المؤتمر الدولي: "التحكيم الالكتروني وتحديات الامن السيبيراني في الطبعة الثانية "

يوم 20 جويلية 2024

المملكة المتحدة

" علاقة الذكاء الاصطناعي بالوقاية من الجرائم الاليكترونية و الإختراعات السبيرانية "

«The relationship of artificial intelligence to the prevention of electronic crimes and cyber intrusions »

منار طالبي

طالب دكتوراه تسجيل ثاني

جامعة الأمير عبد القادر للعلوم الإسلامية – قسنطينة- الجزائر_ مخبر الدراسات الاقتصادية و المالية الإسلامية

الملخص :

تعرف البشرية منذ القدم التطور عبر العصور في شتى و مختلف المجالات إنطلاقا من تطوير وسائل و أدوات العيش البسيطة من أدوات الصيد و الحصاد إلى التنقل و التداول و غيرها وصولا إلى تكنولوجيات المعلومات و التطور التكنولوجي بمختلف أشكاله المعروفة اليوم و التي من بينها ظهور الذكاء الاصطناعي على مستوى التكنولوجيات الحديثة المستعملة في الأنظمة الحياتية للمجتمعات، فيعتبر الذكاء الاصطناعي سلاح ذو حدين له إيجابيات و له سلبيات حيث يعتبر التحكم فيه وفق ضوابط أخلاقية و قانونية فيتم توظيفه في خدمة الفرد و المجتمع بإلغاء السلبيات التي تتضمنه، و من بين آثاره الإيجابية في خدمة المجتمعات هي إستعماله في الوقاية من الجرائم الاليكترونية و الإختراقات السبيرانية لتحقيق الأمن القومي للمجتمع.

فيعتبر الذكاء الاصطناعي وسيلة آلية متطورة في الحماية للممتلكات و الكشف عن مرتكبي الجرائم بصفة عامة بقدرة هائلة على استداء و تجميع المعلومات بسرعة كبيرة ، فبالاضافة على ذلك الذكاء الاصطناعي يعبر عن تطور تكنولوجي كبير في مجال حفظ خصوصيات الأفراد و معلوماتهم الشخصية و دور ذلك في الوقاية من الجريمة الاليكترونية ، الذكاء الاصطناعي يوفر كشف و تدخل سريع للاختراق السبيراني للمراكز الحساسة في الدول فيمكن الاعتماد عليه في وضع أنظمة وقائية للحماية من الاختراقات السبيرانية و تعزيز الأمن القومي للمجتمعات. و هذا كله من خلال تناول دراسة تهدف الدراسة لابراز الدور الذي يلعبه الذكاء الاصطناعي في تعزيز الوقاية من الجرائم الاليكترونية و

الاختراقات السبيرانية و توفير حماية متينة ضدها و منهجية إستخدام هذه الأنظمة في المكافحة العملية و العلمية لهذه الجرائم.

+الكلمات المفتاحية:

الذكاء الاصطناعي ، الجرائم الاليكترونية ، الاختراقات السيبرانية، المعلومات الاليكترونية.

Abstract :

Since ancient times, humanity has known development throughout the ages in various fields, starting from the development of simple means and tools for living, from hunting and harvesting tools to transportation, trading, and others, all the way to information technologies and technological development in its various forms known today, including the emergence of artificial intelligence on... The level of modern technologies used in the life systems of societies. Artificial intelligence is considered a double-edged sword that has advantages and disadvantages, as it is considered to be controlled according to ethical and legal controls, so it is employed in the service of the individual and society by eliminating the negatives that it contains. Among its positive effects in serving societies are Its use in preventing electronic crimes and cyber-intrusions to achieve national security for society.

Artificial intelligence is considered an advanced automated means of protecting property and detecting crime perpetrators in general, with a tremendous ability to retrieve and collect information very quickly. In addition to that, artificial intelligence expresses a major technological development in the field of preserving individuals' privacy and personal information and the role of this in preventing crimes. Electronic crime, artificial intelligence provides rapid detection and intervention of cyber intrusions into sensitive centers in countries. It can be relied upon to develop preventive systems to protect against cyber intrusions and enhance the national security of societies. All of this is done by examining a study that aims to highlight the role that artificial intelligence plays in enhancing the prevention of electronic crimes and cyber intrusions and providing strong protection against them and the methodology of using these systems in the practical and scientific combat of these crimes.

+Keywords:

Artificial intelligence, electronic crimes, cyber intrusions, electronic information.

المقدمة :

تعرف البشرية منذ القدم التطور عبر العصور في شتى و مختلف المجالات إنطلاقا من تطوير وسائل و أدوات العيش البسيطة من أدوات الصيد و الحصاد إلى التنقل و التداول و غيرها وصولا إلى تكنولوجيات المعلومات و التطور التكنولوجي بمختلف أشكاله المعروفة اليوم و التي من بينها ظهور الذكاء الاصطناعي على مستوى التكنولوجيات الحديثة المستعملة في الأنظمة الحياتية للمجتمعات، فيعتبر الذكاء الاصطناعي سلاح ذو حدين له إيجابيات و له

سلبيات حيث يعتبر التحكم فيه وفق ضوابط أخلاقية و قانونية فيتم توظيفه في خدمة الفرد و المجتمع بإلغاء السلبيات التي تتضمنه، و من بين آثاره الإيجابية في خدمة المجتمعات هي إستعماله في الوقاية من الجرائم الاليكترونية و الإختراقات السبيرانية لتحقيق الأمن القومي للمجتمع.

_ فما هو أثر الذكاء الاصطناعي في الوقاية من الجرائم الاليكترونية و الاختراقات السبيرانية؟

حيث تقودنا الإشكالية السابقة التي ننطلق منها في موضوع دراستنا هذه إلى طرح الفرضيات التالية:

_ يعتبر الذكاء الاصطناعي وسيلة آلية متطورة في الحماية للممتلكات و الكشف عن مرتكبي الجرائم,

_ الذكاء الاصطناعي يعبر عن تطور تكنولوجي كبير في مجال حفظ خصوصيات الأفراد و معلوماتهم الشخصية.

_ الذكاء الاصطناعي يوفر كشف و تدخل سريع للاختراق السبيراني للمراكز الحساسة في الدول.

حيث تهدف الدراسة لابراز الدور الذي يلعبه الذكاء الاصطناعي في تعزيز الوقاية من الجرائم الاليكترونية و الاختراقات السبيرانية و توفير حماية متينة ضدها.

وذلك بالاعتماد على مجموعة من الدراسات السابقة أهمها:

_ دراسة خليل سعيدي و مرزوق بن مهدي حول الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السبيراني هدفت الدراسة لابراز أهمية الذكاء الاصطناعي في تحقيق الأمن السبيراني في ظل بيئة رقمية جديدة,

_ دراسة د/ دولي لخضر و د/ ناصري نفيسة حول دور الذكاء الاصطناعي في مواجهة الجرائم الاليكترونية هدفت الدراسة لابراز ضرورة الحماية الاليكترونية للمعلومات في مختلف الدول و ما يوفره الذكاء الاصطناعي من أنظمة حمائية ذات منهجية سريعة في الكشف عن الجرائم الاليكتونية.

_ دراسة آلان بونيه حول الذكاء الاصطناعي واقعه و مستقبله هدفت الدراسة لتناول العلاقة بين الخبرة البشرية و عالم المعلومات و فعالية أنظمة الذكاء الاصطناعي.

المبحث الأول : علاقة الذكاء الاصطناعي بالوقاية من الجريمة:

يجب ألا يفهم من توضيحنا للاختلاف في النظرة إلى الهدف الأساسي للذكاء الاصطناعي أن البرامج التي تكتب لمحاكاة المنطق الإنساني غير مفيدة وأن لا نفع لها . فالنفع وحده لم يكن هدفا للبحث العلمي، ولا يجب أن يحدد مناهج البحث التي تتبع. ولابد من التأكد أن هذه المناهج قائمة على أسس علمية سليمة قبل طرح كفاءة الأداء للمناقشة.

وهو السعي لفهم الذكاء الإنساني مما يثير السؤال التالي : كيف لنا أن نأمل في محاكاة السلوك الإنساني مع أننا لا نفهم الطريقة التي يعمل بها ومع إدراكنا أن هذا السلوك يختلف باختلاف البشر؟ بيد أنه يمكننا أن نعرف عن يقين بعض الطرق التي لا يتبعها الناس في العديد من المواقف، ويساعدنا هذا على استبعاد بعض الاحتمالات. فلننظر مثلا

إلى مسألة فهم اللغة الإنسانية. من الواضح أننا لا نحتاج إلى قراءة أو سماع عبارة ما عدة مرات لكي نفهم مضمونها . وبالتالي يمكن لنا أن نحكم على أي برنامج يعتمد على تكرار الاطلاع على النص اللغوي بأنه لا يعبر عن الواقع السيكولوجي للعملية اللغوية. ومن الواضح أيضا أننا لا نبدأ فهم جملة ما ببناء شجرة الأعراب أولا ثم نشرع في التحليل الدلالي لها كي نصل إلى معناها. وتشير كل الدلائل إلى أن عمليتي إعراب الجملة وتفسير دلالتها مرتبطان ومتلازمتان، وبالتالي فإن برامج التحليل اللغوي التي سادت في الفترة الأخيرة، والتي اعتمدت على الفصل بين هاتين العمليتين لا تعبر عن طرقنا في فهم اللغة وأنها فصلت بين العمليتين لأن ذلك كان أسهل في البرمجة عن إدماج العمليتين كما يفعل الإنسان. ومن جانب آخر فإنه يمكن للاستبطان Introspection ونتائج التجارب التي يجريها علماء النفس على الأفراد أن تمدنا بمعلومات قيمة عما يمكن للعقل الإنساني أن يحتفظ به بسهولة، وعن أي استنتاجات يمكن أن يخرج بها العقل الإنساني مما يقرأ أو يسمع؟ وأي توقعات للقارئ أو السامع تؤكد؟ وأيها يتبين خطؤها ؟ وقت تنبني علاقة وثيقة بين نتائج مثل هذه التجارب والبرامج التي تحاكي هذه العمليات الاستدلالية.

وأخيرا فإن قدرة برامج الذكاء الاصطناعي على تحسين أدائها عن طريق التعلم لهو مؤشر جيد على مدى ملاءمة نظم البرمجة المستخدمة المحاكاة العمليات الاستدلالية لدى الإنسان. كما أن فشل هذه البرامج في التعلم يعني عدم تناظر العملية الاستدلالية بها للمنطق الإنساني. فكما هو متبع في العلوم، يستمر التسليم بصحة النظرية طالما لم تدحضها التجربة العملية. (الذكاء الاصطناعي واقعه و مستقبله، 1993)

تقدم تقنيات الذكاء الاصطناعي وسائل عديدة في الوقاية من الجرائم ، منها التحذير المبكر من خلال أنظمة المراقبة الذكية التي توفر تحليلاً دقيقاً لانفعالات الأشخاص، وتحليل أماكن وبؤر الجرائم، ومراقبة الأشخاص ذوي التصنيف العدواني وغير ذلك من الميزات التي تقدمها تقنيات الذكاء الاصطناعي. وتكمن الوقاية من الجريمة في اتباع بعض الإجراءات منها، تتبع المشبوهين وأرباب السوابق، ومعرفة تحركاتهم، والحد من نشاطهم، ورصد أوكار الجريمة، ومعرفة المترددين عليها، وملاحظة الظواهر الإجرامية، ومكان نشأتها، ووقت حدوثها، والمتغيرات المستجدة في المجتمع الذي نشأت به استناداً إلى المعلومات الدقيقة المثبتة في سجلاته.

فاستخدام الذكاء الاصطناعي يساعد بجدية في تقليل الجرائم عبر التنبؤ النشط بالجرائم باستخدام آليات المراقبة والتحليل، حيث تساعد تقنيات الذكاء الاصطناعي على كشف الجرائم، والتنبؤ بنسب الإجرام، ونوع الجرائم، والأماكن التي ستشكل بؤراً إجرامية مستقبلاً، وذلك عن طريق خوارزميات برمجية يتم إعطاؤها بيانات محددة، وتقوم بتحليل تلك البيانات والخروج بنتائج غاية في الأهمية تساعد في الاستعداد والوقاية من الجرائم المتوقع حدوثها، ولذلك يجب تشجيع تقنيات الذكاء الاصطناعي في هذا المجال للحد من الظاهرة الإجرامية والوقاية منها، وهذا خير من انتظار وقوع الجرائم وعقاب فاعليها، ثم البحث عن طرق تأهيل ودمج للمجرمين للعودة مرة أخرى بين مواطني المجتمع.

ولا تقتصر أهمية تقنيات الذكاء الاصطناعي في الوقاية من الجرائم البشرية ولكن لها أهمية كبيرة في الوقاية والحد من الجرائم الإلكترونية بما توفره من المراقبة وتحليل المخاطر، والإنذار المبكر وغير ذلك وإن من نافلة القول

الاعتراف بأن استخدام هذه التقنيات سيحد من الجرائم، ولكن سيكون له تداعيات على حرمة الأشخاص وحرياتهم وكرامتهم التي كفلها لهم الإسلام والدساتير المعمول بها في دول العالم. (المديني، 2024)

المبحث الثاني : أثر الذكاء الاصطناعي على الوقاية من الجريمة الاليكترونية:

هناك مجموعة من أمن المعلومات يوفرها نظام الذكاء الاصطناعي وذلك لتفادي الجرائم الاليكترونية أبرزها توفير أمن الأجهزة ، توفير أمن البيانات، توفير أمن الأفراد، توفير الحماية الإليكترونية، تأمين جميع مكونات الشبكة، استخدام التشفير و الشهادات الرقمية و البصمة الاليكترونية و التوقيع الرقمي واستخدام كلمات المرور.

حيث إن الهدف من استخدام الأنظمة الخبيرة المعززة بتقنيات الذكاء الاصطناعي هو تطوير وتحسين عمليات المراقبة وإتخاذ القرارات بحجم تأثوي أكبر من قدرة خبراء أمن المعلومات بالإضافة إلى تحسين عملية إنشاء قاعدة المعرفة بخصوص التهديدات والسياسات والإجراءات والمخاطر المتعلقة بأمن المعلومات وإمكانية تكيف النموذج ودعمه المعالجة الأحداث والبيانات وتصنيفهما والتي تقود إلى إمكانية التنبؤ بالمحمات و تحديد طرق المعالجة المناسبة من قبل وقوعها. وتعد أحد أهم مكونات صميم النظام حسب آراء الخبراء هو القدرة على تطوير نموذج ذكي يقوم بتحليل وربط الأحداث والبيانات فورياً) أي في وقت الحدوث وذلك لزيادة إمكانيات الإكتشاف Intrusion Detection(في تقنيات الأمن: أنظمة كشف الخداع)Detection and Prevention والمنع System) و برامج مكافحة الفيروسات و ترشيح الرسائل الدعائية وأنظمة تقييم نقاط الضعف، فعلى سبيل المثال: النماذج الضبابية (fuzzy models) يجب أن تستخدم في إدارة المخاطر (Risk Management) والتي تعتبر إحدى أهم مراحل إدارة أمن المعلومات.

مجالات الذكاء الاصطناعي:

مع التقدم السريع التكنولوجيا الحاسبات وبفضل كون الحواسب مصممة أصلا لتحصيل وتخزين ومعاملة واستخدام المعلومات من المتوقع أن تصبح تقنيات وتطبيقات الذكاء الاصطناعي جزءا هاما من حياتنا.

حيث أن النظم الخبرة عبارة عن تطبيق حاسوبي تصنع القرارات في المجالات الحقيقية للحياة، معتمد على قاعدة معرفة المثل حية إنسان حمير في المجال المحدد، وتستخدم عادة في حقول الطلب التعليم، القانون ، البيولوجيا

الشبكات العصبونية ، Expert Systemsإلى عدة أجزاء منها : النظم الخبيرة AI يمكن تقسيم محالات تمثيل القدرات الحسية للإنسان ، Natural Languagesفهم اللغات الطبيعية Neural Network وخاصة الرؤية الحاسوبية Computer Vision، الروبوتيك Robotic ، المنطق العالم .Fuzzy logic وغالبا ما تتقاطع هذه الأجزاء فيما بينها .. .. Agentالعميل ، Computer gamesألعاب الحاسب الشبكات العصبونية : وهي عبارة عن نظم تقوم بتمثيل " الذكاء " بواسطة مجموعة من عناصر المعالجة تشابه العصبونات في الدماغ، وتتصل هذه العناصر مع بعضها البعض من خلال شبكة من الوصلات الموزونة بحيث تتم (neurons) معايرة هذه الأوزان من خلال التعليم كما يحدث عادة مع الإنسان . وهذه الوصلات في التقنيات الحالية قليلة جدا مقارنة مع ما هو متوفر في الدماغ حيث يوجد بلايين الموصلات . تطبق نظم الشبكات العصبونية في مجال محدد مثل التعرف على الأشكال. 12 المنطق العالم : وهو

منطق يستخدم - بالإضافة إلى المستويين المنطقيين المعروفين : صبح / نعم أو خطأ لا - مستويات وسيطة مستمرة بينهما مثلا أكثر حرارة، بارد نوعا ما، ... وهو بذلك محاولة لتطبيق طريقة تفكير أكثر شبها بالإنسان في برمجة الحواسب. العميل تتصرف لصالح شخصيات أخرى غالبا Computational Entity وهو عبارة عن شخصية حاسوبية بشرية بشكل مستقل مثلا يمكن لشخص أن يملك عميله الخاص الذي يراقب له المقالات الحديثة على وينتخب له المقالات المفضلة لديه . Usenet مكونات النظم الخبيرة يتألف النظام الخبير عادة من: - 1 End User Interface واجهة ربط مع المستثمر : معلومات، حقائق، قواعد، خيرة يقوم المستثمر باستشارة النظام من خلال واجهة الربط والتي تحدد الطلبات واللغة المطلوب استخدامها، ويقوم

النظام بالاستفسار من المستثمر بواسطة نفس الواجهة ليحصل على المعلومات اللازمة لأخذ القرار.

_2 Knowledge Base -قاعدة معرفة تحتوي قاعدة المعرفة على كل المعارف التي يستخدمها الخبير البشري الحل مشاكل المجال المحدد .

3 . Inference Engine -محرك استنتاجي: يقوم المحرك الاستنتاجي باستخدام الاستنتاجات اللازمة وباستخدام قاعدة المعرفة حتى يصل إلى القرار بالنسبة للمسألة المطروحة.

بطريقة أخرى يمكن القول أن قاعدة المعرفة والمحرك الاستنتاجي يمثلان المعرفة المخزنة في ذاكرة الخبير البشري والقدرات الاستنتاجية التفكيرية له . يحتوي المحرك الاستنتاجي على مجموعة من العلاقات المنطقية والتي يمكن أن تشبه أو لا تشبه أحياناً طريقة التفكير التي يستخدمها الإنسان ، تتميز بعض النظم الخبيرة بإمكانية استخدامها. المعطيات غير كاملة حيث تتضمن قاعدة المعرفة درجة التأكد عند تصميم النظام الخبيرCertainty Degree of

تتكون الأنظمة الذكية من جزئين أساسيين هما:

- 1الجزء الداخلي - الحسابي Computational والذي يمكن تصنيفه إلى أربع أنظمة جزئية:

المعالجة الحسية (Sensory processing) - تستخدم الحساسات كأداة إدخال في الأنظمة الذكية وكأداة

المراقبة العالم الخارجي للنظام والنظام نفسه.

نمذجة العالم أو البيئة World Modeling - تضمن قواعد بيانات معرفية عن عالم النظام و وحدة محاكاته

تقوم ببناء حالة مستقبلية العالم النظام.

إنشاء السلوك (Behavior Generation) - وحدة صنع القرارة تقوم بإختيار الأهداف والخطط وتنفيذ المهام.

-التقييم الذاتي (حكم قيمة) _ تقييم الحالة المدركة للنظام والحالة المتنبأة.

تقوم ببناء حالة مستقبلية العالم النظام. - إنشاء السلوك (Behavior Generation) - وحدة صنع القرار، تقوم بإختيار الأهداف والخطط وتنفيذ

المهام. التقييم الذاتي (Value Judgment)تقييم الحالة المدركة للنظام والحالة المتبأة. -2- الجزء الخارجي التفاعلي Interfacingالمدخلات والمخرجات من وإلى النظام الذكي تكون إما عن طريق حساسات أو مشغلا (actuators) ، والتي تعتبر الأجزاء الخارجية للنظام. طريقة العمل: تقوم المعالجة الحسية بمعالجة البيانات المسجلة من الحساسات للحصول على النموذج الداخلي العالم النظام وحفظها، ثم يقوم نظام إنشاء السلوك بإختيار سياق التصرفات (actions)لتحقيق الأهداف وتتحكم بالمشغلات المتابعة الأهداف السلوكية ضمن سياق النموذج العالمي المحسوس البيانات الناتجة من الحساسات تعتبر الأساس لبناء قواعد المعرفة واكتشاف الهجمات على النظام وتوقعها قبل حصولها وكذلك القيام باتخاذ القرارات الزمنية الفورية من الأمثلة على بيانات الحساسات تتضمن قياسات مرتبطة بأداء و أمن و حالة ما يلي: الأجهزة مثل أداء وحدة المعالجة المركزية (CPU) و استخدام الذاكرة ومساحة القرص المستخدمة وعدد الملفات المستخدمة في الاتصالات النشطة وعدد محاولات الدخول إلى النظام الفاشلة و عدد العمليات (من استعلامات و تحديثات و حذف و زمن الاستجابة للطلبات و عدد المستخدمين ذوي الامتيازات الداخلين إلى النظام في نفس الوقت و عدد التغييرات في إعدادات النظام وعدد الاتصالات المنتظرة ونسبة استخدام ملفات النظام و مراقبة ساعة النظام (System Clock) و بروتوكولات تزامن ساعة النظام و حجم ملفات سجل النظام وغيرها)Log Files(

الشبكة مثل سعة الاتصال المتاحة (available band widthy والتأخير وطلبات الدخول إلى الشبكة وعدد المصادر الغير متاحة للإستخدام لبعض الوقت و عدد المنافذ المفتوحة وعدد العمليات على شبكة الانترنت والتغييرات في إعدادات الشبكة وعدد الحزم (Packets) الساقطة وعدد رسائل البريد الالكتروني و إستخدام

بروتوكولات الاتصال وغيره

الواجهات مثل إحصاءات الإستخدام

البيئة المحيطة بالنظام مثل درجة الحرارة والإنذارات.

ضمانات الأمن - Security Safeguards (جدار الحماية وأنظمة إكتشاف التدخل و برمجيات الحماية من الفيروسات و الشبكات الشخصية الإفتراضية والتشفير مثل عدد الاتصالات المرفوضة و عدد التحذيرات و أوقات الصيانة وعدد التحديثات البرمجيات و عدد المفاتيح المستخدمة في عملية التشفير وفكها و الدخول عن بعدRemote Access وغيرها

_سياسات الأمن.

خطط حالات الطوارئ و الاسترداد.

نشاطات مدراء الأمن والشبكات (الدخول والتغييرات في الإعدادات وتثبيت البرمجيات وتحديثها و عدد Notification( )Messagesرسائل التبليغ وغيرها

العميل (Agent) هي وحدات حاسوبية تتكرر عدة مرات (عقد) في النظام الذكي خلال عدة مراحل في كل

عقدة (loop) تعالج حساسات الأمن وتحفظ المعلومات في قاعدة البيانات المعرفية للنظام، في كل مرحلة تبنى

خطط وتحدث بأفاق تخطيطية أخرى على سبيل المثال: متغيرات التحكم قد تكون سعة الإرسال للشبكة. هذا

النموذج المبني على تدرج هرمي المتعدد قرارات (multi-resolutional hierarchy) من العقد الحاسوبية ينتج القدرة على تحليل ظواهر التصرف والفهم والإدراك وحل مشاكل النظام وقدرته على التعلم الذاتي، إن تركيبة النظام المقترحة قائمة على بناء إطار عمل (framework) من العملاء الحاسوبيين، بحيث يكون لكل عميل خصائصه وتركيته الخاصة به والتي تستخدم واحدة أو أكثر من تقنيات الذكاء الاصطناعي، مثل معالجة اللغات الطبيعية والشبكات العصبية الذكية والمنطق الضبابي وكذلك تقنيات تنقيب البيانات. بالإضافة إلى الاستفادة من تقنيات البرمجة التقليدية وحزم الحلول الإحصائية لبناء تركيبة هجينة للنظام، إن الفكرة الأساسية من بناء هذا النظام المحين هو تمكين النظام من القيام بمهام وظيفية مختلفة مستقلة بمعايير ومقاييس مختلفة عن الوظائف الأخرى، بالإضافة إلى تكملة نقاط الضعف في أحد النماذج بنقاط القوة في النماذج الأخرى. فعلى سبيل المثال: قد تستخدم الشبكات العصبية الذكية (Intelligent neural network) في تصنيف أنماط إستطلاعات العملاء الحاسوبيين ولكن تمرير المؤشرات الناتجة إلى أنظمة المنطق الضبابي الخبيرة (Fuzzy Logic Expert System) والتي يمكنها ترجمة المخرجات إلى شكل يدركه المستخدم العادي بسهولة.

إلا أن هذه النظم الخبيرة لها خصائص تتمثل في المزايا والعيوب من ناحية مكافحة الجرائم الاليكترونية و الوقاية منها. المزايا:

النظام الخبير غير معرض للنسيان بينما الخبير البشري لا يتمتع بهذه الميزة . يمكن نسخ عدة نسخ من النظام الخبير بسرعة، بينما يشكل تدريب شخص خبير من قبل آخر عملية طويلة ومجهدة. قد يكون بناء نظام خبير بحد ذاته مكلفا غير أن كلفة التطوير والصيانة له يمكن توزيعها على عدة مستثمرين، وبالتالي تكون الكلفة العامة مقبولة مقارنة مع كلفة الإنسان الخبير يعامل النظام الخبير المسائل المتشابهة بنفس الطريقة، بينما يمكن للإنسان الخبير أن يتأثر بشكل أكبر بعدة عوامل منها:

أحدث المعلومات.

أول المعلومات التي حصل عليها.

يمكن للنظام الخبير أن يوثق قراراته بشكل دائم.

إمكانية تجميع خبرة أكثر من شخص في نظام واحد..

العيوب:

يتميز الشخص الخبير بالإدراك يمكن للإنسان الخبير أن يتجاوب مع حالة غير اعتيادية بينما يتعذر على النظام الخبير القيام بذلك، يتأقلم الشخص الخبير مع تغير الظروف بينما يحتاج النظام الخبير إلى تحديث الظروف. كما أن النظم الخبيرة قاصرة عند المشاكل الخارجة عن نطاق خبرتها . كنتيجة يمكن القول أنه في بعض الحالات في برنامج - Bugsمثلا توقع الحالة الجوية أو البحث عن أعطال ما - يمكن للنظام الخبير أن يكون أسرع و أو أدق من الإنسان، ولكن في مجالات أخرى كالطب يكون النظام الخبير مساعدا فعالا - وليس بديلا عن الخبير البشري. (دولي و ناصري، 2018)

المبحث الثالث : أثر الذكاء الإصطناعي في الوقاية من الاختراقات السبيرانية:

للذكاء الاصطناعي دور كبير في تحقيق الأمن السيبراني فمستقبل الأمن السيبراني مرتبط بالذكاء الاصطناعي و مع تزايد الهجمات الالكترونية على المؤسسات والشركات خلال الأعوام الماضية بدا واضحا ان النهج الحالي للأمن السيبراني يعاني ضعفا مزمنا في القدرة على مكافحة التهديدات الالكترونية وفي اعقاب الهجمات الأخيرة التي تمكن فيها قراصنة روس من اختراق عدد من الوكالات الحكومية الأمريكية، ارتفعت أصوات الكثير من الخبراء الأمنيين مطالبة بتغيير جذري في الاستراتيجيات المتبعة لاكتشاف التهديدات الالكترونية والتعامل معها بحيث تستبدل الاعتماد على مجموعات جامدة من البيانات ينماذج ذكاء اصطناعي مرنة وقادرة على فهم السلوك الطبيعي وربما غير الطبيعي للموظفين وفي هذا الاطار اشارت ارتي بركار نائبة رئيس القسم الأمني لدى شركة أي بي ام الى تزايد اعداد الأجهزة المحمولة في مواقع العمل وتحول الشركات الى استخدان تقنيات السحابة الالكترونية أدى الى وجود عدد لا يحصى من الطرق للوصول الى مساحات العمل الافتراضية ما تسبب بالتبعية في تزايد فرص الاختراق الرقمي.

وفي مقال نشرته على الموقع الالكتروني لمجلة فاست كومباني تحت عنوان: مستقبل الامن مرتبط بالذكاء الاصطناعي وليس بكلمات المرور، أوضحت بركار ان هذا الواقع الجديد يفرض علينا من الآن فصاعدا إعادة تصميم الأنظمة الأمنية بحيث لا تعتمد الطرق التقليدية للمصادقة مثل كلمات المرور وانما تلجا الى الذكاء الاصطناعي للتحقق من الهويات والسلوكيات الرقمية مشيرة الى ان عملية تسجيل الدخول يجب الا يتم بعد ذلك دون ان تثار حولها الشكوك.

وأضافت ان احد ابرز التحديات الحالية التي تواجه المؤسسات والشركات للحفاظ على امان مواردها وبياناتها هو تلاشي الخط الفاصل بين من الذي يمكن اعتباره جزءا من فريق الشركة ومن الذي لا يعد كذلك، وذلك وسط تزايد اعداد الموظفين الذين يعملون عن بعد وعمليات الاندماج المستمرة والاعتماد

على تقنيات السحابة الالكترونية، كما اضافت انه في هذا العالم الذي لا يمكن فيه تمييز شخصيات المستخدمين بسهولة لا يكفي أن تكون فعلا من تدعي انه انت، وانما يجب ان تتوافق تصرفاتك مع ذلك أيضا.

حيث يعتبر الذكاء الاصطناعي كبديل لكلمات المرور في حماية البيانات والخصوصيات فترى بركار انه اذا أراد قراصنة الانترنت اختراق فقاعة الذكاء الاصطناعي التي تحمي المستخدم فلن تكون ملاقبة عاداته الرقمية كافية وحدها بل سيحتاجون أيضا الى مراقبة هذا المستخدم جسديا لمعرفة ادق خصوصياته، وأوضحت أن الذكاء الاصطناعي ليس تقنية جامدة فهو يتعلم في الوقت الفعلي ويتطور باستمرار بناءا على البيانات التي يتلقاها ومن ثم فاننا نحتاج الى اجراء تحليلات الملايين التهديدات المحتملة التي تحدث كل يوم، لان الذكاء الاصطناعي يقوم يتحليلها باستمرار ويعمل على اتمتة الاستجابة الأمنية المناسبة لها، وهو ما يحول النظام المني في نهاية المطاف الى أداة استباقية. واختتمت بركار مقالها بالقول ان العصر الذي كانت فيه الأجهزة الموثوقة وكلمات المرور المكونة من 14 حرف كافية لضمان الامن قد انتهى، وينبغي علينا أن نبتكر تقنيات قادرة على التكيف بشرعة لانه مثلما تتغير نماذج العمل على نحو متزايد تتغير كذلك الأساليب والتكتيكات التي يتبعها قراصنة الانترنت لاختراقها. (سعيدي و بن مهدي، 2022)

خاتمة :

الذكاء الاصطناعي يشكل أنظم خبيرة جد متطورة تحاكي السلوك البشري الطبيعي و غير الطبيعي تمتلك أنظمة تطوير ذاتي تمكنها من التعامل مع مختلف الجرائم بأنواعها بالإضافة إلى أنها تشكل أنظمة وقائية ضد مختلف الاختراقات السبيرانية بتحليلاتها المستمرة و أتمتة استجابتها الأمنية.

+ النتائج و التوصيات:

_ الذكاء الاصطناعي عبارة عن آليات حديثة للوقاية من الجرائم بمختلف أنواعها فينبغي تكييفها حسب مختلف المجالات لتؤدي دورها الوقائي من الجرائم بمختلف أنواعها.

_الذكاء الاصطناعي يوفر آليات و أنظمة خبيرة في متنوعة تمثل حواجز اليكترونية في الوقاية من الجرائم الاليكترونية و قواعد بيانات و معلومات تسهل الكشف و التعرف السريع على مرتكبي الجرائم الاليكترونية.

_تحقيق الأمن السبيراني يمر عبر آليات الذكاء الاصطناعي بأنظمته الخبيرة في محاكاة الطبيعة البشرية و تطوير آلياتها باستمرار عن طريق قاعدة المعلومات المكتسبة باستمرار.

قائمة المصادر و المراجع :

Dans .(1993)آ .بونيه ,*الذكاء الاصطناعي واقعه و مستقبله* .(p. 20)الكويت :عالم المعرفة.

دولي ,ل & .,ناصري ,ن ,2018) .ماي .(دور الذكاء الاصطناعي في مواجهة الجرائم الاليكترونية .*مجلة المؤشر للدّراسات الاقتصادية*.65_57 .p , .

سعيدي ,خ & .,بن مهدي ,م ,2022) .جوان .(الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السبيراني .*دراسات في حقوق الانسان*.36_35 .p , .

المديني, م. (2024, مارس). دور الذكاء الاصطناعي في إثبات الجرائم و الوقاية منها _دراسة فقهية_. مجلة الجامعة الاسلامية للعلوم الشرعية, 204_203 .p.