراني. تؤدي الزيادة في حدوث الهجمات الإلكترونية وجودتها إلى دفع الأنظمة الإلكترونية التي تدعم الذكاء الاصطناعي. أدت الحوادث المتزايدة للهجمات الإلكترونية الضخمة على مستوى العالم إلى خلق الوعي بين المنظمات لتأمين معلوماتها. الدافع وراء هؤلاء المجرمين السيبرانيين هو المنافسة السياسية، ويتحرك المنافسون لتحقيق مكاسب ويؤذون اسم الآخرين، وسرقة المعلومات الدولية. معظم الهجمات الإلكترونية لتحقيق مكاسب[1].

تحمل الجرائم على وجه العموم في طياتها درجة عالية من الخطورة الموجهة ضد أمن و استقرار المجتمعات البشرية فهى تمثل تهديدا لمختلف نواحى الحياة الاجتماعية كما تسهم في خلخلة الروابط الإنسانية القائمة فى كافة المجتمعات، بالإضافة إلى ما تمثله

من تهديد للحقوق الأساسية للإنسان، ولاسيما حقه فى الحياة والتملك وسلامة البدن والشرف والاعتبار، أو هي بوجه عام خروج على القيم والتقاليد والأعراف والمثل التي يقوم عليها مجتمع ما من المجتمعات مهدداً المصالح العامة [2].

يعمل مجرمو الإنترنت بجد مضاعف للحفاظ على ميزة مقابل التدابير الأمنية التي تنفذها الشركات والوكالات الحكومية (بعد كل شيء عملهم هو القيام بذلك. لكن ليست كل الجرائم الإلكترونية تحدث من الخارج. شكلت الهندسة الاجتماعية ٢١ من الأساليب المستخدمة لارتكاب الجرائم الإلكترونية. يمكن أن يكون للجرائم الإلكترونية تأثير ضار على المؤسسة، مما قد يضر بسمعة الشركة وكذلك فقدان العملاء المخلصين يمكن أن يؤدي إلى خسارة في الإيرادات وفقدان بيانات السرية والملاءمة بالإضافة إلى اضطراب النظام الحرج[3].

يتميز الأمن السيبراني بأنه مجموعة من العمليات التي تساعد في حماية البيانات الإلكترونية والنشاط البشري والأنظمة. على غرار قاعدة مور التي تتنبأ بمضاعفة المكونات كل عامين على دائرة متكاملة (إلى جانب انخفاض التكاليف المرتبطة بتطوير الرقائق)، يضاعف مجرمو الإنترنت فعالية هجماتهم المستهدفة بنصف التكلفة كل عدة أشهر. من المقدر أن يتجاوز الإنفاق العالمي على الأمن السيبراني تريليون دولار من 2016 إلى 2021. ارتفع الإنفاق على الأمن السيبراني من 2013 إلى 66 دولارًا هو تطوير أنظمة كمبيوتر معقدة بمساعدة العقلية الذكاء الاصطناعي بالفعل بأكثر من 40 بالمائة. الذكاء الاصطناعي أو البشرية والتي تكون قادرة على أداء وظيفتها مثل الإنسان العادي، على سبيل المثال، يمكنها التعرف على الصوت ومعالجته بلغات مختلفة كإنسان. الذكاء الاصطناعي هو النظام العلمي

الشامل ذو الفروع المختلفة في الرياضيات وعلوم الكمبيوتر والفلسفة التي تهدف إلى تطوير نظام ذكي آخر يُظهر خصائص الذكاء عادةً، وهي كلمة الذكاء الاصطناعي التي تُستخدم في الغالب لوصف الآلية التي تحاكي وظائف «الإدراك»، والتي يرتبط بها البشر إلى عقولهم، أي حل المشكلات وحلها[4].

التعلم الآلي عامل أساسي في البحث والأعمال الحديثة. يتم استخدام الخوارزميات ونماذج محايدة للشبكة لإلزام أنظمة أجهزة الكمبيوتر بتحسين التطوير بنجاح. تقوم خوارزميات التعلم الآلي تلقائيًا ببناء نموذج رياضي باستخدام بيانات العينة التي تسمى بيانات التدريب لاتخاذ القرارات دون الترتيب على وجه التحديد. يعتمد التعلم الآلي على نموذج هو تفاعل خلية الدماغ. قدم دونالد هيب هذا النموذج في 1949[5].

صاغ آرثر صموئيلArthur Samuel مصطلح "التعلم الألي" في" مقالته عام ١٩٥٩، بعض الدراسات في التعلم الآلي ووفقاً له فإن التعلم الآلي هو "ما يمنح أجهزة الكمبيوتر القدرة على التعلم دون أن تتم برمجته بشكل صريح[6].

ما الذي تتطلبه الخوارزمية للعمل والمعالجة؟ بمعنى آخر ما كيفية تحليل الخوارزميات؟ تحليل الخوارزمية يعنى التنبؤ بالموارد التي تطلبها الخوارزمية، في بعض الأحيان تكون الموارد مثل الذاكرة، أو عرض النطاق الترددي، أو أجهزة الكمبيوتر ومعداتها البرمجية، وفي بعض الأحيان يكون في الوقت الحسابي الذي تريد قياسه بشكل عام خلال تحليل عدة خوارزميات مرشحة لمشكلة ما، يمكننا تحديد أكثرها كفاءة، قبل أن نتمكن من تحليل خوارزمية يجب أن يكون لدينا نموذج لتقنية التنفيذ التي سوف تستخدمها بما في ذلك نموذج لموارد تلك التكنولوجيا وتكاليفها [7].

هل يجب أن تكون أجهزة الكمبيوتر خوارزمية؟ كل ما يحدث على الحاسوب يحدث بفصل خوارزمية ما، والخوارزمية في سلسلة محددة من التعليمات ينفذها الحاسوب، انشغلت ألمع العقول خلال الفترة الماضية في تصميم الخوارزميات، ولكن هناك مشكلات

معقدة لدرجة لا يمكن وصفها. ببساطة، وتصميم خوارزمية لحلها مثل تحليل الكلام Speech analysis، والتعرف على الوجوه وظهرت أنواع جديدة من الخوارزميات تدعى بخوارزميات تعلم الآلة. أحدثت خوارزميات تعلم الآلة ثورة هائلة في مجال الحوسبة، وفتحت مجال التطبيقات مثل الرؤية الحاسوبية Computer Vision ، والترجمة الآلية Automatic translation ، وما إلى ذلك. أثبتت الشبكات العصبونية قدرتها على تعلم الأنماط المعقدة بشكل مدهش مثل توليد الأصوات، والوجوه البشرية لوضع ملاحظات على الصورة وحتى اكتشاف الكواكب[8] .

التعلم تحت الإشراف

هذا النوع من التعلم مسؤول عن نمط لتنفيذ خوارزمية التعلم الآلي. نظرًا لأن التعلم الخاضع للإشراف هو أسهل طريقة لفهم الحلول، فقد تم استخدامه على مر السنين في العمل بعديد من الأدوات. من السهل نسبيًا فهم ذلك، مثل تعليم الطفل باستخدام البطاقات الرياضية.

عندما يستخدم شخص نظام بريد إلكتروني جديد، سيكون هناك احتمال أكبر أن يكون لديك بعض مرشحات البريد العشوائي. مرشحات البريد العشوائي هذه هي نظام تعلم خاضع للإشراف. بعد تلقي رسائل البريد الإلكتروني والملصقات، علمت هذه الأنظمة كيفية القضاء على الرسائل غير المرغوب فيها، يمكن لرسائل البريد العشوائي هذه تتبع المستخدم خلال منحهم علامات مبتكرة[9].

يعد التعلم الإشرافي نوعًا من التعلم الآلي حيث تتعلم خوارزمية تعيد تمثيل البيانات الداخلية إلى مخرجات مرغوبة مستندة إلى أمثلة مصنّفة. في التعلم الإشرافي، تتم تدريب الخوارزمية على مجموعة بيانات تشتمل على البيانات الداخلية وقيم المخرجات المقابلة لها. الهدف من الخوارزمية هو تعلم دالة تمثيل تستطيع التنبؤ بشكل دقيق بقيم المخرجات للبيانات الجديدة الداخلة. يتم ذلك عن طريق تقليل وظيفة الخسارة التي تقيس الفرق بين القيم المخرجة المتوقعة والقيم المخرجة الحقيقية. يستخدم التعلم الإشرافي في مجموعة متنوعة من التطبيقات، بما في ذلك تصنيف الصور والتعرف على الكلام ومعالجة اللغة الطبيعية وعديد من التطبيقات الأخرى."[10]

التعلم غير الخاضع للإشراف

هذا النوع من التعلم متناقض مع التعلم الخاضع للإشراف. في هذا لا توجد ملصقات. كبديل لهذه الخوارزمية، فإنها تتطلب قدرًا كبيرًا من البيانات جنبًا إلى جنب مع الأدوات المؤكدة لفهم البيانات وخصائصها. يقوم التعلم غير الخاضع للإشراف بتحديد البيانات باستخدام التعرف على الأنماط وفرز البيانات.

التعلم المعزز

هذا النوع من التعلم مميز تمامًا عن التعلم الخاضع للإشراف ويختلف أيضًا عن التعلم غير الخاضع للإشراف. وبهذه الطريقة، يمكن للمؤلفين تحليل أو رؤية العلاقة بين وجود وغياب الملصقات تستخدم

المحاكاة الصناعية لعدة أنواع من التطبيقات الروبوتية ؛ يمكنها إنهاء المهام دون امتلاك رمز صلب لعملياتها[11].

التعلم العميق هى تقنية من التعلم الآلي ML تمكن الخوارزميات من استخدام التعلم التلقائي للميزات التي توضح أن الخوارزميات تستخدم لدراسة المزيد من التعليم خلال الجمع بين ميزات مختلفة لبيانات الإدخال في مجموعة مجردة من الميزات. هناك أربعة أنواع من خوارزميات التعلم الآلي: تحت الإشراف وشبه إشراف ودون إشراف وتعزيز. يسمح هذا للنظام بعمل تنبؤات معقدة عند معالجتها بمجموعات البيانات الضخمة. في السنوات الماضية، الزيادة السريعة في الأمن السيبراني، استخدم العلماء هذه الخوارزميات في أنظمة التعلم الآلي[12].

اثنان من أكثر طرق الحساب شيوعًا بناءً على مبدأ بقاء لياقة خوارزمية MI للأمن السيبراني – GA و GP. تعمل هذه الخوارزميات على مجموعة الكروموسومات التي تتطور بناءً على مشغلين معينين. المشغل الثلاثي الأساسي المستخدم هو الاختيار والتقاطع والطفرة. تبدأ الخوارزمية بعدد من السكان تم إنشاؤه بشكل عشوائي ؛ يتم حساب قيمة اللياقة البدنية لكل فرد. هذا يدل على قدرة كل فرد على حل المشكلة الحالية والأفراد الذين لديهم احتمال أكبر لديهم فرصة أكبر للاختيار في تجمع التزاوج. سيقوم شخصان قادران بتنفيذ الخطوة التالية المسماة بالتقاطع crossover وأخيرا سيخضع كل منهما للطفرة. من بين الشخصين المتحورين، سيتم حشد الكروموسوم الأعلى ملاءمة للجيل القادم[13].

الهدف الرئيس من هذا التقييم القائم على الخوارزمية هو اختبار قابلية تطبيق بعض خوارزميات التعلم الآلي للكشف عن الهجمات الإلكترونية على بيانات MODBUS. تم استخدام التحقق Tenfold لتطوير نماذج التعلم الآلي. في التحقق المتبادل، يمكن للمؤلفين إنتاج 10 نماذج مختلفة لمجموعة البيانات المقدمة. ثم يتم حساب المتوسط المرجح لهذه النماذج والتي تظهر كنتيجة نهائية. تم تصنيف مجموعة البيانات المستخدمة على بيانات القياس عن بعد من خط أنابيب الغاز الذي طوره مركز حماية البنية التحتية الحيوية[14].

يعد التعلم التعزيزي نوعًا من التعلم الآلي حيث يتعلم العامل (agent) التفاعل مع بيئة ما لتحقيق أقصى إشارة مكافأة (reward signal). يقوم العامل باتخاذ إجراءات داخل البيئة، وتستجيب البيئة بإشارة مكافأة إيجابية أو سلبية. يهدف العامل إلى تعلم سياسة تمثل الحالات إلى الإجراءات بطريقة تزيد من المكافأة التراكمية المتوقعة مع مرور الوقت. تم تطبيق التعلم التعزيزي بنجاح على مجموعة واسعة من المشكلات، بما في ذلك الألعاب، والروبوتات، وأنظمة التحكم. ومع ذلك، لا يزال هذا المجال صعبًا في البحث بسبب صعوبة تصميم وظائف المكافأة والتعامل مع التوازن بين الاستكشاف والاستغلال"[15].

. أنظمة التعلم الآلي القائمة على الحوسبة السحابية للأمن السيبراني

تم دراسة درس انتقال أنظمة التحكم الصناعي ICS من الأنظمة المستقلة إلى البيئات القائمة على السحابة. ثم ناقش الباحثون الأعمال الرئيسة من الصناعة والأوساط الأكاديمية إلى إنشاء ICSs آمنة، لا سيما إمكانية تطبيق تقنيات التعلم الآلي للأمن السيبرانيICS. يمكن أن يساعد العمل في مواجهة

تحديات تأمين العمليات الصناعية، خاصة عندما يتم نقلها إلى السحابة. وبالتالي فإن مجرمي الإنترنت يبتكرون تقنيات متقدمة لاستغلال الأجهزة والشبكات الفردية ونقاط ضعف الحالات[16].

إن الإجرام المعلوماتي هو ذلك الإجرام الذى يتم عن طريق الحاسوب والإنترنت، كذلك هو إجرام الأذكياء بالمقارنة بالإجرام التقليدى، والذى يميل فيه المجرم إلى العنف، ولذلك فالصورة التي نحن بصددها يطلق عليها الإتلاف المعلوماتى الناتج عن تقنيات تدمير ناعم وتمثل جرائم الإنترنتمجموعة الأفعال غير القانونية التى تتم عن طريق الإنترنت أو تبث عبر محتوياته فهو يمثل أحدكم تكنولوجيا العصر التي تم استخدامها في مختلف جوانب الحياة[17].

أحد المشكلات مع مجرمي الحاسوب هي أنهم لا يعاقبون العقاب الكافي، حيث أن المختلسين للملايين من الدولارات قد يحصلوا على عقوبات وأحكام خفيفة، ومن ارتكبوا اختراقات خطيرة لأنظمة الحاسب يدفعون غرامة ويأخذوا فترة خدمة تحت الرقابة أو عمل خدمة عامة للمجتمع. وهناك ميول للشركات لتعيين مجرمي الحاسوب الناجحين لمساعدتهم في الحماية ضد الهجمات والاختراقات[18].

تقوم المؤسسات بجمع بيانات أمنية رفيعة المستوى سنويًا لاختبارات الطب الشرعي المحتملة، مثل حوادث السجل البشري والشبكات وتطبيقات البرمجيات. لا توجد تجربة عمل جيدة مع مقاييس البيانات الكبيرة وأجهزة الإنذار المزيفة العالية، لا سيما عندما يتم نقل الشركات إلى بنية السحابة وجمع المزيد من

المعلومات. بالإضافة إلى ذلك، من الضروري تتبع وتحليل البيانات الأمنية الضخمة بدقة وسرعة لتحديد الهجمات الأكثر حداثة وفخامة، مثل التهديدات المستمرة المتقدمة (APTs). تم استخدام معالجة البيانات الضخمة بنشاط في عدد من المجالات، مثل المعاملات المالية والرعاية الصحية والتطبيقات الصناعية. لفت الجمهور الانتباه مؤخرًا بسبب قدرته الموعودة على مقارنة بيانات السلامة ورسم رؤى فعالة على نطاق لا مثيل له. تحلل هذه الوثيقة التكنولوجيات/النظم التقليدية وأدوات المعلومات الأمنية و إدارة الأحداث SIEM للتعامل مع نطاقات البيانات الضخمة والتهديدات المتطورة وتوضح نقاط ضعفها. ثم يستكشف المتهمون معايير تحليلات البيانات عالية المستوى والتهديدات المتطورة في استخبارات التهديدات الإلكترونية والأمن السيبراني. أخيرًا، يوضح المهتمون تحديات هذا التبني ويقدمون بعض الأفكار للبحوث المستقبلية لمواجهة تحديات التبني. إن التطبيقات القائمة على السحابة قد وسّعت بشكل كبير نماذج الأعمال متعددة القيمة. القطاع المالي هو المستفيد الرئيس، مثل البيانات الضخمة والحوسبة السحابية، من التكنولوجيا الجديدة الناشئة. ساهم هذا النمط المتغير أيضًا في إثارة مخاوف كبيرة بشأن الأمن السيبراني[19].

يعد تأمين الأمن السيبراني مجالًا متناميًا في الصناعة المالية في هذا السياق. ومع ذلك، فإن تأمين الحماية السيبرانية لديه أيضًا بعض المشكلات الإلكترونية باستخدام الأساليب القائمة على الويب. نناقش هنا المقال مجموعة متنوعة من المواد اللازمة لفهم تصنيف مخاطر الأمن السيبراني بعمق باستخدام تقنيات التعلم الآلي. الهدف هو تجنب المخاطر القصوى وتطوير حلول المخاطر المحتملة.يتم إنشاء التغيير الاجتماعي الحالي بواسطة إنترنت الأشياء والحوسبة السحابية والهواتف الذكية والشبكات الاجتماعية. ومع ذلك، يؤدي هذا التحول التكنولوجي إلى تهديدات جديدة وهجمات أمنية تخلق

سيناريوهات جديدة ومعقدة للأمن السيبراني مع كميات كبيرة من البيانات وناقلات الهجوم التي تتغلب على القدرات المعرفية للمحللين الأمنيين. وبهذا المعنى، سيدعم العلم المعرفي العمليات المعرفية لزيادة وقت وفعالية محللي الأمن في تنفيذ عمليات الأمن السيبراني. توفر هذه الدراسة عملية معرفية شاملة للتعلم الآلي وصنع القرار تدعم النظام لمحللي الأمن الذين يقدمون المعلومات والفهم وإجراءات الاستجابة الأمنية. يقدم هذا النموذج الحقائق. المعلومات. يستكشف النموذج بدائل الأتمتة لتنفيذ المهام المعرفية الموجودة في العمليات الإلكترونية. ويشمل المحلل، باستخدام MAPE-K و OODA و Human Loops، كتركيز رئيس له في مرحلة التحقق واتخاذ القرار[20].

يجد الذكاء الاصطناعي تطبيقات واسعة النطاق لعملية طباعة ثلاثية الأبعاد ذكية وموثوقة وعالية الجودة ومخصصة للخدمة. يمكن التعلم قبل أن تبدأ مهمة الطباعة خلال مدقق القابلية للطباعة لتقييم قابلية طباعة العناصر ثلاثية الأبعاد المقدمة. تعمل خوارزميات التقطيع المتوازية على تسريع التصنيع المسبق للشرائح، وتحسين تخطيط المسار بذكاء. توفر خوارزميات مطابقة الطلب الذكي وخوارزميات الموارد للخدمة والأمن للعملاء خدمات عند الطلب والوصول إلى مجموعة من الموارد المشتركة خلال منصة الخدمة السحابية ونموذج التقييم. لدى المؤلفين أيضًا ثلاث خوارزميات للتعلم الآلي في حالة الهجمات الإلكترونية لتحديد عيوب المنتج. يوفر تحليل التطبيقات المختلفة فرصًا جيدة لمزيد من الدراسة، خاصة خلال فترة الثورة الصناعية الرابعة، لطباعة مؤشرات متعددة، وتقليل حدود التعقيد،

وتسارع التصنيع المسبق، والضوابط على الوقت الفعلي، وتعزيز السلامة واكتشاف العيوب للتصميمات الفردية[21].

يعتمد الذكاء الاصطناعي على علم الخوارزميات في أتمته (ميكنة) المهام عن طريق الوصول إلى البيانات ذات الصلة، كما تعتمد الخوارزميات على الشبكات العصبية التي تم تصميمها خلال عمل الخلايا العصبية في الدماغ، بحيث تكون قادرة على التعلم تماما مثل البشر[22].

تم العمل على التطور التكنولوجي في المستقبل. سيتم تحويل القطاع المالي خلال الذكاء الاصطناعي الذي يسمح بتحسين الخدمات وتخصيصها، وخفض التكاليف وتطوير نماذج أعمال جديدة. أصدر الذكاء الإصطناعي مؤخرًا خرائط طريق لمزيد من تطوير الذكاء الاصطناعي في ألمانيا وهيسن، من قبل كل من الحكومة الفيدرالية وحكومة هيسن. على مدى السنوات 5 المقبلة، سيستثمر الاتحاد 3 مليار يورو في مجموعة من المجالات العلمية والصناعية بينما ستنشئ ولاية هيسن مركزًا جديدًا للذكاء الاصطناعي، والذي سينفق تريليون يورو على نمو الرقمنة على مدى السنوات 5 المقبلة. تواصل مراكز الذكاء الاصطناعيتقديم حلول عامة دقيقة للغاية. وينصب التركيز على تحسين استخدام نتائج البحوث في أنشطة الشركات، وتوسيع الشبكات والنظم الإيكولوجية، وتطوير المراكز القائمة. ستستفيد هذه البرامج بشكل خاص في المنطقة الرئيسة في راينلاند فرانكفورت، والتي تعد بالفعل مركزًا قويًا لشركة Fintech و Cyber Safety و AI. بالإضافة إلى الجامعة الأوروبية والبنية التحتية للكمبيوتر التي لا مثيل لها، يتمتع مركز فرانكفورت المالي بتكنولوجيا نابضة بالحياة ومتزايدة بسرعة ومجتمع مستعد: أكبر مركز للبيانات والخدمات السحابية في أوروبا، والأكبر في العالم والجامعات والمؤسسات البحثية الأجنبية مع

جودة أبحاث الذكاء الاصطناعي ومتخصصي الذكاء الاصطناعي والاستشارات بالإضافة إلى المجالات المحيطة. يهدف الذكاء الاصطناعي إلى إنتاج سلع مخصصة للغاية بجودة أعلى وتكاليف أقل خلال الاندماج في مصانع الإنتاج للإنترنت الصناعي وتحليل البيانات الضخمة والحوسبة السحابية والروبوتات المتقدمة. أصبحت أنظمة الإنتاج الرقمي أكثر انفتاحًا من أي وقت مضى، حيث يتم تعديل آلات التصنيع بشكل متزايد بأجهزة استشعار وترتبط عبر الشبكات اللاسلكية أو Ethernet السلكية. على الرغم من أن التقدم في الاستشعار والذكاء الاصطناعي والتكنولوجيا اللاسلكية يجعل من الممكن حدوث تحول نموذجي في الإنتاج، فإن الهجمات الإلكترونية تشكل تهديدات كبيرة للتصنيع. ندرس هنا الحماية السيبرانية في أنظمة التصنيع الرقمية، وتحديد جوانب توصيف الأجهزة والخطر والضعف ورصدها وتحديد المخاطر وتحديد التحديات والعمل المحتمل[23].

إن التصنيع الذكي خلال دمج الشبكة الصناعية للأشياء وتحليلات البيانات الضخمة والحوسبة السحابية والروبوتات المتقدمة في أرضيات المصانع. مع المزيد والمزيد من معدات وأجهزة التصنيع المجهزة بأجهزة استشعار، بالإضافة إلى الشبكات اللاسلكية واتصالات Ethernet السلكية، أصبحت أنظمة التصنيع الذكية أكثر سهولة من أي وقت مضى عبر الإنترنت. في حين أن التقدم في الاستشعار والذكاء الاصطناعي والتكنولوجيا اللاسلكية يسمح بتحول في نموذج التصنيع، فإن الهجمات الإلكترونية تشكل تهديدًا كبيرًا لقطاع الإنتاج. نهدف هنا إلى مراجعة ومناقشة أحدث التقنيات التي يمكن أن تعالج قضايا الأمن السيبراني في الإنتاج الذكي. ويرد على وجه الخصوص تقييم لأوجه الضعف والهجمات

الحاسوبية (مثل هجوم الوسيط والحرمان من الخدمة). هناك أيضًا استراتيجيات قائمة للتخفيف من الاختراقات الإلكترونية المستهدفة. بالإضافةإلى ذلك، تم تحديد الثغرات والتحديات البحثية في الصناعات التحويلية الحيوية لتحسين الأمن السيبراني. إن ثورة الصناعة أحدثتها زيادة التكنولوجيا واستخدام الإنترنت. يعد إنترنت الأشياء وأجهزة الكمبيوتر الذكية والأشياء الذكية والمعرفة والبيانات تطورًا تكنولوجيًا في عديد من الأنظمة. تكمن بعض المشاكل في العناصر الرئيسة للثورة الصناعية الرابعة مثل الأنظمة الفيزيائية الإلكترونية وإنترنت الأشياء والبيانات الضخمة والحوسبة السحابية. الأول هو الأمن السيبراني. نتاولهنا الإطار التكنولوجي للثورة الصناعية الرابعة وتحليلات متطلبات الأمن السيبراني لتلك التقنيات. من المقرر استخدام هذه الابتكارات بأمان في الثورة الصناعية الرابعة مع هذه الإرشادات. ثم، تم تناول الاحتياطات اللازمة لمكافحة الهجمات والتهديدات الإلكترونية فيما يتعلق بتطوير التكنولوجيا واستخدام النظم الأمنية[24].

أظهرت أنظمة التعلم الآلي المعتمدة على الحوسبة السحابية إمكانات كبيرة في مجال الأمن السيبراني. إن القدرة على معالجة كميات كبيرة من البيانات بسرعة وكفاءة هي فائدة رئيسة للحوسبة السحابية، مما يجعلها منصة مثالية لأنظمة الأمن السيبراني التي تعتمد على التعلم الآلي. يمكن لهذه الأنظمة تحليل كميات ضخمة من البيانات من مصادر مختلفة للكشف عن التهديدات المحتملة وتوفير الحماية في الوقت الحقيقي ضد الهجمات السيبرانية. يمكن أيضًا لأنظمة التعلم الآلي المعتمدة على الحوسبة السحابية التكيف والتعلم من البيانات الجديدة، مما يحسن دقتها مع مرور الوقت. ومع ذلك، هناك تحديات في تنفيذ هذه الأنظمة، مثل ضمان خصوصية وأمان البيانات، واختيار الخوارزميات

المناسبة للمهام السيبرانية المحددة. على الرغم من هذه التحديات، فمن المتوقع أن يستمر استخدام أنظمة التعلم الآلي المعتمدة على الحوسبة السحابية في مجال الأمن السيبراني في السنوات القادمة"[25].

. تقييم المخاطر التنظيمية للأمن السيبراني باستخدام الذكاء الاصطناعي

يوفر الأمن السيبراني الحماية من سرقة البيانات، ويحمى أجهزة الكمبيوتر من السرقة، ويقلل من تجميد الكمبيوتر ، ويوفر الخصوصية للمستخدمين ويقدم تنظيما صارمًا. قد يكون من الصعب تكوين جدران الحماية بشكل صحيح. قد تمنع جدران الحماية المكونة بشكل خاطئ المستخدمين من أداء أي سلوك على الإنترنت قبل تثبيت جدار الحماية بشكل صحيح، وستستمر في ترقية أحدث العاديين، تحاكي القرصنة الأخلاقية هجوماً خبيثاً دون محاولة إحداث ضرر. إذا كنت بحاجة إلى فهم البرامج للاحتفاظ بالحماية الحالية. يمكن أن تكون الحماية الإلكترونية باهظة الثمن للمستخدمين الإجراءات المضادة، فأنت بحاجة أولاً إلى فهم مراحل الهجوم من الضروري فهم خطوات مواجهة الهجوم بمجرد اكتشافه ووقف الهجوم قبل وصوله إلى المرحلة التالية بشكل عام[26].

إن الذكاء الإصطناعي يجب أن يشجع على إنشاء عمليات وممارسات تنظيمية مناسبة ثقافيًا لتقليل الموارد الطبيعية وموارد كثافة الطاقة للأنشطة البشرية من أجل تسهيل العلوم الإبداعية وحلول الاستدامة البيئية العملية للذكاء الاصطناعي. قد لا تتمثل المزايا الرئيسة للذكاء الاصطناعي في كيفية السماح للمجتمع بتقليل كثافة الكهرباء والمياه واستخدام الأراضي، ولكن كيف يسهل ويشجع مستويات أعلى من

الإدارة البيئية. أظهرت مراجعة شاملة للدراسات علي (1) الاعتماد المفرط على البيانات التاريخية في نماذج التعلم الآلي، (2) الاستجابات السلوكية البشرية غير المتوقعة للتدخلات الموجهة نحو الذكاء الاصطناعي، (3) زيادة المخاطر السيبرانية، (4) التنفيذ الضار للذكاء الاصطناعي و (5) الصعوبات في قياس تأثيرات سياسات التدخل المهددة بسبب أبحاث الذكاء الاصطناعي المستدامة. إن دراسات الذكاء الاصطناعي المستدامة المستقبلية يجب أن تتضمن (1) وجهات نظر متعددة المستويات، (2) مناهج النظام الديناميكية، (3) التفكير التصميمي، (4) اعتبارات الفوائد الاقتصادية من أجل إظهار كيف يمكن للذكاء الاصطناعي تقديم حلول فورية دون إدخال مخاطر طويلة الأجل على البيئة المستدامة[27].

إن الطائفة الواسعة من الآثار على الحكومات والمقاطعات والشركات والأشخاص من الذكاء الاصطناعي، وبحثت النتائج الإيجابية والسلبية على السواء. نشير أيضاً إلى الأثر العام الذكاء الإصطناعي من البحث والتطوير قبل التنفيذ. إن النجاحات الأكاديمية الرئيسة والتقدم الذي أحرزه الذكاء الإصطناعي وتأثيره على ممارسات الأعمال وبالتالي على السوق العالمية. وتبحث هذه المادة أيضا العوامل المسؤولة عن تطوير الذكاء الاصطناعي. من أجل تحليل أنشطة تنظيم المشاريع مقابل الذكاء الاصطناعي، كانت هناك قائمتان لأفضل 100 شركة ناشئة في مجال الذكاء الاصطناعي. ستعمل نتائج الأبحاث على تحسين الفهم التكنولوجي وتأثير الذكاء الاصطناعي على الشركات والمجتمع ككل. كما ستكتسب مزيدًا من المعرفة بكيفية تغير الأعمال والاقتصاد العالمي من الذكاء الاصطناعي[28].

إن بحثًا ببليومتريًا حول البيانات الكبيرة وتكنولوجيات الذكاء الاصطناعي قد تم فحصه من أجل 279 دراسة في الصناعة الملاحية أجراها 842 باحثًا في 214 منفذًا جامعيًا. تم الحصول على

المعلومات الببليوغرافية من شبكة العلوم من قبل الباحثين وتم تحليلها عبر برنامج R Bibliometric process. كشف الباحثون عن والمجلات والكتّاب والمنظمات الأكثر تأثيرًا على أساس الاقتباسات. مع طريقة الاقتران الببليوغرافية، طور المتهمون أربع مجموعات بحثية. (2) تطبيقات البيانات الضخمة للذكاء الاصطناعي، و (3) فعالية الطاقة، و (4) التحليل التنبؤي. (2) التحول الرقمي في الصناعة البحرية. وجرى تحليل هذه المجموعات تحليلا دقيقا ونوقشت المسائل المحتملة للدراسة[29]. بالإضافة إلى ذلك، يقدم الباحثون شراكات بحثية مؤسسية وشبكات المؤلفين.

إن التحول الرقمي المستمر يتطلب استثمارات وابتكارات كبيرة من أجل ضمان سلامة الإنترنت، ومجموعة متنوعة من البنى التحتية الحيوية والخدمات الأساسية التي تعتمد أكثر فأكثر على البنية التحتية الرقمية، وكذلك لزيادة المرونة في الاستخدام الضارللفضاءالسيبراني من قبل المنظمات والمجتمعات والقطاعات والدول والتحالفات. باع طويل يغطي تبادل المعلومات الإلكترونية والوعي بالأوضاع، ومزايا وتحديات التكنولوجيات الناشئة مثل الذكاء الاصطناعي، والعامل البشري، والتثقيف والتدريب في مجال الأمن السيبراني، والمرونة السيبرانية، وستشجع الحاجة إلى تضمين جهود السلامة الإلكترونية في البحث عن سلسلة مؤتمرات DIGILIENCE على تبادل المعلومات والخبرات في إدارة تكنولوجيا المعلومات والأمن السيبراني والمرونة، وتسهيل نشر الممارسات الجيدة[30].

تعد التقييمات الخاصة بتحديد المخاطر المؤسسية عنصرًا حيويًا في إدارة الأمن السيبراني. لدى استخدام الذكاء الاصطناعي للتقييم المخاطر، يتم تحسين دقة وكفاءة هذه العملية. يمكن لأنظمة التقييم المبنية على الذكاء الاصطناعي تحليل كميات كبيرة من البيانات من مصادر مختلفة، بما في ذلك سجلات الشبكة، وتكوينات النظام، وسلوك المستخدم لتحديد الثغرات والتهديدات المحتملة. يمكن أيضًا لهذه الأنظمة أن تتعلم من البيانات الجديدة، مما يحسن دقتها مع مرور الوقت. ومع ذلك، هناك تحديات في تنفيذ أنظمة التقييم المبنية على الذكاء الاصطناعي، مثل ضمان خصوصية وأمان البيانات، واختيار الخوارزميات والنماذج المناسبة للسياق المؤسسي المحدد. بالإضافة إلى ذلك، هناك حاجة إلى الإشراف البشري وتفسير النتائج التي تقدمها هذه الأنظمة. على الرغم من هذه التحديات، من المتوقع أن يستمر استخدام أنظمة التقييم المبنية على الذكاء الاصطناعي للأمن السيبراني في الزيادة في المستقبل، حيث يسعى المؤسسات إلى تحسين موقفها في مجال الأمن السيبراني"[31].

تكنولوجيا Block Chain باستخدام الذكاء الاصطناعي

قامت تكنولوجيا Block Chain بالتحقيق في تطبيقات الأعمال الحالية والمستقبلية لمحاسبة معينة وأمن إلكتروني. بالنسبة لمشاكل الإنترنت والمحاسبة الحالية، يتقدم المهتمون بطلب استخدامات Block Chain. يقوم الباحثون بمراجعة الدراسات التي تتضمن موضوعات مثل البيانات واسعة النطاق في الحسابات، واستخدام سلسلة الأمن المالي والأمن السيبراني واستخدام تقنية دفتر الأستاذ في الحسابات المالية، وتتبع المخالفات المالية. من أجل فهم خطط الحكومة الأمريكية فيما يتعلق بالأمن السيبراني، ينظر الباحثون أيضًا في سياسة الأمن السيبراني لوزارة الأمن الداخلي في السنوات القادمة. أظهر

الباحثون أن Block Chain لها عواقب تدقيق مختلفة من شأنها أن تغير المهنة بشكل كبير. يعتقد الباحثون أيضًا أنه من الضروري التنفيذ الفعال لتكنولوجيا Block Chain في عدد من المجالات، مثل التدقيق والمحاسبة، والأمن السيبراني والمحاسبة[32].

تعد تقنية Block Chain والذكاء الاصطناعي من أكثر التقنيات الابتكارية والمختلفة في العصر الحديث. توفر تقنية Block Chain منصة للبيانات المؤمنة والموزعة للمشاركة والمعاملات في حين يمكن للذكاء الاصطناعي أن يحدث ثورة في عديد من الصناعات بتمكين الآلات من التعلم واتخاذ القرارات كالإنسان. يمكن أن يؤدي اجتماع تقنية Block Chain والذكاء الاصطناعي إلى تطبيقات أكثر قوة وتحويلية. فعلى سبيل المثال، يمكن استخدام تقنية Block Chain لإنشاء منصات آمنة وشفافة لمشاركة البيانات في تطبيقات الذكاء الاصطناعي، مما يتيح للمؤسسات مشاركة البيانات وفي الوقت نفسه الحفاظ على الخصوصية والأمان. يمكن أيضًا استخدام خوارزميات الذكاء الاصطناعي لتحليل بيانات Block Chain ، وتوفير رؤى والكشف عن الأنماط التي يصعب على الإنسان تحديدها. ومع ذلك، هناك تحديات في تنفيذ Block Chain والذكاء الاصطناعي معًا، مثل ضمان التوافق بين شبكات Block Chain المختلفة وأنظمة الذكاء الاصطناعي. على الرغم من هذه التحديات، فإن الفوائد المحتملة لدمج هاتين التقنيتين كبيرة، ومن المتوقع أن يؤديان دورًا رئيسًا في تشكيل مستقبل عديد من الصناعات"[33].

أنظمة الوقاية من الهجمات الإلكترونية القائمة على إنترنت الأشياء

إن الهجمات الإلكترونية التي تدعم إنترنت الأشياء والتي تم العثور عليها منذ عام 2010 في كل مجال تطبيق. تم التأكيد على أحدث هجمات IOTA والأحداث المشهورة عالميًا وإثبات الهجمات المفاهيمية الصادرة لكل قطاع. يقوم المتهمون بتحليل الهجمات التمثيلية بشكل منهجي ويظهرون المسارات التي يتم خلالها معالجة الأهداف الحرجة بشكل مباشر وغير مباشر.

إنترنت الأشياء (IOT) هي شبكة من الأجهزة المختلفة المتصلة بالإنترنت قادرة على جمع البيانات وتبادلها، وتنتج أجهزة IOT هذه قدرًا كبيرًا من المعلومات ليتم جمعها وتخزينها لاستخدامها في الذكاء الاصطناعي للتعامل مع تدفقات البيانات الهائلة والتخزين خلال شبكة IOT. تشكل الشبكة ذاتية التحسين والشبكة المحددة بالبرمجيات جزءً من بارامترات نظام إنترنت الأشياء الرئيسة[34].

أدى التحول النموذجي نحو إنترنت الأشياء (IoT) إلى خلق قدرة هائلة لمشاهد إنترنت الأشياء المستقبلية المختلفة مثل المنزل الذكي والنقل الذكي والصحة الذكية والطاقة الذكية والتقدم في مفهوم قياس الحافة. هناك أيضًا مجموعة من التهديدات الناشئة للأمن السيبراني. في هذا الاتجاه تحدث المتهمون عن التهديدات الجديدة الكبيرة للأمن السيبراني والفرص ذات الصلة في هذه الرؤية. والهدف من ذلك هو تحديد وتحليل المسائل التقنية ذات الصلة وعرض التطورات الأخيرة، وتحديد الحلول الممكنة واقتراح توجيهات جديدة للدراسة. أولاً، لدى المؤلفين مسح لميزات mMTC ومشاكل QoS مع عوامل تمكين رئيسية لـ mMTC في شبكات الهاتف المحمول. بالإضافة إلى النقاط البارزة حول عدم كفاءة الوصول العشوائي (RA) ضمن سيناريو MMTC، يقدم المتهمون الخصائص الرئيسة وآليات الوصول إلى القنوات لخلايا إنترنت الأشياء الناشئة، LTE-M و IoT الضعيف (NB-IoT). ثم يقدم المتهمون إطارًا

لتحليلات الأداء لجدولة الإرسال مع دعم QoS جنبًا إلى جنب مع المشاكل المتعلقة بإرسال الحزم القصيرة. بعد ذلك، يقدم المتهمون مراجعة شاملة للتقنيات الحالية والجديدة لحل مشاكل ازدحام RAN في الشبكة الخلوية ومعالجة المزايا والتهديدات وحالات الاستخدام المحتملة لتقنيات التعلم الآلي المتطورة (ML). ركز المتهمون على استخدام طريقة التعلم Q منخفضة التعقيد في سيناريو MMTC مع التطورات الأخيرة في تحسين أداء التعلم والتكامل من عديد من تقنيات ML. أخيرًا، يستكشف المتهمون حواجز العلوم المفتوحة واتجاهات البحث المستقبلية المثيرة[35].

إن نماذج التعلم العميق في شبكات إنترنت الأشياء للأمن السيبراني. شبكة إنترنت الأشياء هي تقنية واعدة تربط بين الحياة وعدم الحياة في جميع أنحاء العالم. يتزايد نشر إنترنت الأشياء بسرعة، لكن الأمن السيبراني هو انهيار، ومن المحتمل أن يكون هناك عديد من الهجمات الإلكترونية ونجاح الشبكة مستقر في الغالب، لذلك لن يكون الناس مستعدين لاستخدام هذه التكنولوجيا. في الماضي القريب، أثر هجوم DDoS (رفض الخدمة الموزع) على عدد كبير من شبكات إنترنت الأشياء، مما أدى إلى خسائر كبيرة. اقترح المتهمون واختبروا نماذج تعلم عميقة باستخدام قواعد بيانات DDoS للكشف عن هجوم CICIDS2017 الجديد والتي كانت دقيقة للغاية حيث تمت مقارنة 97.16٪ من النماذج المقترحة بالفعل بخوارزميات التعلم الآلي. تم تناول قضايا البحث المفتوحة لاستخدام خوارزمية التعلم العميق للأمن السيبراني لإنترنت الأشياء[36].

إنترنت الأشياء، الحوسبة في كل مكان – الإنترنت: المشاريع الجارية بالفعل لتجهيز الأشياء اليومية بأجهزة استشعار لاسلكية بسيطة) على سبيل المثال، علامات(RFID ، بالإضافة إلى مشاريع لتوفير الوصول إلى الإنترنت عالي السرعة على مستوى العالم، يجب أن تتوج بالوصول إلى الإنترنت في كل مكان، وكذلك «البيئات الذكية العالمية ستكون جميع بيناتاتنا قادرة على الاستجابة لاحتياجات الوكلاء الموجودين بالإضافة إلى تنظيم شبكات الطاقة والاتصالات والنقل بكفاءة[37].

تاريخ التطور الكيميائي الحيوي كتاريخ منظم بواسطة الظلمة متحركة . الحياة غير الحية إلى الحياة، والحياة وحيدة الخلية إلى الحياة متعددة الخلايا، وما إلى ذلك تميل هذه التحولات إلى الحدوث عندما تتمايز العوامل من أجل أن تصبح أكثر تخصصا في وظيفتها وتكاملية من أجل أن تصبح أكثر اعتماداً على بعضها البعض للعمل في المستقبل. عندما تتسارع عملينا التمايز والتكامل هذه نحو ظهور صفات تحكم جديدة [38].

لكي يتسنى لمنظومتنا (الحضارة الإنسانية) أن تحقق نظاما فارغا جديدا، ستكون هناك حاجة إلى زيادة هائلة في التعاون والتنسيق العالميين. هذا تفكر في هذا الاحتمال باستخدام المفاهيم التطورية السيبرنية للزوال والوصم. الإفريز هو مفهوم يصف عمليات الحد من الاحتكاك المادي والوصم هو مفهوم يصف عمليات الحد من الاحتكاك الاجتماعي سيسمح كل من التخفيضات في الاحتكاك المادي والاجتماعي بظهور عوامل أكثر تميزا وتكاملاً، تمتلك معرفة أعلى لتحقيق أهداف ذات مغزى بشكل متكرر في عالم سريع الزوال، ستكون هناك مستويات متزايدة من الوفرة انخفاض مستويات الندرة) لأن العمليات النفسية والاجتماعية التكنولوجية التي تتوسط فيها الانترنت ستتمكن بشكل متزايد من فعل المزيد

بأقل». في عالم الوصم ستكون هناك مستويات أعلى من السلام والتعاون لأن العمليات النفسية والاجتماعية التكنولوجية التي تتوسط فيها الإنترنت ستسمح بوسيط بعزر باستمرار التفاعلات التي تفيد الجميع[39].

يمكننا أن نتوقع أن تتبع تكنولوجيات المعلومات والاتصالات مسارات تطورية يمكن التنبؤ بها إلى حد ما تنتقل إلى المستقبل القريب بسبب فهمنا للتقدم الحسابي السابق في قوة المعالجة ما هى أنواع الميزات والأشكال التي قد تصبح متاحة للعمل العدواني عبر هذا النطاق الزمني ؟ هنا نصنف بعض السمات الموجية لهذا الدماغ العالمي الناشي:[40]

1- الويب الدلالي والشبكات العصبية والذكاء الاصطناعي وأنظمة التوصية: يجب أن تكون الخوارزميات المتقدمة بشكل متزايد قادرة على تجميع جميع المعارف البشرية (بما في ذلك البيانات الذاتية والمجزأة وغير (المحتملة والكشف عن الاتجاهات والارتباطات الأساسية وينبغي أن تكون هذه النظم قادرة على التكيف مع احتياجات فرادى المستعملين عن طريق التوصية بحلول محددة السياق، لذلك، يجب أن يتمكن جميع البشر من الوصول إلى حلول مرنة وقويةوربما دون الحاجة إلى طرح أي أسئلة علىالاطلاق.

2- الدورات المفتوحة على نطاق واسع عبر الإنترنت، والدورات المفتوحة عبر الإنترنت شخصيا يجب أن يكون الوصول إلى البرامج الأكثر تقدما لتدريس أي مادة أكاديمية مجانيا ويسهل

الوصول إليه لأي شخص في أي مكان في العالم من المحتمل أن تتضمن هذه البرامج بنية تشبه اللعبة» أكثر استرخاء. يجب أيضا أن تصبح مصممة بشكل فردي لكل مستخدم الضمان أقصى قدر من كفاءة التدريس (أيمعرفة ما يعرفه كل فرد بالضبط، وما يريد يحتاج كل فرد إلى معرفته) مع توفر مثل هذه البرامج لأي إنسان، بالإضافة إلى ضغوط الاختيار.

التركيز على دراسة حالة إفرادية لإطار العمليات الأمنية الذي يجمع بين طبقات معالجة البيانات التقليدية ومحرك قاعدة بيانات تحليلي حديث. يمكّن المحرك خبراء الأمان من الاستعلام عن مجموعات بيانات أحداث السجل الكبيرة بتنسيق علاقة نموذجي. نتائج الاستعلام أكبر من حلول قاعدة البيانات الحالية، والتي تعمل بموارد مماثلة، وهي أيضًا موثوقة بما يكفي لتحديد حالات الزاوية المشبوهة بشكل صحيح. يتم تشغيل المحرك الداخلي عن طريق قواعد البيانات وإجراءات العرض العام. وتشمل هذه المبادئ مبادئ تحديد كمية البيانات، والحسابات المقدرة، ومجموعات البيانات، وانتشار الاحتمالات. يحلل المتهمون تأثير البارامترات الحركية في البيئة المعينة على كفاءتها. بالإضافة إلى ذلك، يستكشف المتهمون بعض قرارات التصميم عالية المستوى مثل اختيار مقياس تقديري لدقة نتائج الاستعلام التي تعكس تفاصيل عمليات مراقبة المخاطر [41].

أصبح أنظمة الوقاية من الهجمات السيبرانية المستندة إلى إنترنت الأشياء (IoT) مهمة بشكل متزايد مع ارتفاع عدد أجهزة IoT بشكل سريع. تكون أجهزة IoT عرضة للهجمات السيبرانية بسبب قدراتها المحدودة في الحساب ونقص التدابير الأمنية. يمكن لأنظمة الوقاية من الهجمات السيبرانية المستندة إلى IoT مساعدة في الكشف عن الهجمات ومنعها خلال مراقبة أجهزة IoT وحركة المرور في شبكاتها في الوقت الحقيقي. يمكن لهذه الأنظمة استخدام خوارزميات التعلم الآلي لتحليل أنماط حركة المرور في

الشبكة والكشف عن الاختلافات التي قد تشير إلى وجود هجوم. يمكن أيضًا استخدام التحليل السلوكي لتحديد سلوك غير عادي للجهاز والكشف عن التهديدات المحتملة. ومع ذلك، هناك تحديات في تنفيذ أنظمة الوقاية من الهجمات السيبرانية المستندة إلى IoT، مثل ضمان التوافق مع أنواع مختلفة من أجهزة IoT والشبكات، ومعالجة القضايا المتعلقة بالخصوصية المتعلقة بمراقبة أجهزة IoT. على الرغم من هذه التحديات، فإن الحاجة إلى أنظمة الوقاية من الهجمات السيبرانية المستندة إلى IoT ستستمر في الزيادة مع ارتفاع عدد أجهزة IoT وتصعيد الهجمات السيبرانية[42].

مشاركة الذكاء الاصطناعي في نظام الكشف عن الاقتحام

ثمة خوارزميات لتوجيه النظام الذي يتركز في سيناريوهات IDS. من أجل القيام بذلك، يتم أخذ التصنيف في الاعتبار لمجموعات بيانات الأمن السيبراني التي تجمع بياناتها في عديد من المجموعات. سيقرر هذا العمل النماذج الموجودة في الشبكة العصبية (متعددة الطبقات أو متكررة)، ووظائف التنشيط وخوارزميات التعلم، اعتمادًا على قاعدة البيانات، لتحقيق دقة أعلى. أخيرًا، تم استخدام النتائج لتحديد فئة البيانات لمجموعة بيانات السلامة الإلكترونية التي كانت أكثر أهمية لاكتشاف التطفل والتكوين الأكثر ملاءمة لخوارزمية التعلم الآلي لتقليل عبء الحساب. هناك أيضًا مخاطر كبيرة على السلامة في عمليات الربط البيني اللازمة لتمكين بعض الميزات الأكثر فائدة للسيارات. من أجل تنسيق عملياتها،

يجب على السيارات إخطار المركبات الأخرى بخططها وحالتها وسلوكها والاعتماد على المعلومات التي تقدمها المركبات الأخرى[43].

تم تقديم نموذجًا للتعلم الآلي للسلامة يعتمد على نظام كشف التسلل IntruD Tree يأخذ تصنيف ميزة الأمان بناءً على أهميته ويبني نموذجًا شاملاً للكشف عن التسلل. لا يتمتع هذا النموذج بدقة تنبؤية لحالات الاختبار القبيحة فحسب، بل يقلل أيضًا من تطوير الكمبيوتر للنموذج عن طريق تقليل قياسات الميزات. أخيرًا، يتم استخدام مجموعات بيانات الأمن السيبراني والدقة وقياسات قيم ROC في اختبار فعالية نموذج IntruDTree الخاص بنا.

تحظى تقنية التعلم الآلي ـ كما سبقت الإشارة ـ بشعبية في عديد من المجالات، ولدى تقنية التعلم الآلي عديد من التطبيقات للأمن السيبراني. تشمل أمثلة البرامج الضارة تحليل البرامج الضارة، ولا سيما الكشف عن البرامج الضارة في الهجوم دون انتظار، وتحليل التهديدات، واكتشاف شذوذ التطفل، وغيرها كثير في عديد من منتجات الأمن السيبراني، يستخدم العلماء اكتشاف التعلم الآلي بسبب عدم كفاءة الأساليب القائمة على التوقيع في اكتشاف الهجمات غير اليومية أو حتى المتغيرات البسيطة للهجمات الحالية. حيث التعلم الآلي هو طريقة، يناقش المتهمون مجالات مختلفة للأمن السيبراني. من أجل التلاعب بالتدريب والبحث في تصنيف البيانات، يتمتع المتهمون أيضًا ببعض الخبرة في الهجوم السلبي على خوارزميات التعلم الآلي حتى لا تنجح هذه الأساليب[44].

التعلم الآلي أو تعلم الآلة هو جعل الحاسب يتعلم كيفية حل المشاكل بنفسه، وذلك يتم إما بالتعلم من اكتساب الخبرات السابقة أو خلال تحليل الحلول الصحيحة واستنباط طريقة الحل منها أو حتى من التعلم

خلال الأمثلة) أو هو مجموعة من تقنيات البرمجيات التي تسمح للآلة بتكييف السلوك مع بيتها دون تدخل الإنسان أو بتدخله بشكل جزئي تقنياً، أو هو تصميم خوارزميات قادرة على اتخاذ قرارات مستقلة دون برمجة مسبقة أو عبارة عن مجموعة من الخوارزميات التي يتم تغذيتها بالبيانات المنظمة من أجل اتمام المهمة دون برمجة كيفية القيام بذلك[45].

يمكن التوصل إلى أنه في حالة الذكاء الاصطناعي لا تحتاج الخوارزميات إلى فهم سبب تصحيحها وتحسينها ذاتيا فهي مبرمجة فقط للقيام بذلك. أما عندما يصل التعلم الآلي يتم تدريب الأجهزة مع مجموعة من البيانات والخوارزميات ومنحها القدرة على تعلم كيفية تنفيذ مهمة ما السبب في سماعنا التعريفيين المتبادلين هو أن الذكاء الاصطناعي يمكن أن يوجد من تعلم الآلة على الرغم من أن التعلم الآلي لا يمكن أن يوجد بكون الذكاء الاصطناعي ، وإذا كان التعلم الألي وسيلة لتحقيق الذكاء الاصطناعي ، فإن التعلم العميق هو تقنية للتعلم الألي ، فالتعلم العميق ليس بديلا للتعلم الألي ولكنه جزء من التعلم الألي نفسه[46].

نظرا لأن القرصنة أصبحت أكثر انتشارًا في جميع مجالات أسلوب الحياة المليء بالتكنولوجيا الذي اعتاد عليه هذا العالم، يجب بذل المزيد لتقليل تأثيرها على الأشخاص والشركات والكيانات الأخرى. وبقدر ما أصبحت التكنولوجيا مفيدة، فإن لديها أيضا القدرة على تحقيق زوال المنظمات التي لا تقوم

بدورها للحماية الفاعلة من الهجمات الإلكترونية وتأمين البيانات المخزنة داخل أنظمتها لا يمكن التعامل السليم مع الأمن السيبراني خلال استخدام الأدوات القائمة على التكنولوجيا فقط. سيكون استخدام التفاعل البشري ضروريًا دائما لرصد أفضل ممارسات الأمن السيبراني واختبارها وتنفيذها[47].

أصبح القراصنة أكثر تطوراً ومهارة في هجماتهم الهندسية الاجتماعية. إنهم قادرون على تجميع بيانات متباينة من مصادر مختلفة، وهي وسائل التواصل الاجتماعي ومدونات الشركات والبيانات، وسحب البيانات المهمة والمفتاحية بصعوبة من الموظفين ذوي النوايا الحسنة الذين يستخدمهم مجرمو الإنترنت هؤلاء لمهاجمة الشبكات وسرقة البيانات التي لا تقدر بثمن وحتى احتجاز الشركات كرهائن وفي بعض الحالات إتلاف أهدافهم[48].

أدى تورُّط الذكاء الاصطناعي في نظام الكشف عن الاختراق (IDS) إلى تحسين دقة وفعالية الكشف عن مختلف أنواع الهجمات السيبرانية. يمكن لنظام IDS المستند إلى الذكاء الاصطناعي الكشف عن الهجمات التي قد يغفلها نظام IDS القائم على القواعد التقليدية عن طريق تحليل حجم كبير من حركة المرور عبر الشبكة وتحديد الأنماط التي تشير إلى وجود هجوم. يمكن أيضًا لخوارزميات الذكاء الاصطناعي أن تتعلم من الهجمات السابقة وتحسين دقة وقدرات الكشف باستمرار. تزداد استخدام تقنيات التعلم العميق، مثل الشبكات العصبية المتراكبة (CNN) والشبكات العصبية الدورية (RNN)، في نظام IDS لتحليل حركة المرور عبر الشبكة والكشف عن الشذوذ. ومع ذلك، هناك تحديات في تنفيذ نظام IDS المستند إلى الذكاء الاصطناعي، مثل الحاجة إلى كميات كبيرة من البيانات التدريبية وامكانية وجود

إيجابيات خاطئة. على الرغم من هذه التحديات، يتوقع استمرار استخدام الذكاء الاصطناعي في نظام IDS مع تصاعد الهجمات السيبرانية وصعوبة نظام IDS التقليدي في مواكبة التطورات [49].

هجمات الشبكات المحددة للبرمجيات والذكاء الاصطناعي

تعد البرمجيات وضعف الإنترنت، وتراكم البيانات غير المعالجة في البيانات الضخمة، مشاكل حاسوبية خطيرة. كلاهما مرتبط بالبشر. الأول يرجع إلى العيوب التي سببتها التدخلات البشرية. في الحالة الأخيرة، يتدخل البشر أيضًا «لربط النقاط»، وإيجاد أنماط ذات مغزى ولها معنى. تستند الحلول المقترحة إلى المزيد من التدخلات البشرية، والتي تميل إلى تفاقم المشكلات بدلاً من حلها. في كلتا الحالتين، تم اقتراح القضاء التام على التدخلات البشرية. ومن السهل تحقيق هذا الهدف من الناحية المفاهيمية. ومع ذلك، فإن النهج جذري ونظري. تعد مجموعة الأسباب، وهي كائن رياضي، اللغة العالمية الكامنة وراء جميع المعلومات، وبالتالي كل الحسابات. يُعترف بهذا الافتراض كمبدأ السببية الأساسي، الذي يتبع أسبابه. فقط مجموعة السبب ومقياسها ومجموعة واسعة من خصائصها الجبرية هي أساس هذه النظرية الجديدة. الآثار غير متوقعة ورائعة وجديدة تمامًا. نظرًا لأن الترجمة بين المجموعات السببية ولغات البرمجة سهلة، ثمة اقتراح أن يقتصر استخدام اللغات على الواجهة البشرية ويتم إنشاء طبقة داخلية من الشفرة الرياضية التي يتم التعبير عنها كمجموعة سببية. تتحدث الآلات فقط إلى رمز خالٍ من الأخطاء وآمن ويتم التحقق منه رياضيًا. ثمة إشارة إلى عمليات التحقق من النظرية التجريبية

والحسابية، وتطبيقات ثغرات الإنترنت المقترحة، والعلوم والتكنولوجيا، والتعلم الآلي، وذكاء الكمبيوتر، والتفاصيل لإنشاء نموذج أولي[50].

إن تصميم وتنفيذ هيكل للتحالف من شأنه أن يوفر دعما ذكيا لأخصائيّ الأمن البشري. من الأهمية ومن الصعب التركيز على التطور السريع للأحداث الخبيثة التي لها تأثير كبير على العمليات الإلكترونية العادية. من أجل الاستجابة بفعالية للهجمات الإلكترونية، التي نمت بمعدلات غير مسبوقة، سيتطلب التعلم الآلي المتقدم اكتشافًا آليًا للهجمات ويقترح بذكاء آليات لمنع المهاجمين من استئناف المزيد من الهجمات. من أجل حل هذه التحديات بشكل فاعل، يقدم المتهمون تصميم وتنفيذ مساعد إلكتروني ذكي يدعم محللي الأمن خلال الدفاع عن التهديدات الحالية والجديدة بكفاءة وسرعة. يوضح المتهمون أيضًا أن ICSA يمكنها التكيف والتعلم بشكل فعال لتعزيز قدراتنا على جمع الذكاء وتحليله لإكمال مهام التوعية المعقدة بالوضع السيبراني وتطوير سلوك آلي وشبه آلي لحماية نقاط الضعف[51].

يقدم المتهمون إطارًا للاستخراج التلقائي وتحليل النص باللغة الطبيعية المتاحة عبر الإنترنت باستخدام تقنيات الويب الدلالي. يقدم النظام نتائج يقوم خبراء الأمن السيبراني بتحليلها بشكل أكبر لاكتشاف عمليات قراصنة القبعات السوداء. يدرس المتهمون عددًا من الميزات حول التواصل وعمل مجموعات القرصنة عبر الإنترنت وكيف يوفر تحليل شبكات الإنترنت المختلفة التفاصيل. يوفر النموذج مقتطفات ويحلل المصادر عبر الإنترنت كبيانات مدخلات مع لغة متعلقة بالأمن السيبراني الوجودي

الطبيعي. الهدف الرئيس هو جمع المعلومات حول عمليات قراصنة القبعة السوداء المحتملة، والتي يمكن للخبراء تحليلها لاحقًا[52].

يعتقد أن مصطلح «القبعة السوداء» نشأ من الأفلام الغربية حيث ارتدى الأشرار قبعات سوداء وارتدى الأخيار قبعات بيضاء .قرصان القبعة السوداء هو فرد يحاول الوصول غير المصرح به إلى نظام أو شبكة بهدف استغلالها لأغراض خبيثة. ليس لدى قراصنة القبعة السوداء أي إذن أو سلطة لاختراق أهدافهم المقصودة. يحاولون إحداث فوضى خلال المساس بأنظمة الأمان، أو تعديل وظائف مواقع الويب والشبكات ، أو إغلاق الأنظمة . غالبا ما يفعلون ذلك بقصدسرقة كلمات المرور، و المعلومات المالية والتفاصيل الشخصية الأخرى أو الوصول إليها .

تصبح هجمات شبكات البرمجيات المحددة (SDN) مصدر قلق متزايد مع تزايد اعتماد تقنية SDN في شبكات المؤسسات. يمكن لهجمات SDN استغلال الطائرة التحكم المركزية في SDN لتعطيل عمليات الشبكة أو سرقة المعلومات الحساسة. يمكن للذكاء الاصطناعي أن يؤدى دوراً حاسماً في كشف وتخفيف هجمات SDNخلال تحليل حركة المرور عبر الشبكة وتحديد السلوك غير العادي. ويمكن لخوارزميات الذكاء الاصطناعي أن تتعلم التعرف على السلوك العادي في الشبكة والكشف عن الانحرافات عن هذا السلوك التي قد تشير إلى وجود هجوم. يمكن أيضًا استخدام الذكاء الاصطناعي لتعديل سياسات الشبكة بشكل ديناميكي لمنع الهجمات وتقليل تأثيرها. ومع ذلك، هناك تحديات في تنفيذ أمان SDN المستند إلى الذكاء الاصطناعي، مثل الحاجة إلى كميات كبيرة من البيانات التدريبية

وامكانيـة وجـود إيجابيـات خاطئـة. علـى الـرغم مـن هـذه التحـديات، يتوقـع اسـتمرار اسـتخدام الـذكاء الاصطناعي في أمان SDN مع انتشار SDN وتزايد استهداف المهاجمين لشبكات SDN"[53].

التهديد المادي السيبراني للمباني ديناميكي وغير خطي وسريع التغير لأن المباني مرتبطة بالفضاء الإلكتروني خلال التشغيل وتكنولوجيا المعلومات. يمكن أن يؤدي بناء الهجمات الإلكترونية إلى الاستفادة من فحوصات المباني وإلحاق الضرر بشبكات الشركات ماديًا وماليًا وسمعة. يمكن أن يؤدي ذلك إلى الخسارة والتعطيل والفساد والإضرار بالمعلومات السرية حول التمويل والبناء، بما في ذلك الأنظمة اللازمة لأعمال البناء الآمنة والفعالة. من الضروري وضع خطة وطنية شاملة لبناء الأمن السيبراني، تتضمن إرشادات قابلة للتنفيذ لاختيار وتنفيذ ضوابط الأمن السيبراني المناسبة، واستراتيجيات لتقييم نضج وكفاءة مبرمجي الأمن السيبراني. تم تعديل نموذج الأمن السيبراني والنضج (C2M2) شائع الاستخدام التابع لوزارة الطاقة الأمريكية إلى نسخة تم فحصها بحثًا عن الأصول الإلكترونية الحساسة وضوابط البناء من أجل تقييم نضج مبرمجي الأمن السيبراني لبناء أنظمة التحكم. يوفر نموذج المبنى –B) C2M2 (C2M2 المحدّث مقاييس النضج في المجالات البرنامجية للسلامة السيبرانية[54].

تقدم نسخة «B–C2M2 لايت» تقييمات سريعة للأمن السيبراني لمديري المرافق ومهندسي أنظمة إدارة البناء وموظفي تكنولوجيا المعلومات. في منشآت متعددة تم اختبار الأداتين بشكل تجريبي. أثبتت التطورات في الذكاء الاصطناعي والتعلم الآلي في مجموعة متنوعة من المجالات أنها مفيدة جدًا في مجموعة كبيرة من التطبيقات العسكرية. لذلك ستصبح البيانات شريان الحياة لعديد من التقنيات التي تم تمكينها بواسطة الذكاء الاصطناعي والتعلم الآلي. ومع ذلك، فإن تطوير مجموعات بيانات سرية للتدريب

واختبار تطبيقات الذكاء الاصطناعي والتعلم الآلي سيصبح قضية رئيسة من أجل توليد سلوك يمكن التنبؤ به لهذه التكنولوجيا من أجل تعزيز الثقة في النظم المستقلة. لذلك، لا يمكن لوزارة الدفاع الأمريكية (DOD) أن تظل عاطلة طالما بقيت التطورات في الذكاء الاصطناعي والتعلم الآلي في مكانها. بدلاً من ذلك، يمكن للجيش الأمريكي البدء في تمهيد الطريق لتطوير بيانات تدريب خاصة بالمجال والتي ستساعد في الالتقاء في المستقبل مع الذكاء الاصطناعي والتعلم الآلي[55].

الإنترنت أداة رئيسة لتطوير الأعمال والعلاقات الاجتماعية. لذلك، يجب تقييم الأمن السيبراني بشكل صحيح لمواجهة التهديدات الجديدة والمتطورة، على سبيل المثال. ولتوفير خدمات واسعة النطاق، يجب اتخاذ تدابير مضادة مناسبة ذات أثر لا يُذكر على الطاقة. تُستخدم التدابير التي تم جمعها لتشكيل العلاقات بين مصارف الطاقة وحجم المفتاح أو الحمل المقدم خلال نهج الصندوق الأسود. يمكن أيضًا تجنب حملات تحليل حركة المرور الكلاسيكية مع النتائج.

ينمو العالم بمزيد من التكنولوجيا المعنية، ومن الضروري تعليم الأمن السيبراني. وافق المؤيدون على تطوير طريقة مبتكرة لتحسين الأمن السيبراني من أجل دعمنا في هذا المسعى. يتحقق نهجنا مما إذا كان نظامنا الجديد تعليمًا قابلاً للتطبيق للأمن السيبراني. وللقيام بذلك، طُلب إلى المشاركين إجراء دراسات استقصائية والتعليق على أنفسهم[56].

منع الهجمات الإلكترونية والتهديدات باستخدام الذكاء الاصطناعي

كان الذكاء الاصطناعي مجرد نوع من إصدار الذكاء البشري المحوسب. كانت الطريقة التي يعمل بها الذكاء الاصطناعي مثل التعلم، كما يفعل الناس، مرارًا وتكرارًا. إن خطر المناظر الطبيعية يتطور بلا شك في هذا القرن. يعتمد المهاجمون السيبرانيون فقط على الحوافز المالية. تم إيجاد طريقة جديدة لردع الهجمات قبل حدوثها لأنها لا تستطيع الاعتماد على الطريقة التقليدية القديمة بعد الآن. نشير هنا إلى الحاجة إلى تطوير مهارات السلامة الإلكترونية وكيف يمكن أن يعني استخدام الشبكات العصبية الاصطناعية وخوارزميات التعلم الآلي تحسين المهارات. كما تم تضمين نظرة عامة وتعريف للهندسة الاجتماعية والدور الذي تؤديه في التواصل وسرقة الهوية الإلكترونية، والأسباب والتأثير على الجرائم الإلكترونية. أوصى المتهمون أخيرًا بالعمل الوقائي والحلول المحتملة للتهديدات ونقاط الضعف في الهندسة الاجتماعية. وثمة إشارة إلى أن الضعف يكمن في سلوك الإنسان والنبضات العقلية والاستعدادات النفسية، على الرغم من أن التكنولوجيا مفيدة في الحد من تأثير هجمات الهندسة الاجتماعية. بينما تدعم الدراسات مخاطر الاستثمار في معسكرات التعليم التنظيمي عليها خلال حساسيات الهندسة الاجتماعية، فإنها متفائلة بإمكانية تقليل الهجمات عليها[57].

الهندسة الاجتماعية، المعروفة أيضا باسم القرصنة البشرية، هي فن خداع الموظفين والمستهلكين للكشف عن أوراق اعتمادهم ثم استخدامها للوصول إلى الشبكات أو الحسابات. إنه استخدام صعب للقراصنة للخداع أو التلاعب بميل الناس إلى الثقة أو أن يكونوا شركات أو ببساطة متابعة رغبتهم في الاستكشاف والفضول. لا تستطيع أنظمة أمان تكنولوجيا المعلومات المتطورة حماية الأنظمة من القراصنة أو الدفاع ضد ما يبدو أنه وصول مصرح به يتم اختراق الأشخاص بسهولة مما يجعلهم وما ينشرون على وسائل التواصل الاجتماعي أهدافا هجومية عالية الخطورة عاليا ما يكون من السهل إقناع

مستخدمي الكمبيوتر بإصابة شبكة الشركات أو الهواتف المصولة الخاصة بهم عن طريق استدراجهم إلى محاكاة مواقع الويب و / أو خداعهم للنقر على الروابط الضارة و/أو تنزيل وتثبيت التطبيقات الضارة و/أو التحايل[58].

نجمت خسارة مليارات الدولارات عن الجرائم الإلكترونية، وأنظمة التشغيل الفاشلة، وتدمير المعلومات السرية، وأمان الشبكة وسريتها. أصبح أمن أنظمة الكمبيوتر ضروريًا لتقليل تأثير الجرائم الإلكترونية وردعها على الأرجح في ضوء هذه الجرائم المرتكبة كل يوم. يناقش المؤيدون أحدث التقدم في استخدام مجموعات بيانات الأمن السيبراني لتقييم التعلم الآلي وأنظمة الكشف عن اختراق تعدين البيانات. وُجد أن أحدث معايير الأمن السيبراني لـ KDD و UNM لم تعد موثوقة، لأن قواعد بياناتها التي لم تعد تتبع التطورات الحالية في تكنولوجيا الكمبيوتر. وبالتالي، اقتُرح وضع معيار جديد للأمن السيبراني لمجموعة بيانات لينكس (ADFA–LD) ADFA في عام 2013 لتلبية التطورات الحالية في تكنولوجيا الكمبيوتر العالمية من أجل تحليل التعلم الآلي لاستخراج البيانات وأنظمة الكشف عن التسلل. وترد في وثيقة ADFA–LD تعاريف أفضل لخصائصها. سيتم استخدام كل هذا للتخلي عن مجموعات بيانات قياس الأمن السيبراني الحالية والبدء في استخدام مجموعة بيانات القياس المنفذة حديثًا لإجراء تقييم فعال ومنهجي لنظام الكشف عن اقتحام التعدين الحاسوبي والبيانات[59].

يعد التحليل الاجتماعي وتحليل حركة المرور عبر الإنترنت مهمًا لتحديد التهديدات الإلكترونية والدفاع ضدها. تحل مناهج التعلم الآلي المتزايدة محل الأساليب التقليدية التي تعود إلى القواعد المحددة يدويًا. يتم تسريع هذه الثورة خلال مجموعات البيانات الضخمة التي توفر نماذج التعلم الآلي بكفاءة أعلى. هذه ليست رغبة منعزلة، ولكن الاستخدام العام لمختلف الشبكات والحركات الاجتماعية يعزى إلى ذلك. تظهر التدفقات أيضًا عددًا من الميزات، بما في ذلك الحجم الثابت وعديد من الرسائل بين المصدر والوجهة. تقدم المقالة منهجية البحث الحالية وتطبيقها في أمن الإنترنت القائم على بيانات النقل الاجتماعي والإنترنت (DDCS). يتضمن نهج DDCS ثلاثة عناصر: جمع البيانات للأمن السيبراني وهندسة الأمن السيبرانيونمذجة الأمن السيبراني. هناك أيضًا مناقشة للتحديات والمسارات المستقبلية[60].

تزود الهجمات الإلكترونية الولايات المتحدة بتهديدات كبيرة للأمن القومي. اليوم، تنفذ مجموعة متزايدة من الأدوات الضارة عديد من الهجمات الإلكترونية. تم التخطيط للمعرفة والأدوات لردع الهجمات والتخفيف من حدتها من أجل استخبارات التهديد السيبراني (CTI) والبوابة التي تحلل البرامج الضارة. ومع ذلك، تم اتهام بوابات CTI الحالية وتحليلات البرامج الضارة بأنها شديدة التفاعل لأنها تعتمد على الهجمات الإلكترونية السابقة لجمع البيانات. توفر منتديات المتسللين عبر الإنترنت بوابة CTI والبرامج الضارة الاستباقية مصدرًا جديدًا للمعلومات.

في العقود الأخيرة، زادت تهديدات الأمن السيبراني. يعتقد الخبراء أن الإجراءات الأمنية الحالية لن تكون كافية قريبًا لتجنب انتشار الهجمات الإلكترونية الأكثر تقدمًا وخطورة. في الآونة الأخيرة، هيمنت الأساليب المستعارة من الذكاء الاصطناعي على تعقيد الأمن السيبراني بشكل متزايد لتعزيز الأتمتة.

تم وضع مسحًا شاملاً للأعمال المتعلقة بالتعلم الآلي للأمن السيبراني ، والقواعد والحماية المقابلة للهجمات الإلكترونية، وأساسيات خوارزميات التعلم الآلي الأكثر شيوعًا وخطط التعلم الآلي وخطط تعدين بيانات الأمن السيبراني المقترحة للميزات، الحد من الأبعاد والتصنيف والكشف[61].

أصبح منع الهجمات السيبرانية والتهديدات باستخدام الذكاء الاصطناعي مجالًا بحثيًا مهمًا يتزايد أهميته. يمكن استخدام الذكاء الاصطناعي لكشف ومنع الهجمات في الوقت الفعلي عن طريق تحليل حركة المرور عبر الشبكة وتحديد السلوك غير العادي. كما يمكن لخوارزميات الذكاء الاصطناعي أن تتعلم من الهجمات السابقة وتحسين دقتها وفعاليتها باستمرار. يتم استخدام تقنيات التعلم الآلي، مثل آلة الدعم النوعي (SVMs) والغابات العشوائية، بشكل متزايد في الأمن السيبراني للكشف عن الهجمات ومنعها. كما تستخدم تقنيات التعلم العميق، مثل الشبكات العصبية المتراكبة (CNNs) والشبكات العصبية الدورية (RNNs)، لتحليل حركة المرور عبر الشبكة والكشف عن الهجمات. ومع ذلك، هناك تحديات في تنفيذ الأمن السيبراني المستند إلى الذكاء الاصطناعي، مثل الحاجة إلى كميات كبيرة من البيانات التدريبية وامكانية وجود إيجابيات خاطئة. على الرغم من هذه التحديات، يتوقع استمرار استخدام الذكاء الاصطناعي في الأمن السيبراني مع تزايد التهديدات السيبرانية وعدم كفاية الأساليب التقليدية للكشف والوقاية"[62].

تدخلات الأمن السيبراني والذكاء الاصطناعي القائمة على الأعمال التجارية

تم تسليط الضوء على مزايا استخدام الذكاء الاصطناعي لزيادة القدرة التنافسية للأعمال وفي الوقت نفسه زيادة الوعي من أجل حل الخوف في استكشاف التقنيات الناشئة بسبب الهجمات الإلكترونية. ما مدى عدم أمان شركات الحوسبة؟ 100%. 100%. كان الإنترنت مكانًا مشتركًا للجميع. قد تصبح بيانات التخزين على أي جهاز كمبيوتر متصل بالإنترنت في أي ثانية معرضة للخطر. تمت مناقشة حالة الذكاء الاصطناعي الحالية في الأمن السيبراني، وتم تحديد عديد من دراسات الحالة والتطبيقات الخاصة بالذكاء الاصطناعي لدعم المجتمع لفهم المشكلات والقضايا التي لم يتم حلها بشكل أفضل في الأمن السيبراني، بما في ذلك الهندسة والقادة والأكاديميين والمعلمين والمبتكرين ورجال الأعمال والطلاب[63].

يخضع الأمن السيبراني لتغييرات تقنية وتنظيمية كبيرة في عالم الحوسبة في الأيام الأخيرة، وعلم البيانات يقود التقدم. من أجل أتمتة وبناء بنية أمنية بذكاء، يجب استخراج الأنماط أو الرؤى من بيانات الأمن السيبراني وإنشاء النموذج المقابل القائم على البيانات. من أجل فهم وشرح الظواهر الفعلية باستخدام البيانات، يتم استخدام عديد من طرق البحث وتقنيات التعلم الآلي والعمليات والأنظمة، والتي تسمى عادة دراسات البيانات. تتيح نظرية علوم بيانات الأمن السيبراني للحوسبة الأمنية السيبرانية أن تكون أكثر تشغيلاً وذكاء من العمليات التقليدية. ثم يجري تناول عدد من المشاكل والتوصيات البحثية ذات الصلة وتلخيصها. لدى المؤيدون أيضًا إطار عمل متعدد الطبقات لنمذجة الأمن السيبراني للتعلم الآلي. باختصار، الهدف هو التركيز على تطبيق عملية صنع القرار الذكية التي تدعم البيانات على أنظمة المساعدة الإلكترونية وكذلك على علوم السلامة السيبرانية وكذلك التقنيات ذات الصلة[64].

أصبح تورُّط الذكاء الاصطناعي في الأمن السيبراني المستند إلى الأعمال التجارية أمرًا مهمًا يتزايد أهميته مع استمرار الهجمات السيبرانية المستهدفة للشركات. يمكن استخدام الذكاء الاصطناعي لكشف ومنع الهجمات عن طريق تحليل كميات كبيرة من البيانات وتحديد الأنماط السلوكية التي قد تشير إلى هجوم. كما يمكن لخوارزميات التعلم الآلي أن تتعلم من الهجمات السابقة لتحسين دقتها وفعاليتها. ويمكن أيضًا استخدام الذكاء الاصطناعي لمراقبة سلوك المستخدمين وتحديد التهديدات الداخلية المحتملة. ومع ذلك، هناك تحديات في تنفيذ الأمن السيبراني المستند إلى الذكاء الاصطناعي في سياق الأعمال التجارية، مثل الحاجة إلى خبرة متخصصة وامكانية وجود إيجابيات خاطئة. بالإضافة إلى ذلك، هناك اعتبارات أخلاقية تحيط باستخدام الذكاء الاصطناعي في الأمن السيبراني، مثل احتمالية وجود تحيز والحاجة إلى الشفافية في عملية صنع القرار. على الرغم من هذه التحديات، يتوقع استمرار استخدام الذكاء الاصطناعي في الأمن السيبراني المستند إلى الأعمال التجارية مع سعي الشركات لحماية أنفسها من الهجمات السيبرانية وانتهاكات البيانات"[65].

الجرائم الإلكترونية هي أي جرائم تنطوي على شبكة وجهاز كمبيوتر. يمكن ارتكاب الجرائم إما على الكمبيوتر أو يمكن أن يكون الكمبيوتر هدفًا للجريمة. غالبًا ما تتكون الجرائم الإلكترونية من جرائم تقليدية مثل سرقة الهوية والاحتيال والمطاردة عبر الإنترنت والتنمر عبر الإنترنت واستغلال الأطفال في المواد الإباحية[66].

معالجة الصور الطبية والهجمات الإلكترونية بالذكاء الاصطناعى

ينمو التعلم الآلي والذكاء الاصطناعي بشكل غير مسبوق. تحتوي هذه التكنولوجيا على عديد من التطبيقات المفيدة، من الترجمة الآلية إلى معالجة الصور الطبية. ويجري تطوير عدد لا يحصى من هذه الابتكارات ويمكن التخطيط لها على المدى الطويل. كانت الطريقة التي يمكن بها إساءة استخدام الذكاء الاصطناعي تحظى باهتمام أقل تاريخيًا. يستكشف التقرير المشهد الطبيعي لمخاطر السلامة المحتملة من إساءة استخدام تقنيات الذكاء الاصطناعي ويقترح طرقًا للمساعدة في التنبؤ بها وتجنبها والتخفيف منها. يحلل المؤيدون التوازن طويل المدى بين المعتدين والمدافعين، لكن المؤيدون لا يعالجون هذه القضية. بدلاً من ذلك، يركز الباحثون على أنواع الهجمات التي سيقوم مؤلفو الهجمات قريبًا بمعرفة ما إذا لم يتم تطوير حماية كافية[67].

معالجة الصور الطبية مجال مهم يمتلك القدرة على ثورة الرعاية الصحية. ومع ذلك، كما هو الحال مع أي تقنية تتضمن بيانات مرضى حساسة، فهناك خطر هجمات الإنترنت. يمكن أن تؤدي هجمات الإنترنت على نظم معالجة الصور الطبية إلى عواقب خطيرة، بما في ذلك سرقة بيانات المرضى، وتزوير الصور الطبية، وتعطيل الرعاية الصحية للمرضى. وهناك عدة أنواع من هجمات الإنترنت التي يمكن تشنها على نظم معالجة الصور الطبية، بما في ذلك هجمات الفدية، وهجمات الخدمة المنكرة، وهجمات البرامج الضارة. ومن أجل الحماية من هذه الهجمات، يجب على المؤسسات الطبية تنفيذ إجراءات أمنية قوية، مثل جدران الحماية، ونظم اكتشاف الاختراقات، والتشفير. بالإضافة إلى ذلك، ينبغي تصميم نظم معالجة الصور الطبية بمراعاة الأمان، مع مزايا مثل ضوابط الوصول وسجلات

المراجعة. كما أنه من المهم بالنسبة للمؤسسات الطبية تدريب موظفيها على أفضل الممارسات في الأمان السيبراني وتحديث بروتوكولات الأمان بانتظام للبقاء على اطلاع بالتهديدات الناشئة"[68].

الأمن السيبراني مجال تكنولوجيا دائم التطور، على هذا النحو، سيكون هناك دائما اتجاهات لا تعد ولا تحصى يجب مراعاتها خلال تقدم الأمن السيبراني نأتي الحاجة المتزايدة للمنظمات لمواكبة التطور السريع للتكنولوجيا. ومع ذلك، أصبحت فجوة المهارات الحالية لمتخصصي الأمن السيبراني مدعاة للقلق بشكل كبير . أدى انتشار الحوسبة السحابية إلى خلق حاجة إلى إجراءات جديدة للتحليل الجنائيالسحابي، وقد أدى استخدام الأجهزة الطبية المتصلة بالإنترنت إلى زيادة المخاوف بشأن هيكل أمن المعلومات لعديد من المنظمات .ومن أجل حل هذه المسائل، يتعين إجراء اختبار مناسب للثغرات الأمنية وتنفيذ عمليات جديدة لمواكبة التغيرات في التكنولوجيا للحد من إمكانية حوادث القرصنة والمساعدة في الإصلاح. إذا استفاد المزيد من المنظمات من المهارات والموظفين المتاحين لها، فهناك طرق التقليل فجوة المهارات وغيرها من القضايا التي تؤثر على الأمن السيبراني[69].

التقدم في تقنيات التشفير والذكاء الاصطناعي

الأمن السيبراني نظام دائم التغير كان في الاعتبار على مدار العقد الماضي، حيث يتزايد عدد التهديدات ويحاول مجرمو الإنترنت بنشاط إبقاء تطبيق القانون في المقدمة. في حين أن الأسباب الأولية للهجمات الإلكترونية تظل دون تغيير نسبي على مر السنين، أصبح مجرمو الإنترنت متطورين بشكل

متزايد في تقنياتهم. أصبح الكشف عن التهديدات الإلكترونية الجديدة والتخفيف من حدتها غير فاعل في حلول الأمن السيبراني التقليدية. يعد التقدم في تقنيات التشفير والذكاء الاصطناعي (لا سيما التعلم الآلي والتعلم العميق) واعدًا للسماح لخبراء الأمن السيبراني بمعالجة التهديد المتزايد باستمرار الذي يشكله المعارضون. هنا، يناقش المؤيدون قدرة الذكاء الاصطناعي على تحسين حلول الأمن السيبراني، سواء خلال التعرف على نقاط قوته أو قيوده. يتحدث المتهمون عن فرص البحث المحتملة في مجال الأمن السيبراني المتعلقة بتقدم تقنيات الذكاء الاصطناعي عبر مجموعة متنوعة من مجالات التطبيق[70].

تم اقتراح حل إعادة إنشاء وتعويض هجين كلاسيكي ذكي للهجمات الإلكترونية على CPS ومدخلات إنترنت الأشياء الصناعية عبر شبكات الاتصالات المشتركة. من أجل التعويض عن الهجمات الإلكترونية، تم بناء نظام تحكم كلاسيكي ذكي. تم تصميم الشبكات العصبية (NN)، وهو نظام تحكم غير خطي تقليدي يعتمد على إطار التحقق المتغير، للتعويض عن الهجمات والتحكم في نتيجة الجهاز في تطبيقات المراقبة. في المنهجية المقترحة، يتم استخدام نظرية التحكم غير الخطية لضمان استقرار الجهاز عند حدوث الهجمات. في هذه التقنية، NN هو تقييم عبر الإنترنت وإعادة بناء الهجمات الإلكترونية التي بدأت على البنية التحتية الشعاعية الغاوسية المترابطة. يأتي قانون تكيف المقدر الذكي من خاصية ليابونوف. أشارت نتائج المحاكاة إلى أن التقنية المقترحة موثوقة وممكنة التنفيذ كاختبار لتطبيقات التحكم في السرعة بالسيارة[71].

يمكن تعريف شبكة الانترنت بأنها شبكة اتصالات عالمية تربط بين الحواسيب، معتمدة في ذلك على بروتوكولات الاتصال التي تنظم عملية نقل المعلومات والبيانات واستقبالها بين هذه الحواسيب سواء كانت فردية أو شبكات محلية أو إقليمية[72]

كانت الشبكة العنكبوتية العالمية (شبكة الانترنت خلال العقدين الماضيين من أكثر النفايات تأثيراً، في ما يعرف حالياً بثورة المعلومات، بدأت فكرة الشبكة العالمية حكومية، وصلاحاً وقائياً خلال الحرب الباردة وتطورت تطوراً سريعاً خلال فترة قصيرة نسبياً للصبح أهم أداة في عصر المعلوماتية، ونظراً إلى التأثير الكبير للإنترنت والذى يشمل حقولاً عديدة من أهمها حقل التعليم والأبحاث والسباحة والتجارة، فإن عدد المستخدمين لهذه الشبكة ازداد بشكل فلكي، كما شكلت أيضا سهولة الربط مع شبكة الإنترنت، وتطور أجهزة الاتصال تلقائيا، وانخفاض أسعارها عاملا لجلب اعداد كبيرة من المستخدمين حيث ترتبط حاليا مئات الشبكات سواء الحكومية، أو المحلية، أو الهجمات الأكاديمية أو التجارية وحتى الشخصية لتؤلف بيئة افتراضية ضخمة، يتفاعل معها الملايين بعض النظر عن أماكن تواجدهم ..صاحب تطور الانترنت السريع تزايداً في عدد الأصوات التي تنتقد هذه الثقافة وتتهمها بخلق عديد من السلبيات والمخاطر التي تهدد المجمعات وكأي تقانة ذات حضور كبير في الحياة اليومية[73].

أصبحت الجرائم الإلكترونية تهديدًا دائمًا للتقدم الذي لا مثيل له في تكنولوجيا المعلومات (IT). كل يوم، تتعرض البنية التحتية الإلكترونية لجرائم واعتداءات إلكترونية كبيرة. ولم تكن مراقبة وأمن هذه

الهياكل الأساسية فعالة تماما بالأجهزة المادية والتدخل البشري ؛ لذلك هناك حاجة إلى أنظمة دفاعية عالية الكفاءة، يجب أن تكون قابلة للتطوير وقابلة للتكيف والمرونة، للدفاع عن البنية التحتية لتكنولوجيا المعلومات من عدد لا يحصى من الهجمات الإلكترونية الممكنة للغاية. أدت أدوات الذكاء الاصطناعي الحديثة دورًا حيويًا في تحديد الجرائم السيبرانية والوقاية منها. نهدف أيضاً إلى إظهار التقدم في المعركة ضد الجرائم الإلكترونية المتعددة في الذكاء الاصطناعي وإظهار كفاءة تقنيات الذكاء الاصطناعي المختلفة في اكتشاف ومنع الهجمات الإلكترونية وأيضًا لتوفير مجال للعمل في المستقبل. خلال العقد الماضي، زادت الهجمات الإلكترونية على نطاق واسع. أصبح مجرمو الإنترنت أكثر تقدمًا. لا تكفي عمليات التفتيش الأمنية الحالية لحماية الشبكات من مجرمي الإنترنت المؤهلين تأهيلاً عاليا. تعلم مجرمو الإنترنت كيفية التهرب من التقنيات الأكثر تقدمًا مثل IDPS، وتكاد تكون شبكات الروبوت غير مرئية لأحدث الأدوات. لحسن الحظ، يمكن أن يؤدي استخدام الذكاء الاصطناعي إلى تحسين معدلات اكتشاف أجهزة IDPS، ويمكن لتقنيات التعلم الآلي (ML) استخراج بيانات مصدر شبكة البوتات. ومع ذلك، يمكن أن ينطوي تطبيق الذكاء الاصطناعي على مخاطر أخرى ويجب على خبراء الأمن السيبراني تحقيق توازن بين المخاطر والربح[74].

"أحدث التطورات في تقنيات التشفير والذكاء الاصطناعي قد أدت إلى إسهامات كبيرة في مجال الأمان السيبراني. يوفر التشفير وسيلة لتأمين البيانات والاتصالات عن طريق تشفير الرسائل بطريقة تمكن فقط الأطراف المصرح لها من فك تشفيرها. وأدى التحسين الأخير في تقنيات التشفير إلى تطوير خوارزميات التشفير الأكثر أمانًا، مثل تشفير المنحنى البيضوي والتشفير المتجانس. بالإضافة إلى ذلك، تم استخدام الذكاء الاصطناعي لتحسين الأمان السيبراني عن طريق تحليل كميات كبيرة من البيانات

وتحديد الأنماط التي قد تشير إلى خرق أمني. كما يمكن لخوارزميات التعلم الآلي أن تتعلم من الهجمات السابقة لتحسين دقتها وفعاليتها. ومع ذلك، فهناك أيضًا نواحٍ سلبية في استخدام الذكاء الاصطناعي في الأمن السيبراني، مثل خطر الإيجابيات الخاطئة والحاجة إلى خبرة متخصصة. على الرغم من هذه التحديات، فإن الجمع بين تقنيات التشفير والذكاء الاصطناعي لديه القدرة على تعزيز الأمان السيبراني بشكل كبير وحماية ضد الهجمات السيبرانية المعقدة والمتطورة باستمرار "[75].

الاتصالات اللاسلكية القائمة على الهجمات الإلكترونية والوقاية من الذكاء الاصطناعي

من المتوقع ظهور اتجاهات جديدة مع ظهور شبكات الاتصالات اللاسلكية، مثل السيارات ذاتية القيادة وأنظمة الهواء غير المأهولة والروبوتات المستقلة وإنترنت الأشياء والحقائق الافتراضية. مع الجيل الخامس من الشبكات اللاسلكية، تتطلب هذه التكنولوجيا سرعات بيانات عالية جدًا ووقت انتقال منخفض بشكل لا يصدق وموثوقية كبيرة (G5). ادعى عدد كبير من المنظمات البحثية أن G5 لا يمكنها تلبية احتياجاتها دون تكامل الذكاء الاصطناعي ، لأن شبكات G5 اللاسلكية ستولد حركة مرور لا تضاهى وتمكن العلماء اللاسلكيين من الوصول إلى البيانات الضخمة للمساعدة في التنبؤ بالمطالب وتصميمات الخلايا لتلبية متطلبات المستخدم. استخدم عديد من الباحثين بعد ذلك الذكاء الاصطناعي في عديد من جوانب بنية الشبكات اللاسلكية G5 ، بما في ذلك تخصيص الموارد اللاسلكية وإدارة الشبكة[76].

بالنسبة لجميع جوانب العالم الحديث، أصبح الفضاء الإلكتروني عنصرًا لا غنى عنه. يعتمد الكوكب بشكل متزايد على الإنترنت في الحياة اليومية. كما أدى الاعتماد المتزايد على الإنترنت إلى زيادة مخاطر التهديدات الخبيثة. نظرًا لتزايد مخاطر الأمن السيبراني، أصبح الأمن السيبراني عنصرًا أساسيًا في عالم الإنترنت لمكافحة جميع التهديدات الإلكترونية والهجمات والاحتيال. يتعرض الفضاء الإلكتروني المتنامي بشكل كبير لاحتمال حدوث تهديدات إلكترونية لا نهاية لها. الغرض من هذا الاستطلاع هو تقديم لمحة عامة موجزة عن تقنيات التعلم الآلي المختلفة لمعرفة جميع الابتكارات المتعلقة بطرق الكشف عن مخاطر السلامة السيبرانية المحتملة. تُستخدم تقنيات الأمن السيبراني هذه في المقام الأول للكشف عن الاحتيال والكشف عن التسلل والرسائل غير المرغوب فيها واكتشاف البرامج الضارة. في هذه الدراسة، يعتمد المؤيدون على الدراسات المتاحة حاليًا على نماذج التعلم الآلي لتطبيقات الأمن السيبراني ويتضمنون مراجعة متعمقة لتقنيات الأمن السيبراني التعلم الآلي. وفقًا لفهمنا، حاول المتهمون أولاً مقارنة التعقيد الزمني لنماذج التعلم الآلي للأمن السيبراني المستخدمة على نطاق واسع. قارن المؤيدون بشكل شامل إنتاج كل مصنف بناءً على مجموعات البيانات المستخدمة غالبًا والمجالات الفرعية للتهديدات الإلكترونية. يقدم هذا العمل أيضًا نماذج التعلم الآلي لفترة وجيزة بالإضافة إلى مجموعات بيانات السلامة المستخدمة على نطاق واسع. على الرغم من سابقتها الأساسية، فإن الحماية الإلكترونية لها تنازلات ومشاكل مع قيودها[77].

تم إنشاء نظام اختبار الأمن السيبراني باستخدام شاشة التحكم واكتساب البيانات المقدمة (SCADA). يتكون سرير الاختبار من جهاز التحكم في خزان المياه وهو مستوى معالجة المياه وتوزيعها. تم تنفيذ هجمات إلكترونية شاملة ضد الاختبار. جمعت الهجمات حركة مرور الشبكة وجمعت

خصائص حركة المرور لإنشاء مجموعة بيانات للتدريب واختبار خوارزميات التعلم الآلي المختلفة. تم استخدام خمس خوارزميات قياسية للتعلم الآلي كتدريب على الهجمات، مثل الغابات العشوائية وأشجار القرار والاسترداد اللوجستي و المصنف البايزي الساذج و KNN. ثم تم بناء نماذج التعلم الآلي المدربة ووضعها في الشبكة لإجراء اختبارات جديدة باستخدام حركة مرور الشبكة عبر الإنترنت. تم مقارنة الإنجازات الناتجة مع النتائج التي تم الحصول عليها خلال الاستخدام عبر الإنترنت لهذا النموذج في الشبكة أثناء التدريب واختبار نماذج التعلمالآلي. تظهر النتائج فعالية نماذج التعلم الرئيسة في اكتشاف الهجمات في الوقت الفعلي. يوفر سرير الاختبار نظرة ثاقبة مباشرة لتأثير وتأثيرات الهجمات على إعدادات SCADA الحقيقية[78].

أنماط الهجوم السيبراني معقدة ومتنوعة وغالبًا ما يكون من الصعب تحديد أنواع ديناميكية من الهجمات والتنبؤ بها. في عديد من المجالات، أصبحت الأبحاث حول الرسوم البيانية للمعلومات أكثر نضجًا. من المهم جدًا حاليًا لعديد من الباحثين دمج فكرة الرسم البياني للمعرفة والأمن السيبراني لبناء قاعدة معرفية للأمن السيبراني. ستانفورد هو أيضًا أداة التعرف على الكائنات (NER) المستخدمة لتدريب المستخرج للحصول على معلومات مفيدة. تظهر النتائج التجريبية أن Stanford NER لديها عديد من الميزات وهي قادرة على تدريب معرفات الأمن السيبراني باستخدام Gazettes للتحضير للعمل المستقبلي. تشير التطورات الحديثة في الذكاء الاصطناعي إلى أن هذه التكنولوجيا الجديدة سيكون لها

تأثير أكثر حتمية بشكل عام وربما ثورية على القوة العسكرية والمنافسة الجيوسياسية والسياسة العالمية. بعد الطفرة الأولية للتكهنات واسعة النطاق في أدب الذكاء الاصطناعي[79].

أصبحت الاتصالات اللاسلكية جزءًا لا يتجزأ من الحياة الحديثة، ولكنها تشكل أيضًا مخاطر أمنية كبيرة. يمكن أن يستغل المهاجمون الثغرات في الشبكات اللاسلكية للحصول على وصول غير مصرح به إلى المعلومات الحساسة، والتقاط الاتصالات، وتشنيع أنواع أخرى من الهجمات. في السنوات الأخيرة، كان هناك اهتمام متزايد في استخدام الذكاء الاصطناعي لتحسين أمن الشبكات اللاسلكية. يمكن استخدام الذكاء الاصطناعي لكشف والرد على التهديدات في الوقت الحقيقي، وتحديد أنماط النشاط المشبوه، وتحسين أداء الشبكة العامة. على سبيل المثال، يمكن تدريب خوارزميات التعلم الآلي لتعرف على أنماط غير طبيعية في سلوك الشبكة وتنبيه المسؤولين عن احتمالية وقوع خرق أمني. كما يمكن استخدام الذكاء الاصطناعي لتعزيز بروتوكولات التشفير والمصادقة، مما يجعل من الصعب على المهاجمين اختراق الشبكات اللاسلكية. على الرغم من المزايا المحتملة للذكاء الاصطناعي في أمن الشبكات اللاسلكية، إلا أن هناك مخاوف بشأن المخاطر المرتبطة بالاعتماد بشكل كبير على الأنظمة الآلية. كما هو الحال مع أي إجراء أمني، فمن المهم إيجاد توازن بين المزايا والمخاطر المترتبة على استخدام الذكاء الاصطناعي في أمن الشبكات اللاسلكية"[80].

أنظمة الأمن السيبراني القائمة على التعلم العميق

الإطار المقترح للشبكات العصبية الاصطناعية له درجة دقة ممتازة تبلغ 99.97 في المائة ومنطقة ROC (خصائص مشغل الاستقبال) بمتوسط مساحة 0.999 ومتوسط إيجابي للخطأ يبلغ 0.001

فقط. النظام المقترح باستخدام ذكاء الكشف عن هجوم الشبكة الاصطناعية فعال ودقيق. يمكن تنفيذ الإطار الجديد المقترح لتحليل النقل الشبكي القياسي وبيانات حركة مرور النظام السيبراني الفيزيائي وتحليل حركة مرور الشبكة في الوقت الفعلي على الأجهزة (n[81]).

تُظهر الهجمات الأخيرة أن التهديدات الإلكترونية لا تتزايد من حيث الحجم فحسب، بل يتم تحسينها بشكل متزايد. يمكن أن تنطوي الهجمات على عدة تدابير يصعب تمييزها من الأنشطة الودية. لذلك يجب معالجة المعدلات الإيجابية المزيفة العالية خلال تقنيات الكشف القياسية. بسبب الفشل في إجراء تقنيات الكشف الآلي، تعتمد الاستجابات لمثل هذه الهجمات بشكل كبير على عمليات صنع القرار التي يوجهها الأشخاص. على الرغم من استخدام نظرية اللعبة في عديد من القضايا التي تنطوي على اختيار معقول، إلا أن المؤيدون يقيدون استخدام مثل هذا الإجراء في الألعاب الأمنية إذا كان لدى المدافعين الحد الأدنى من المعرفة باستراتيجيات وفوائد اللاعب المنافس. على الرغم من وجود الحد الأدنى من المعرفة حول المنافسين، إلا أن نتائج المحاكاة تشير إلى إمكانيات (Q–Learning[82]).

جذب تقدم الذكاء الاصطناعي انتباه العلماء والممارسين وفتح مجموعة متنوعة من الفرص المفيدة في القطاع العام لاستخدام الذكاء الاصطناعي. وفي ضوء هذا السياق، بدأ يظهر فهم شامل لنطاق وآثار التطبيقات القائمة على الذكاء الاصطناعي والتحديات ذات الصلة. ومع ذلك، فإن الأبحاث السابقة تنظر فقط في العزلة والتجزئة في تطبيقات الذكاء الاصطناعي والتحديات. نظرًا لعدم وجود نظرة عامة شاملة

علـى التطبيقـات القائمـة علـى الـذكاء الاصـطناعي وتحـديات القطـاع العـام، فـإن نهجنـا المفـاهيمي يحلـل ويجمع رؤى الدراسات العلمية القابلة للتطبيق لتقديم لمحة عامة شاملة عن تطبيقات الذكاء الاصطناعي والتحديات ذات الصلة.

قد حددت الدراسات الاستقصائية لدراسات تحليل الشبكات في مجالي التعلم الآلي ، التعلم العميق ، وتقدم وصفا موجزا لكل عملية من عمليات ML و DL. تتم مناقشة عملية تحليل ML و DL. تم فهرسة الارتباط الزمني أو الحراري وقراءته وتوليفه في الوثائق التي تمثل كل عملية. نظرًا لأهمية البيانات في طرق ML/DL، يوضح المؤيدون بعض مجموعات بيانات الشبكة الشائعة في ML/DL، ويتعاملون مع مشاكل الأمن السيبراني مع ML/DL، ويقدمون توصيات للتحليل[83].

التعلم العميق شكل من أشكال الذكاء الاصطناعي مستمد من التعلم الألي يرتكز علي مجموعة من الخوارزميات تشمل عدة تقنيات كالشبكات العصبية الاصطناعية والتي تحاكي الخلايا العصبية في جسم الإنسان. واستوحت الشبكات العصبية الاصطناعية مبدأها خلال طريقة عمل الدماغ البشري فهي تتكون من عدة خلايا عصبية اصطناعية مرتبطة ببعضها البعض، كلما زاد عددها كانت الشبكة أعمق. وكانت مجالاً جديداً من أبحاث التعلم الألي ، والذي تم تقديمه بهدف نقل تعلم الألة أقرب إلي أحد أهدافها الأصلية، فأصبحت ثورة الذكاء الاصطناعي الحديثة ممكنة بسبب التعلم العميق وهي تقنية جعلت تعلم الألة أسرع وأكثر دقة، وتستفيد خوارزميات التعلم العميق من البرمجة المتوازية، وتعتمد علي طبقات متعددة من الشبكات العصبية[84]

ثم التركيز على نُهُج التعلم العميق DL الحديثة في مجال الأمن السيبراني، مثل الكشف عن التسلل، وكشف البرامج الضارة، وكشف التصيد/البريد العشوائي، والكشف الافتراضي عن موقع الويب. الأول هو شرح الأوصاف الأولية لنماذج وخوارزميات DL الشائعة. ثم يتم اقتراح وتوضيح بنية DL عامة على أساس الوحدات الرئيسة الأربع لتطبيقات الأمن السيبراني.

ثم مسح شامل للذكاء الاصطناعي والتعلم العميق بين عامي 1961 و 2018. تمنح الدراسة الباحثين والممارسين دليلاً قيمًا خلال التحليل المنهجي متعدد الزوايا للذكاء الاصطناعي، من الآليات الأساسية إلى التطبيقات الوظيفية، من الخوارزميات الأساسية إلى الإنجازات الصناعية، من الوضع الحالي إلى التطورات المحتملة. الذكاء الاصطناعي هو مساعد مبتكر ومخترق مع عديد من التطبيقات والقطاعات المختلفة، على الرغم من الصعوبة الكبيرة[85].

إن الحماية الإلكترونية تتطلب تقنيات ذكاء اصطناعي جديدة وخاصة تم تطويرها لهذا النوع من الاستخدام. في الواقع، نود إلقاء نظرة عامة واسعة على الأساليب المختلفة التي يمكن أن تغير ألعاب الأمن السيبراني. ونركز على أمان تطبيقات الويب وتشجع على استخدام KNS والمنطق الاحتمالي وترقيات Bayesian لرصد احتمالية العناصر الإيجابية والسلبية المزيفة[86].

نظرًا لزيادة التهديدات الإلكترونية والقرصنة الإلكترونية، ظهرت السلامة الإلكترونية بسرعة في السنوات الأخيرة. تسلط الأبحاث الناشئة حول التكنولوجيا الضوء على المخاطر وتهمل أحيانًا المساهمة

الإيجابية المحتملة في الأمن السيبراني. يهدف التقرير إلى إجراء مسح طويل الأجل متوازن بشكل معقول لتحديد محركات التهديدات الرئيسة والتقنيات الجديدة التي يمكن أن يكون لها تأثير مباشر على حماية الأمن السيبراني وقدرات الهجوم. كانت الأدوات الرئيسة المستخدمة هي مسح الأفق واستطلاعات الخبراء عبر الإنترنت حول التهديدات الناشئة والتأثير المحتمل لعديد من التقنيات الجديدة على قدرات الدفاع السيبراني والهجوم السيبراني. أظهرت دراسة خبراء أن القوة الإلكترونية والتشفير المتجانس وسلسلة الكتلة block chain هي في الأساس تكنولوجيا أمنية. إن إنترنت الأشياء والقرصنة العضوية ومؤشر HMI والتكنولوجيا المستقلة تزيد بشكل أساسي من القدرة على الإضراب. هناك تقنية مستقلة وحوسبة كمومية وذكاء اصطناعي في المركز تساعد في الدفاع عن القدرات ومهاجمتها ولها التأثير نفسه تقريبًا على بعضها البعض. نقدم منظورًا متوازنًا وطويل الأجل وتقييمًا خبيرًا للآثار السلبية والإيجابية، بما في ذلك نضج وتوافق الآراء، للتكنولوجيات الناشئة. تم استخدام مقياسين جديدين من Likert لتصنيف النتائج إلى 4 مجموعات لتقييم الآثار المحتملة لتطوير التقنيات على الأمن السيبراني (صافي إيجابي، صافي سلبي، إيجابي – إيجابي، سلبي – سلبي)[87].

أظهرت تقنية التعلم العميق التابعة لتعلُّم الآلة إمكانيات كبيرة في الكشف عن ومنع مختلف تهديدات الأمن السيبراني. يستخدم خوارزميات التعلم العميق للكشف عن اختراقات الشبكات، البرمجيات الخبيثة، هجمات الصيد الاحتيالي، وسلوك المستخدم غير المعتاد. تتميز هذه الخوارزميات بالقدرة على التعلُّم من كميات كبيرة من البيانات والقيام بحسابات معقدة بسرعة، مما يجعلها مناسبة بشكل كبير لتطبيقات الأمن السيبراني. يمكن أيضًا لنماذج التعلم العميقالتكيُّف مع البيئات المتغيرة، مما يجعلها فعّالة في الكشف عن

التهديدات الجديدة والمتطورة. بالإضافة إلى ذلك، يمكن استخدام التعلم العميقللحصول على معلومات وتحليلات حول التهديدات، بالإضافة إلى التنبؤ بالاحتمالية المرتقبة لحدوث هجمات مستقبلية.[88].

يرتفع اهتمام الذكاء الاصطناعي والمعرفة بسرعة كبيرة لدرجة أن الأوساط الأكاديمية والتعليم العالي تكافح لتلبية الطلب المتزايد على الصناعة. كان من المتوقع أن يستخدم 75 بالمائة من برامج الأعمال الذكاء الاصطناعي أو التعلم الآلي أو تقنيات التعلم العميق من قبل 2021، ولكن البرامج الجامعية مثقلة أيضًا بالطلاب الذين يتلقون تدريبًا اختياريًا خلال عديد من الأقسام لتلقي تدريبهم على علوم البيانات. يدعو علم البيانات إلى إعداد خاص للرياضيات خاصة لطلاب الأمن السيبراني الذين قللت برامجهم من متطلبات الرياضيات المتقدمة. لتعزيز تخطيط المناهج والاستخدام العملي لتقنيات الذكاء الاصطناعي، كانت الخطوة الأولى في إدخال طلاب علوم الكمبيوتر والأمن السيبراني في مفاهيم وقدرات الذكاء الاصطناعي هي دفتر ملاحظات ("شبكة لممارسي الذكاء الاصطناعي المبتدئين تم إعداده بلغة البرمجة R. تملأ الشبكة الفجوة النظرية والواقعية للطلاب خلال إنشاء نموذج تنبؤي للتطفل من الصفر لشبكة ANN. تعمل كنموذج ولكنها تعزز أيضًا التغييرات البيئية الخطيرة ويمكن الاعتماد عليها في عدد من مجموعات البيانات في جميع مجالات التخصص في المراحل الأولية من أنشطة علم البيانات لممارس السلامة السيبرانية[89].

الأمن السيبراني القائم علي الذكاء الاصطناعي

تم تقديم منظور مفصل حول «الأمن السيبراني الذي يحركه الذكاء الاصطناعي»، والذي يمكن أن يؤدى دورًا مهمًا في خدمات وإدارة الأمن السيبراني الذكية. ستؤدي نمذجة ذكاء التهديدات باستخدام أساليب الذكاء الاصطناعي هذه إلى تبسيط وجعل عملية حوسبة الأمن السيبراني ذكية على أنظمة الأمن التقليدية. في إطار تقريرنا، يسلط المتهمون الضوء أيضًا على عديد من الاتجاهات للبحث لمساعدة الباحثين على إجراء أبحاث مستقبلية في هذا المجال. الغرض العام هنا هو العمل كنقطة مرجعية وتوجيه للباحثين والممارسين في مجال الأمن السيبراني في الصناعة، لا سيما من وجهة نظر كمبيوتر ذكي أو تكنولوجي من أساس الذكاء الاصطناعي[90].

تم تصميم RMO لتحديد الشبكات ومجال الأمن السيبراني لحساب المعلومات المتعلقة بإمكانية الوصول. مصفوفة الوصول تقرر ما إذا كانت العقدة يمكن أن تصل إلى عقدة أخرى (عبر البروتوكول على طبقات ISO/OSI). وتحدد المنظمة عناصر الشبكة، وتفاصيل إمكانية الوصول إلى الشبكة، وسياسات مراقبة الدخول لتحقيق هذا الهدف. يتضمن RMO أيضًا بعض قواعد SWRL لحساب مصفوفة إمكانية الوصول. بالإضافة إلى قوانين RMO و SWRL، يتوفر أيضًا عدد من استفسارات SPARQL لتحسين حساب مصفوفة الوصول. يعكس RMO نهجًا رائدًا لحساب مصفوفة إمكانية الوصول، على أفضل ما نفهمه. ثم يحدد المتهمون نهجنا على أساس استراتيجية باستخدام مزيج من OWL وقواعد منطق التعريف واستفسارات SPARQL.[91].

سيجعل إنتاج تكنولوجيا المعلومات الآلة تتصرف وتفكر مثل الناس. الذكاء الاصطناعي هو جانب استثنائي من تكنولوجيا المعلومات يتطلب تطوير جهاز كمبيوتر يتفاعل ويعمل كعقل بشري. تشمل

الجوانب الأساسية للذكاء الاصطناعي مقارنة الحواس البشرية. النظام قادر على التعرف على اللمس والكلام كميزات موضوعة داخل النظام لتشغيل الأنشطة المحتملة لحالة الحياة الطبيعية دون مساعدة بشرية. ومع ذلك، فإن الذكاء الاصطناعي هو بحث وكيل الذكاء، الذي يأخذ حالة العالم ويحقق هدفه بنجاح. ومعظم الهياكل الحاسوبية في العالم مبنية لخدمة الأغراض وفقا لجوهر الحالة مع التطبيق الخاص للعناصر البشرية. عادة ما يكون الذكاء الاصطناعي إنسانًا يستخدم طرق استكشاف الأخطاء وإصلاحها ويتعلم فهم المستويات العالية من الأنشطة في تشغيل العناصر المستوحاة من الإنسان وصنع القرار والدورة العاطفية. الذكاء الاصطناعي هو ذكاء قائم على الآلة بدلاً من الذكاء البشري. تقدمت طرق الذكاء الاصطناعي بسرعة في السنوات الأخيرة ويمكن رؤية استخداماتها في عديد من المجالات من التعرف على الوجوه إلى معالجة الصور. ستعمل تقنية الذكاء الاصطناعي على تحسين أدوات الأمن السيبراني والسماح للمعارضين بتطوير أساليب الهجوم في سوق الأمن السيبراني. لكن اللاعبين الخبيثين يدركون الآفاق الجديدة ومن المرجح أن يحاولوا إيذائهم[92].

مع استمرار ارتفاع عدد الهجمات السيبرانية وتعقيداتها، أصبحت تقنيات الذكاء الاصطناعي الموجهة للأمن السيبراني ضرورة. يمكن استخدام تطبيقات الذكاء الاصطناعي مثل التعلم العميق، ومعالجة اللغة الطبيعية لمجموعة واسعة من المهام الأمنية، بما في ذلك الكشف عن التهديدات وتصنيفها، وتقييم الضعف، وإدارة المخاطر. يمكن لخوارزميات تعلُّم الآلة تحليل مجموعات بيانات كبيرة لتحديد الأنماط والانحرافات التي تشير إلى الهجمات السيبرانية، في حين يمكن استخدام التعلم العميق لتطوير نماذج

تنبؤية دقيقة للغاية. يمكن أيضًا لمعالجة اللغة الطبيعية المساعدة في تحديد وتصنيف التهديدات في البيانات غير المهيكلة مثل الرسائل الإلكترونية ومنشورات وسائل التواصل الاجتماعي. ومع ذلك، تطرح الأمن السيبراني المدفوع بتقنيات الذكاء الاصطناعي تحديات جديدة، بما في ذلك الحاجة إلى كميات كبيرة من البيانات عالية الجودة، والمخاطر المحتملة للتحيز في خوارزميات تعلُّم الآلة، وصعوبة تفسير النماذج الذكية المعقدة. يجب معالجة هذه التحديات بشكل جاد لضمان نجاح حلول الأمن السيبراني المدفوعة بتقنيات الذكاء الاصطناعي[93].

على اية حال، نظرًا لأن الجرائم الإلكترونية أصبحت معقدة بشكل متزايد، فإن هناك حاجة إلى مناهج الأمن السيبراني لتكون أكثر قوة وذكاء. سيسمح هذا لآليات الدفاع باتخاذ قرارات في الوقت الفعلي يمكن أن تتفاعل بشكل فاعل مع الهجمات المعقدة. للمساعدة في ذلك، يحتاج الباحثون والممارسون إلى معرفة طرق الأمن السيبراني الحالية. استخدام الذكاء الاصطناعي على وجه الخصوص في مكافحة الجرائم الإلكترونية. ومع ذلك، لا يتم تلخيص الأساليب الذكية الاصطناعية لمكافحة الجرائم الإلكترونية. إن الأساليب الذكية الاصطناعية أسهمت بشكل ملحوظ في الجرائم الإلكترونية خلال تحسين أنظمة الكشف عن التسلل بشكل كبير. كما وجد أنه تم تقليل تعقيد الكمبيوتر وأوقات تدريب النماذج والإنذارات الكاذبة. ومع ذلك، فإن المجال منحرف بشكل كبير. كانت معظم الأبحاث التي تركزت على أنظمة الكشف عن التسلل والوقاية منه وآلات ناقلات الدعم هي التقنية الأكثر انتشارًا المستخدمة[94].

تعقيب

تسهم الجرائم الالكترونيةفى خلخلة العلاقات الانسانية فى كل المجتمعات، خصوصياً حق الانسان فى الحياة والتملك لذلك فهى تمثل خروجاً على القيم الأخلاقية والأعراف والتقاليد التى تقوم عليها المجتمعات، قامت تقنيات الذكاء الاصطناعى بتحسين أدوات الأمن السبيرانى، بل أصبحت ضرورة لمواجهة التهديدات الالكترونية.

الهوامش

(1)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.1.

(2) عبد الناصر حريز :الإرهاب السياسي، مكتبة مدبولى، القاهرة، 1966، ص95.

(3)Nabie Y. Conteh, N. Staton, the Socio-Economic Impact of Identity theft and Cybercrime, Preventive Measures and Solutions, in ed. Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 107.

(4)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.1.

(5) Ibid,p.2.

(6)Pathak,N.: Artificial Intelligence For/NET: Speech, Language, And search: Buliding smart Applications With Microsoft Congnitive Service Apis, press,2017,p.7.

(7) محمد وزيرى:الحاسوب بين الأساس المنطقى والتمثيل المعرفى، رسالة دكتوارة، كلية الآداب، جامعة جنوب الوادى، 2021، ص24

(8) المرجع نفسه، ص21.

(9)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.2.

[10]Alpaydin, E. (2010). Introduction to machine learning (2nd ed.). MIT Press.P. 1.

[11]Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.2.

[12]Ibid,p.2.

[13]Ibid,p.2.

[14]Ibid,p.2.

[15]Sutton, R. S., &Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). MIT Press. P. 1.

[16]Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.2.

[17] جعفر حسن جاسم:التطبيقات الاجتماعية لتكنولوجيا المعلومات، ص192،193.

[18]Stacey Ledger, Morality and machines, Perspectives on computer edicts, London, Jones & Bartlett,1997,p.168.

[19]Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.2.

[20]Ibid,p.3.

[21]Ibid,p.3.

[22]Iafrate,F: Artificial Intelligence And Big Data, John Wiley & Sons, Britain and the United States,2015,p.33.

[23]Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.3.

[24]Ibid,p.3.

[25]Alazab, M., Xu, Z., &Choo, K. R. (2019). Cloud computing-based machine learning systems for cybersecurity. IEEE Cloud Computing, 6(4), 32-39. P.1.

[26]Nabie Y. Conteh, N. Staton, the Socio-Economic Impact of Identity theft and Cybercrime, Preventive Measures and Solutions, in ed. Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 11.

(27)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.4.

(28)Ibid,p.4.

(29)Ibid,p.4.

(30)Ibid,p.4.

(31)Khan, S., &Javaid, N. (2021). Organizational risk assessment of cybersecurity using artificial intelligence: A comprehensive review. Computers & Security, 105, 102250. P. 1

(32)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.4.

(33)Li, X., & Lu, R. (2019). Blockchain and artificial intelligence: complements or substitutes?. IEEE Intelligent Systems, 34(4), 92-96. P. 1.

(34)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.4.

(35)Ibid,p.5.

(36)Ibid,p.5.

(37)Last Codell,(2020) Glolop Brain: Foundation of a Distributod Singularity: 10.100/978-3-030-33730-8-16.

(38)Ibid,p.369.

(39)Ibid,p.369.

(40)Ibid,p.370.

(41)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.5.

(42)Hossain, M. S., Muhammad, G., & Gupta, B. B. (2020). IoT-based cyberattacks prevention systems: Current status and future directions. Computers & Security, 92, 101729. P. 1.

(43)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.5.

(44)Ibid,p.6.

(45)BerendBerendsen: What's the Difference between Artificial Intelligence, Machine Learning And Algorithms?, Nov 15, Https://Widgetbrain.com/Difference-between-Ai-Ml-Algorithms

نقلاً عن فاطمه بدر: التمثيل المعرفى بين الحاسوب والعقل البشرى، رسالة ماجستير، كلية الآداب جامعة المنصورة،2020، ص144

(46) المرجع نفسه، ص145.

(47)Alicia Leslie-Johnes, The Analysis of Top Cyber Investigation Trends, in ed. Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 62.

(48)Nabie Y. Conteh, N. Staton, the Socio-Economic Impact of Identity theft and Cybercrime, Preventive Measures and Solutions, in ed. Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 22.

(49)Alazab, M., &Venkatraman, S. (2018). The role of artificial intelligence in intrusion detection systems. Journal of Information Security and Applications, 38, 1-13. P. 1.

(50)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.5.

(51)Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.6.

(52) Ibid,p.6.

(53) Wang, J., Zhang, X., & Li, W. (2021). Software defined networks security: attacks, countermeasures and challenges. Journal of Network and Computer Applications, 179, 102998. P. 1.

(54) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.7.

(55) Ibid,p.7.

(56) Ibid,p.7.

(57) Ibid,p.7.

(58) Nabie Y. Conteh, N. Staton, the Socio-Economic Impact of Identity theft and Cybercrime, Preventive Measures and Solutions, in ed. Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 19.

(59) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.7.

(60) Ibid,p.8.

(61)Ibid,p.8.

(62) Sengupta, S., Chakraborty, S., & Mukherjee, A. (2021). A survey on artificial intelligence-based cyber security. Journal of Network and Computer Applications, 183, 102983. P. 1.

(63) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.8.

(64) Ibid,p.8.

(65) Gharanfoli, M., &Asghari, H. (2021). The role of artificial intelligence in business-based cyber-security: A survey. Journal of Network and Computer Applications, 185, 103043. P. 1.

(66) C.V. Anchugam, Essential Security Elements and Phases of Hacking Attacks, in ed.Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 107.

(67) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.9.

(77) Al-Qershi, O. M., & Al-Khafaji, Z. A. (2021). Cybersecurity of medical image processing systems: A review. Journal of Medical Systems, 45(5), 52. P. 1.

(78) Alicia Leslie-Johnes, The Analysis of Top Cyber Investigation Trends, in ed. Nabie Y. Conteh, Ethical Hacking Techniques and Countermeasures for Cybercrime prevention, pub in The United Hershery SA, U.S., of Ameriva by IGI Global, 2021, p. 60.

(79) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.9.

(1)Ibid,p.9.

(80) صقر عبد الرحيم، إدوار جاسر: أخلاقيات التعامل مع شبكة الانترنت، مركز تكنولوجيا المعلومات، عمان، الأردن، ص345.

(8). صقر عبد الرحيم، إدوار جاسر ، ص346[1]

(82) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.9.

(83) Kshetri, N., &Voas, J. (2019). Cryptography and artificial intelligence: Complements for cybersecurity. Computer, 52(5), 10-13. P. 1

(84) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.10.

(85) Ibid,p.10.

(86) Liu, Y., Liu, W., &Ning, K. (2019). Wireless communication based cyberattacks and prevention from AI. Journal of Ambient Intelligence and Humanized Computing, 10(1), 139-150. P. 1.

(87) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.11.

(88)Ibid,p.11.

(89) فاطمه بدر : ص145.

(90) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.11.

(90) Ibid,p.11.

(91) Khan, S., &Khattak, A. M. (2020). Deep Learning based Cybersecurity Systems. IEEE Access, 8, 78516-78530.

(92) Feng Tao, Muhammad ShoaibAkhtar and Zhang Jiayuan : The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, published on 07 July 2021, EAI Endorsed Transactions on Creative Technologies,p.12.

(93) Ibid,p.12.

(94)Fernandes, R. A., & Rodrigues, J. J. (2020). AI-Driven Cybersecurity: A Review. IEEE Access, 8, 110923-110946.

(102)Ibid,p.12.