الذكاء الاصطناعي والتعمية الكمومية*

تأليف: بيترراداناليف

جامعة أكسفورد-بريطانيا

ترجمة: أبوبكرخالد سعد الله

المقدمة

التعمية الكمومية هي فرع متقدم من علم التعمية يعتمد على مبادئ ميكانيكا الكم لضمان الاتصالات الآمنة. على عكس التعمية التقليدية، التي تعتمد عادةً على خوارزميات رياضية معقدة لتشفير البيانات، تستخدم التعمية الكمومية الخصائص الفيزيائية للجسيمات الكمومية، مثل الفوتونات، لإنشاء نظام اتصالات آمن بطبيعته.

إن الركيزة الأساسية للتعمية الكمومية هي توزيع المفاتيح الكمومية "تمك" (QKD)، وهي طريقة تمكّن طرفين من إنشاء مفتاح سري مشترك يُستخدم لتشفير وفك تشفير الرسائل بطريقة تضمن كشف أي محاولة للتجسس على الاتصال. ويعتمد أمان توزيع "تمك" على المبادئ الأساسية لميكانيكا الكم، مثل مبدأ عدم اليقين لهايزنبرغ (Heisenberg) والتشابك (intrication) الكمومي.

يقر مبدأ عدم اليقين بأنه لا يمكن قياس نظام كمومي دون التأثير على حالته. وبالتالي، فإن أي محاولة اختراق يقوم بها أحد متصفحي الشابكة أو قياس للمفاتيح

---

* **العنوان الأصلي للمقال:**

Radanliev, P. Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, vol. 15, no. 4, 2024.
https://doi.org/10.1186/s40543-024-00416-6

الكمومية ستُحدث اضطرابات قابلة للكشف، مما ينبّه الأطراف المتصلة إلى وجود اختراق. أما التشابك الكمومي فهو مفهوم أساسي آخر للميكانيك الكمومي. فهذا التشابك يربط بين جسيمين كموميين بحيث تؤثر حالة أحدهما فورًا على حالة الآخر مهما كانت المسافة الفاصلة بينهما. يمكن استخدام هذه الخاصية لإنشاء مفتاح آمن بين طرفين.

تتمثل الفائدة الرئيسية للتعمية الكمومية في قدرتها على توفير قنوات اتصال محصنة ضد الاختراق، مما يجعلها تتفوق على العديد من أساليب التعمية التقليدية، خاصة فيما يتعلق بالقدرة على سرعة إجراء العمليات الحسابية، مثل الحوسبة. ولذلك، تُعدّ التعمية الكمومية مجالًا للدراسة بالغ الأهمية من أجل تأمين البيانات الحساسة في عصر الحوسبة الكمومية.

لقد أصبح التقارب بين الذكاء الاصطناعي والتعمية الكمومية منذ عهد قريب موضوعًا مثيرًا للاهتمام في الأوساط العلمية والتكنولوجية. فكل من هذين المجالين أحدث ثورة في قطاعه: وهكذا مكّن الذكاء الاصطناعي من تحقيق تقدم كبير في مجالات، مثل الرعاية الصحية والتمويل بفضل قدرته الفائقة على معالجة البيانات والتعرف على الأنماط واتخاذ القرارات المستندة إلى البيانات. وفي الوقت نفسه، توفر التعمية الكمومية أمانًا لا يُضاهي يعتمد على القوانين الفيزيائية، لا سيما من خلال تقنيات توزيع المفاتيح الكمومية "تمك" والبروتوكولات ذات الصلة.

إن اقتران الذكاء الاصطناعي والتعمية الكمومية ليس مجرد مصادفة. ففي عصرنا الرقمي الحالي -المتسم بتزايد عمليات نقل البيانات وبتفاقم تهديدات الأمن السيبراني- يبدو من المنطقي دمج قوة الذكاء الاصطناعي الحسابية مع إجراءات الأمان غير القابلة للاختراق التي توفرها التعمية الكمومية. يمكن لخوارزميات الذكاء الاصطناعي، من خلال تحليل كميات هائلة من البيانات، تحسين عمليات التعمية الكمومية وجعلها أكثر قوة وكفاءة. وبالموازاة مع ذلك، يمكن للتعمية الكمومية توفير إطار أمني قوي لحماية أنظمة الذكاء الاصطناعي، مما يضمن عدم تعرض البيانات والخوارزميات التي تديرها للاختراق.

اكتسبت التعمية الكمومية أهمية متزايدة مع الوصول الوشيك للحواسيب الكمومية التي تمتلك القدرة على كسر الشفرات التقليدية خلال فترات زمنية قصيرة، مما يشكل تهديدًا كبيرًا للأمن السيبراني الحديث. لذلك، فإن دمج الذكاء الاصطناعي مع التعمية الكمومية ليس مجرد تمرين أكاديمي، بل هو ضرورة ملحة لمواجهة هذا التحدي الداهم.

تستكشف هذه الدراسة بشكل مستفيض العلاقة بين الذكاء الاصطناعي والتعمية الكمومية. سنحلل بعمق التطورات التاريخية لكلا المجالين، وكذا كيفية تفاعلهما والتحديات والفرص السانحة التي يجلبها هذا التقاطع. كما سنسلط الضوء على التجارب والتطبيقات المهمة في هذا المجال. ذلك أن هدفنا هو تمكين القارئ من الإلمام بالمشهد البحثي الحالي وإبراز الإمكانيات الهائلة لهذا التكامل في المستقبل.

مبرر الدراسة

يمثل التقاء الذكاء الاصطناعي والتعمية الكمومية اتحادًا رائدًا بين مجالين من أكثر المجالات تحولًا وتأثيرًا. لقد غيّر الذكاء الاصطناعي الطريقة التي نعالج بها البيانات ونحللها، في حين توفر التعمية الكمومية مستوى لا مثيل له من الأمان في نقل المعلومات. ومع استمرار تطور هذين المجالين، فإن تقاطعهما يشكّل مجالًا مثيرًا للاهتمام والبحث. تستعرض هذه الورقة البحثية التفاعل بين الذكاء الاصطناعي والتعمية الكمومية، والتطورات المحتملة الناتجة عن هذا التقارب، إلى جانب التحديات التي تواجه هذا الاندماج.

أهداف الدراسة

تهدف هذه الدراسة إلى استكشاف السياق التاريخي للذكاء الاصطناعي والتعمية الكمومية. كما تسعى إلى معالجة وضع البحوث والتطبيقات الراهنة في نقطة التقائها. وسنحلل أيضا التحديات المرتبطة بتكامل الذكاء الاصطناعي

والتعمية الكمومية، ومن ثمّ سنبرز الفرص السانحة والآفاق المحتملة في هذا المجال متعدد التخصصات.

أسئلة البحث

1. كيف تطورت مجالات الذكاء الاصطناعي والتعمية الكمومية عبر التاريخ؟
2. كيف يمكن للذكاء الاصطناعي تحسين بروتوكولات التعمية الكمومية، والعكس بالعكس؟
3. ما هي التحديات الرئيسية في الجمع بين الذكاء الاصطناعي والتعمية الكمومية؟
4. ما الفرص السانحة التي تنشأ عن تفاعل الذكاء الاصطناعي والتعمية الكمومية، وكيف يمكن أن تؤثر على الأبحاث والتطبيقات المستقبلية؟

ستتناول الأقسام التالية هذا التقاطع المثير للاهتمام، مما يوفر توجيهًا للباحثين والمختصين في هذا المجال.

لمحة تاريخية عن الذكاء الاصطناعي والتعمية الكمومية

مقدمة في علم التعمية

يعود أصل دراسة التعمية (cryptoghraphy)، المعروف أيضًا بـ"علم التعمية " (Cryptology)، إلى الكلمات اليونانية kryptósوتعني "مخفي" أو "سري"، وgrapheinوتعني "الكتابة"، وlogia التي تعني "الدراسة". في اللغة اليونانية، تُعرَّف التعمية بأنها "الكتابة السرية" (Liddell 1894).

ترتكز التعمية الحديثة على خوارزميات تشفير مصممة وفقًا لمفهوم "فرضية الصعوبة الحوْسيية "(Computational Hardness Assumption, Braverman et al. 2015). يجد هذا العلم تطبيقاته في العديد من المجالات، مثل بطاقات الدفع الذكية، والعملات الرقمية، وكلمات مرور الحواسيب، والاتصالات العسكرية (Paar and Pelzl 2009). كما يلعب دورًا حيويًا في مجال الأمن السيبراني حيث يضمن تأمين

الاتصالات عبر التعمية (مثل تقنية "بروتوكول نقل النص التشعبي الآمن"HTTPS وتقنية "السرّية حسنة الجودة" PGP).

في مجال العملات المشفرة والاقتصاد القائم على التعمية، تُعدّ تقنيات "إثبات المعرفة الصفرية" أو "اثبات بلا كشف "(Zero-Knowledge Proofs - ZKP)"، والمفاتيح التعمَوية، ودوال التجزئة التعمَوية، من بين التقنيات الأكثر استخدامًا.

من بين خوارزميات التشفير، نجد "خوارزمية التشفير الثلاثي للبيانات" (DEA - Triple Data Encryption Algorithm3)، المعتمدة على "معيار التشفير المتقدم (AES - Advanced Encryption Standard)". يقوم هذا النظام بتشفير البيانات ثلاث مرات باستخدام "معيار التشفير الثلاثي للبيانات"(DES3)، المستمد من تشفير البيانات "معيار تشفير البيانات"(DES) الذي يستند بدوره على التشفير باستخدام خوارزمية المفتاح المتماثل المعروفة باسم "لوسيفر (Lucifer)" المسماة "خوارزمية تشفير البيانات (Feistel 1971)" (DEA).

ثمة طريقة أخرى شائعة للتشفير هي خوارزمية التشفير بالمفتاح العام غير المتماثل "رش أ" (RSA) التي طورها رون ريفست، وأدي شامير، وليونارد أدلمان (RSA - Rivest-Shamir-Adleman Algorithm)، عام 1978 (Rivest et al. 1978).

إضافةً إلى ذلك، تؤدي أنظمة الامتثال التنظيمي، مثل "محلل التوصيل البيني الفيزيائي" (IPAA) و"اللائحة العامة لحماية البيانات (GDPR)"، و"معايير أمان بيانات صناعة بطاقات الدفع (PCI-DSS)، أدوارًا أساسية في ضمان أمن وسلامة البيانات الحساسة.

التعمية مقابل الأمن السيبراني

خلال السنوات الأخيرة، كان معظم التطور الذي أُنجِز في حقل التعمية موجَّهًا نحو تعزيز الأمن السيبراني. في هذا القسم القصير من الدراسة، نسلط الضوء على نقاط القوة والضعف في تطبيقات التعمية الحديثة في المجال السيبراني.

1. نلاحظ قبل كل شيء أن نجاعة التعمية ترتبط بتعقيدات المسألة الرياضية

التي يستند إليها. بمعنى أن قوة التشفير تعتمد على قدرة الخوارزمية التشفيرية في موضوع حل المسألة الرياضية.

2. يتعلق العامل الثاني بجودة التنفيذ حيث إن أي خلل في تنفيذ الخوارزمية قد يُعرِّض النظام بأكمله للاختراق.
3. أما المطلب الثالث فهو مستوى السرية ذلك أن مفاتيح التعمية يجب تخزينها في بيئة آمنة، وعادة ما يكون ذلك لدى سلطة مركزية موثوقة. هبْ أنك قرصان إلكتروني تحاول اختراق نظام تعمية. في هذه الحالة، ستبدأ بمحاولة حل المسألة الرياضية بالبحث عن ثغرات في تنفيذ الخوارزمية، أو بمحاولة الوصول إلى المفاتيح السرية.

التعمية الكمومية مقابل التعمية منخفضة الذاكرة

أعلن المعهد القومي [الأمريكي] للمعايير والتكنولوجيا (NIST) عن اختيار خوارزمية "أسكون" (Ascon) كمعيار رسمي للتعمية خفيفة الوزن (Lightweight Cryptography)، المصممة خصيصًا للأجهزة منخفضة الذاكرة، مثل أجهزة إنترنت الأشياء[1](IoT). منذ إطلاق مسابقة هذا المعهد عام 2018، استمر البحث عن أكثر الخوارزميات كفاءةً وأمانًا، ومن المتوقع أن يكون المعيار جاهزًا بحلول نهاية عام 2023[i]. ومع ذلك، من المهم ان نشير إلى أن معاهد أخرى، مثل المنظمة الدولية للتوحيد القياسي (ISO) والوكالة الأوروبية للأمن السيبراني (ENISA)لا تزال في طور تحديد أفضل الخوارزميات المناسبة. ومن المحتمل أن تعتمد هيئات أخرى، تُعنى بالمعايير عبر العالم، من جهود المعهد القومي [الأمريكي] للمعايير والتكنولوجيا. أما الخيار الآخر لتلك الهيئات فهو أن تجري بنفسها هذه العملية، لكن ذلك سيترك بنيتها التحتية لإنترنت الأشياء عرضة للتهديدات السيبرانية.

وفقًا للمعهد القومي للمعايير والتكنولوجيا، فما كان يلفت الانتباه أكثر من غيره في عملية الاختيار هو فعالية هذه الخوارزميات الجديدة: "لقد أظهر معظم المتأهلين للتصفيات النهائية مزايا من حيث الأداء مقارنةً بمعايير المعهد القومي للمعايير والتكنولوجيا على مختلف المنصات المستهدفة، وهذا **دون التسبب في أي**

مشكلات أمنية[2]. " هذا الرأي مثير للقلق بشكل خاص نظرًا لكون المعهد القومي للمعايير والتكنولوجيا يُعدّ من أكثر أطر عمل الأمن السيبراني تحديثًا، وهو معترف به عالميًا بوصفه يمثل إحدى المؤسسات الأكثر تقدمًا. وإذا اعتبرنا أن المنظمات الأخرى المعنية بوضع المعايير لم تبدأ بعدُ بتحديد معيار تعمية بسيطة، وأن هناك العديد من الخوارزميات المتاحة. فذلك يؤكد أن الأمن السيبراني والتعمية مرتبطان ارتباطًا وثيقًا بتوحيد مرجعيات ولوائح الأمن على المستوى العالمي.

أدى طلب تقديم العروض الأولي[3] لمعيار التعمية الخفيفة لدى المعهد القومي للمعايير والتكنولوجيا إلى تقديم 57 حلًا خضعت لمراجعة وتقييم من قبل المعهد. تضمن التعمية الخفيفة نقل البيانات بأمان من وإلى أجهزة إنترنت الأشياء الصغيرة "التي لا حصر لها". وهذا يستدعي إصدار فئة جديدة من خوارزميات التعمية. تعمل معظم الآلات الدقيقة وأجهزة الاستشعار والمشغلات وأجهزة إنترنت الأشياء الأخرى منخفضة الذاكرة المستخدمة لتوجيه الشبكة والاتصالات بطاقة كهربائية ضعيفة. تحتوي هذه الأجهزة على دوائر كهربائية دنيا، مثل الإلكترونيات الموجودة في شارات الدخول بدون مفتاح وعلامات تحديد الترددات الراديوية (RFID) المستخدمة في سلاسل التموين والمستودعات. وللمقارنة نلاحظ أن حتى أبسط الهواتف المحمولة ستكون لها شريحة أكثر فعالية، والميزة الرئيسية لتقنيات إنترنت الأشياء هذه هي تكلفتها المنخفضة وصغر حجمها. تتطلب خوارزميات التعمية الحالية طاقة حسابية وموارد إلكترونية أكبر مما تحتاجه أجهزة إنترنت الأشياء. وبالتالي، فإن نقطة الضعف الرئيسية لجميع أجهزة إنترنت الأشياء مرتبطة بقوتها الأساسية.

تقدم التعمية الكمومية مقاربة فريدة من نوعها مقارنةً بالتعمية الخفيفة، مثل "أسكون"، وهي مقاربة تُلبي احتياجات الأجهزة منخفضة الذاكرة، مثل أجهزة إنترنت الأشياء. تتبع هذه التعمية مبادئ ميكانيكا الكم، وتركز بشكل أساسي على توزيع المفاتيح الكمومية (QKD)، مما يوفر أمانًا يستحيل اختراقه نظريًا.

يركز المعهد القومي للمعايير والتكنولوجيا على "أسكون" لحماية البيانات على الأجهزة الصغيرة لإنترنت الأشياء ذات القدرات الحسابية المحدودة. من ناحية أخرى،

تهدف التعمية الكمومية إلى الاستفادة من الخصائص المميزة للبِتَّات الكمومية (الكيوبِتَّات qubits) لضمان اتصال آمن، بغض النظر عن القدرة الحسابية للجهاز. ومن أبرز عقبات التعمية الكمومية قابليتها للتوسع وتوافقها مع أنظمة الاتصالات التقليدية. ومن ناحية أخرى، يجب أن تحافظ التعمية الخفيفة على الأمان رغم محدودية مواردها الحسابية. ونظرًا لهذه المحدودية، تواجه أجهزة إنترنت الأشياء صعوبات في استخدام خوارزميات التعمية التقليدية. وإذا ما تم تطبيق أساليب التعمية الكمومية المباشرة، فمن المحتمل أن تواجه هذه الأجهزة صعوبات أكثر تعقيدا.

لقد مهد التقارب بين المجالين الكلاسيكي والكَمومي الطريق لتطوير تقنيات تعمية هجينة توفر إجراءات أمان مُحسّنة، حتى على الأجهزة منخفضة الطاقة. وقد صُممت هذه الحلول لدمج نقاط قوة كلٍّ من الأنظمة الكلاسيكية والكَمومية، ذلك ما يضمن أقصى حماية للبيانات والمعلومات الحساسة. ومن خلال الاستفادة من الخصائص الفريدة لميكانيكا الكم، تستطيع خوارزميات التعمية الهجينة التغلب على قيود التعمية الكلاسيكية، وتوفير مستويات أمان متقدمة تُعدّ أساسية في العصر الرقمي الحالي.

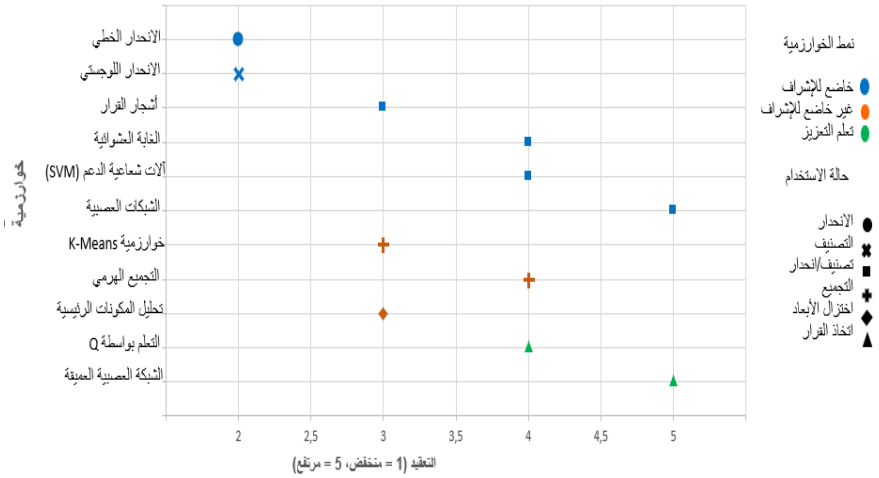
مراجعة التقدم الحاصل في مجال الذكاء الاصطناعي

على الرغم من أن مفهوم الآلات والتماثيل التي تحاكي الفكر والسلوك البشري موجود في الأساطير والخرافات القديمة، فإن المجال العلمي للذكاء الاصطناعي ظهر في منتصف القرن العشرين. لقد وضع عالم الرياضيات البريطاني آلان تورينغ Alan Turing في عام 1950 "اختبار تورينغ" كمعيار لقياس قدرة الآلة على إنجاز أعمال ذكية مطابقة لأعمال الإنسان.

شهدت الأبحاث في مجال الذكاء الاصطناعي، على مرّ السنين، فترات من التذبذب أطلق عليها أحيانا "شتاء الذكاء الاصطناعي" و"ربيع الذكاء الاصطناعي". خلال ستينيات القرن الماضي، ساد التفاؤل والتمويل للذكاء الاصطناعي حيث أظهرت خوارزميات حل المشكلات وتمثيل المعارف إمكانات معتبرة. ومع ذلك، سرعان ما ظهرت قيود حسابية وصعوبات في محاكاة الذكاء البشري. ثم شهدت ثمانينيات القرن الماضي انتعاشًا مع تطوير ما يُعرف بالنُظم الخبيرة (expert systems) التي تحاكي مهارات اتخاذ

القرار البشري. ومع ذلك، بحلول نهاية ذلك العِقد، أصبحت عيوب هذه النُظم أكثر وضوحًا. يمكننا من خلال الشكل 1 مقارنة تعقيد الخوارزميات المختلفة بالعين المجردة.

مقارنة خوارزميات التعلم الآلي



الشكل 1. التنقل عبر خوارزميات التعلم الآلي الشائعة والتقليدية

نلاحظ أن بعض الخوارزميات الأكثر تعقيدًا الموضحة في الشكل 1 لم تكن موجودة في ثمانينيات القرن الماضي. وقد شهد القرن الحادي والعشرون تقدمًا جليا في موضوع القدرة الحاسوبية وإمكانية الوصول إلى البيانات. وبفضل التعلم الآلي والتعلم المكثف، أصبحت الآلات قادرة على التعامل مع مجموعات بيانات ضخمة وأداء مهام مثل التعرف على الصوت والصور بمهارة. ونتيجة لذلك، أصبح الذكاء الاصطناعي عنصرًا أساسيًا في التقدم التكنولوجي الحديث.

مراجعة التقدم الحاصل في التعمية الكمومية

يعود تاريخ التعمية الكمومية إلى أوائل القرن العشرين. فقد طرحت ميكانيكا الكم تحدياتٍ وفرصًا لمعالجة المعلومات نظرًا للخصائص غير المألوفة التي ظهرت في النُظم الكمومية، مثل التراكب والتشابك.

خلال سبعينيات وثمانينيات القرن الماضي، شهدت نظرية المعلومات

الكمومية تطورات لافتة. قدّم تشارلز بينيتCharles Bennett وجيل براسارد Gilles Brassard مفهوم توزيع المفاتيح الكمومية عام 1984 من خلال بروتوكول عُرف باسمBB84"[ii]"، استنادًا إلى أبحاث سابقة في ميكانيكا الكم ونظرية المعلومات. استخدَم هذا البروتوكول مبادئ ميكانيكا الكم حتى يسمح لطرفين بإنشاء مفتاح عشوائي سري مشترك وآمن وفقًا للقوانين الفيزيائية.

في السنوات التي تلت ذلك، شهدت التعمية الكمية تطورات محسوسة في الجانب النظري كما في الجانب العملي. ففضلا عن موضوع التوزيع البالغ الأهمية، توسع نطاق بروتوكولات التعمية الكمومية ليشمل التوقيعات الرقمية الكمومية والاتصالات المباشرة الآمنة. ومع التقدم في علم الفوتونيات (Photonics)[iii] وفي التقنيات الكمومية، طُبّقت هذه البروتوكولات واختُبرت في سيناريوهات واقعية، وهو ما فتح آفاقًا لشبكات تجارية خاصة بالاتصالات الكمومية الآمنة.

وعلى الرغم من أن نشأة الذكاء الاصطناعي والتعمية الكمومية منبثقة من تقاليد علمية مختلفة، فإنهما تقاربا بفضل الاعتماد على معارف أساسية وتطورات تكنولوجية، وسعي مستمر نحو التعمق في المفاهيم وأدوات الابتكار. ويطرح هذا التقارب فرصًا وتحديات عديدة من شأنها أن تُحدث نقلة نوعية في أمن المعلومات والذكاء الحاسوبي.

مراجعة تكامل الذكاء الاصطناعي والتعمية الكمومية

لقد كان للتطورات التكنولوجية في مجال الذكاء الاصطناعي والحوسبة الكمومية أثرٌ بالغ أدى إلى تغييرات جوهرية في مجالات مُختلفة، منها التعمية. ومن الأهداف الرئيسية لدمج الذكاء الاصطناعي والتعمية الكمومية استغلال قدرات هذا الذكاء الحسابية لتعزيز كفاءة نُظم التعمية الكمومية وأمنها ومتانتها. ذلك أن منهجيات الذكاء الاصطناعي قادرة -بفضل قدرتها على معالجة كميات هائلة من البيانات، والتعرف على الأنماط المعقدة، والتكيّف مع السيناريوهات الجديدة- على المساهمة بشكل كبير في تحسين بروتوكولات التعمية الكمومية وإيجاد الحلول للتحديات المُعقدة التي تواجهها.

وبالموازاة مع ذلك، توفر التعمية الكمومية وسيلةً فريدةً لحماية نُظم الذكاء

الاصطناعي، وهذا نظرًا لأمانه الأساسي القائم على قوانين ميكانيكا الكم. ويأتي هذا التكامل الوجيه في وقته المناسب ونحن نعيش عصر الرقمنة الذي يتميز بتبادلات مكثفة للبيانات وبتهديدات متزايدة للأمن السيبراني. وهنا، يبرز دور الذكاء الاصطناعي بشكل جليّ. فمن خلال تحليل وتفسير مجموعات البيانات الضخمة، يمكن لخوارزميات الذكاء الاصطناعي أن تؤدي دورًا محوريًا في تعزيز أمن وفعالية ممارسات التعمية الكمومية.

ومع ذلك، فقد طرح ظهور الحواسيب الكمومية تحديًا جديدًا بالغ الخطورة لنظم التعمية: إنه "التهديد الكمومي". يخيّم هذا التهديد على طرق التعمية التقليدية لأن الحواسيب الكمومية قادرة على اختراق العديد من خوارزميات التعمية المستخدمة حاليًا. وهكذا يتضح أن تآزر الذكاء الاصطناعي والتعمية الكمومية ليس مجرد مسعى أكاديمي، بل يمثل تطورا ضروريا في مقاربتنا للأمن الرقمي. تهدف منهجيات التعمية الكمومية المعتمدة على الذكاء الاصطناعي إلى استباق التهديد الكمومي والتخفيف من حدته والدفاع ضده بفعالية، ومن ثمّ ضمان مستقبل معلوماتي آمن.

تحاول هذه المراجعة استكشاف التفاعل بين الذكاء الاصطناعي والتعمية الكمومية، مستعرضة تطورهما التاريخي والتحديات التي يطرحها ظهور الحوسبة الكمومية والإمكانات التحويلية لدمجها مع الذكاء الاصطناعي. وهكذا تهدف الحوسبة الكمومية إلى توفير فهم شامل للمشهد الحالي والآفاق الواعدة التي يوفرها هذا الاندماج متعدّد التخصصات لمستقبل الحوسبة الآمنة.

مراجعة التهديد الكمومي

يشير "التهديد الكمومي" إلى الضعف المحتمل لنُظم التعمية الحالية في مواجهة قدرات الحوسبة الكمومية المتقدمة. تعتمد طرق التعمية مثل"RSA"[iv] و"ECC" تعمية المنحنى الناقصي (Elliptic Curve Cryptography) على الصعوبة الحسابية لمسائل رياضية محددة. على سبيل المثال، تعتمد خوارزمية "RSA"على صعوبة تفكيك الأعداد الأولية الكبيرة، بينما تعتمد خوارزمية "ECC" على تعقيدات حلّ مسألة اللوغاريتم المتقطع على منحنى ناقصي. هذه المسائل، التي تُعدّ حاليًا صعبة المعالجة على الحواسيب التقليدية، يمكن حلها بفعالية بواسطة الحواسيب

الكمومية وهذا باستخدام خوارزميات جديدة مثل خوارزمية شورShor [٧].

تعمل الحواسيب الكمومية وفقًا لمبادئ ميكانيكا الكم -مثل التراكب والتشابك- وذلك لمعالجة المعلومات بشكل مختلف عن الحواسيب التقليدية. تتيح هذه القدرة للحواسيب الكمومية إجراء حسابات دقيقة بكفاءة تفوق بكثير كفاءة الحواسيب التقليدية. تُظهر خوارزمية شور أن الحاسوب الكمومي قادر على تحليل الأعداد الكبيرة بشكل أسرع بكثير من أشهر الخوارزميات التي تعمل على الحاسوب التقليدي. ونتيجة لذلك، ستصبح نظم التشفير -التي تعتمد على صعوبة حلّ هذه المسائل لأغراض أمنية- عرضة للخطر بمجرد تطوير حواسيب كمومية قوية.

التهديد الكمومي ليس مجرد انشغال ذي طابع نظري، بل سيكون واقعا على المدى القصير. لذا، يستلزم ظهور الحوسبة الكمومية تطوير نظم تعمية جديدة آمنة ضد الهجمات الكمومية، يُطلق عليها غالبًا اسم التعمية "المقاومة للكم" أو "ما بعد الكم". تهدف هذه النظم إلى استخدام خوارزميات وطرق تعمية لا تستطيع الحواسيب الكمومية اختراقها بفعالية.

يُعدُّ دمج الذكاء الاصطناعي مع التعمية الكمومية استجابةً استراتيجيةً لمواجهة هذا التهديد. إن قدرات الذكاء الاصطناعي المتقدمة في مجال التنبؤات وكذا التعرف على الأشكال كفيلة بمساعدة تطوير واختبار وتحسين خوارزميات مقاومة ضد هجومات الحوسبة الكمومية. وعلاوةً على ذلك، يُمكن للذكاء الاصطناعي أن يُساهم في التقييم الفوري لنظم التعمية وتكييفها، مما يجعلها أكثر مرونةً في مواجهة التطور السريع للحوسبة الكمومية. ولذلك أصبح تقارب الذكاء الاصطناعي والتعمية الكمومية محورا بحثيًا بالغ الأهمية من شأنه أن يضمن أمن البيانات وسريتها في عصر الحوسبة الكمومية.

منهجية البحث

يعتمد هذا البحث على مقاربة نوعية في إطار سياق تفسيري وذلك حتى نستطيع القيام بتحليل عميق للعلاقة المعقدة بين الذكاء الاصطناعي والتعمية الكمومية. مع ظهور أدوات ونظم معلومات موحدة تسعى إلى تعزيز تبادل المعلومات

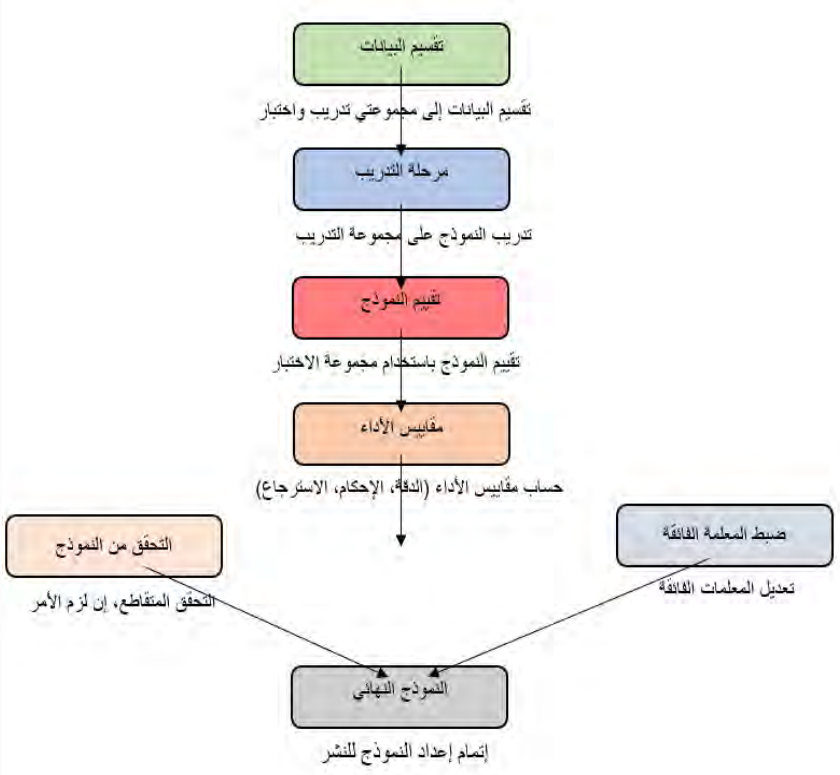
وأتمتة إدارة الثغرات الأمنية، صار مشهد الأمن السيبراني يتطور بسرعة. ومن هذه الأدوات "الأنطلوجيا [vi] المرجعية للمعلومات العملياتية الخاصة بالأمن السيبراني" (Takahashi& Kadobayashi, 2015)، يوفر هذا النظام إطارًا مُهيكلا لمعلومات الأمن السيبراني، ولذا فهو يسهّل تبادلها ضمن نطاق عمليات الأمن السيبراني. وتقترح هذه المقاربة انطولوجيا مرجعية تعزّز التعاون وتبادل المعلومات بين المؤسسات. كما تقوم بتنظيم معلومات الأمن السيبراني بتوافق مع خصوصيات القطاع. وقد تعاون المؤلفان مع مؤسسات الأمن السيبراني لتطوير هذه الأنطلوجيا، وأثبتا سهولة استخدامها من خلال مناقشة نطاق تغطية خصوصيات القطاع. كما أنشأوا بنية معلومات قابلة للتكيّف تستكمل مواصفات خصوصيات القطاع، وتُحدد نمطا أوليًا لقاعدة معارف الأمن السيبراني تُسهل تبادل المعلومات. يستكشف هذا المقال سيناريوهات الاستخدام المحتملة لهذه الانطولوجيا ولقاعدة المعارف في عمليات الأمن السيبراني. تهدف الأنطولوجيا المقترحة إلى تعزيز تبادل المعلومات المتعلقة بالأمن السيبراني.

يُعدّ إطار مشروع "سايبكس" CYBEX[vii] (Rutkowski et al. , 2010) خطوة مهمة نحو وضع معيار عالمي لتبادل معلومات الأمن السيبراني. كمبادرة من "الاتحاد الدولي للاتصالات - قطاع تقييس الاتصالات (ITU-T)، يهدف هذا المشروع إلى توحيد كيفية تواصل كيانات الأمن السيبراني وضمان سلامة هذا التبادل. سيخفض استخدام سايبكس" من تجزئة كمية معلومات الأمن السيبراني، مما يسمح بوضع دفاعي أكثر اتساقًا في جميع أنحاء العالم. يسعى المقال إلى وصف خصوصيات هذا الإطار وتوضيح تطبيقاته العملية وتقدمه. يتميز سايبكس" بهيكلة فريدة حول خمس محاور وظيفية: وصف المعلومات، واكتشاف المعلومات، وتقصّي المعلومات، وضمان المعلومات، ونقل المعلومات. تعمل هذه المحاور معًا على تعزيز أتمتة وأداء عمليات الأمن السيبراني، مما قد يؤدي إلى التقليل من ارتكاب الأخطاء البشرية ومن تكاليف التشغيل. وعلى الرغم من أن هذه الأعمال توفر معلومات قيّمة وتساهم في تحقيق الأهداف العامة لتبادل معلومات الأمن وإدارة الثغرات الأمنية، فإنها لا تمثل المحور الرئيسي لهذه الدراسة. وبالتالي، فإن بحثنا لا يتعمق في هذه المجالات، ولكنه يقرّ بأهميتها في سياق أوسع للأمن السيبراني.

يهدف هذا البحث إلى تعزيز فهمنا لتأثير تقدم هذين المجالين التكنولوجيين على الأمن السيبراني. وتستند الدراسة إلى الجهود العالمية المبذولة لتطوير وتحسين وإنشاء مجموعة من خوارزميات التعمية الكمومية الآمنة(Kumar, September 2022).

جمع البيانات

استخدمنا منهجين أساسيين لجمع البيانات. أولًا، جمعنا البيانات الأولية انطلاقا من المعايير والإرشادات الصناعية (Nist et al. 2016; NIST 2023a, b, 2011; Tabassi 2023; https://www.nist.gov/news-events/news/2018/04/nist-releases- version-11-its-popular-cybersecurity-framework). ثم أجرينا دراسة حالةً حالةً مع المؤلفين والمؤسسات التي تقف وراء هذه المعايير. سُجِّلت هذه التفاعلات، ونُسخت، وشُفّرت بشكل منهجي قبل أن يتم تحليلها بعمق. العملية مُسجَّلة ويمكن مشاهدتها في الشكل 2.



الشكل 2. تقييم نموذج الذكاء الاصطناعي والتحقق من صحته

ثانيًا، راجعنا جلّ ما كُتب في الموضوع من خلال دراسة مقالات المجلات ومتون الكتب العلمية المرموقة. وقد ركزنا على المقالات التي قيّمت بشكل نقدي دور التشفير في سياق الذكاء الاصطناعي وميكانيكا الكم (Kop, 2023)، وخاصةً تلك المتعلقة بتطبيقات التكنولوجيا الكمومية (Broadbent et al. , 2015) وتأثيرها المجتمعي، والتي تم دمجها أثناء التحليل (Elaziz et Raheman, 2022).

تحليل البيانات

كان التحليل الموضوعاتي (Yin, 2009a) هو الطريقة الأساسية لتحليل التفاعلات بين المعايير الوطنية والدولية. في البداية، تم توليد رموز تمهيدية انطلاقا من معالجة دقيقة للتفاعلات (Eisenhardt, 1989)ثم تم فرز تلك الرموز وترتيبها ضمن موضوعات أكثر شمولاً. لقد كانت عملية تحليل مفصلة وتكرارية تطلبت مراجعة مستمرة للبيانات بهدف ضمان تمثيل دقيق (Yin, 2009b). وعلاوة على ذلك، تم دمج معلومات قيّمة -مأخوذة من الأدبيات الأكاديمية- في التحليل (Eisenhardt, 1989)، مع التركيز بشكل صريحً على التأثير المجتمعي لتطبيقات التكنولوجيا الكمومية (Alyami et al. , 2021).

إجراءات التصديق

حتى نتأكد من موثوقية نتائج بحثنا، استخدمنا تقنية التثليث لتقييم أمان البرمجيات من خلال تقنيات الحوسبة الكمومية، مثل عامل الديمومة (Alyami et al. , 2021)، والمقاربة الهجينة الضبابية المعروفة بالرمز "ANP-TOPSIS" [viii] (Agrawal et al. , 2020)، وإطار صنع القرار المتكامل القائم على الطريقة الضبابية المتردّدة، وهذا لتقييم الطاقة المستدامة والمتجدّدة (Sahu et al. , 2023). يستوجب ذلك التحقق من الرؤى التي استخلصناها من تفاعلات الدراسات حالة بحالة مع الاستنتاجات المستنبطة من المؤلفات العلمية. وعلاوة على ذلك، عاينّا أوراقًا بحثية تمت مراجعتها من قبل الأقران، وقيّمنا أجزاء بيانات محددة والتحليلات المتعلقة بها. كانت إسهامات هذه البحوث محورية في موضوع تأكيد نتائج البحث ومواءمتها مع نقاشات أكاديمية أوسع.

مراجعة التفاعل بين الذكاء الاصطناعي والتعمية الكمومية

يُمثل تقارب الذكاء الاصطناعي (Ying, 2010) والتعمية الكمومية (Shapna Akter, 2023) تطورًا رائعًا يُتيح إمكانياتٍ واعدة في مجال الأمن المعلوماتي وأمن المعلومات. ويُعدّ هذا التقاطع مقاربة جديدة لتأمين الاتصالات ومعالجة البيانات الذكية من شأنها إحداث ثورة في طريقة إدراكنا للتطورات التكنولوجية واستخدامنا لها. سنتعمق هنا في هذا الاندماج، وسنعالج عن كثب تفاصيله التقنية، وكذا التقدم المُحرز مؤخرًا، والتحديات التي تواجه المعايير التنظيمية. يهدف هذا التحليل الشامل إلى الإلمام بتشعبات هذا المجال المُتطور وبتداعياته المُحتملة على مستقبل التكنولوجيا والأمن.

الذكاء الاصطناعي في التعمية الكمومية

في التعمية الحديثة (Paar & Pelzl, 2009) ، يمكن للمرء أن يجد "صناديق الإبدال[ix] (S-Box)"، وهي هياكل رياضية معقدة تُعدّ مكونات أساسية داخل العديد من خوارزميات المفاتيح المتماثلة. لقد تم إنشاء هذه الصناديق باستخدام دوال بوليانية [x]شعاعية والذكاء الاصطناعي، وبالاستفادة على الخصوص من تقنيات تعتمد على الشبكات العصبية (Nitaj & Rachidi, 2023). تسمح هذه المقاربة التي يسيّرها الذكاء الاصطناعي بعملية تصميم أكثر انسيابية، وتأخذ على عاتقها تحليل خصائص التعمية، مما يؤدي في النهاية إلى تطوير بروتوكولات تعمويّة أكثر أمانًا وأحسن أداءً (Sevilla & Moreno, 2019). وبفضل هذه الطريقة، يتم تحسين سرعة وأداء عملية التصميم (Ying, 2010 ; Diffie & Hellman, 1976) مع ضمان كفاءة بروتوكول تشفير قوي وموثوق (Ayoade et al. , 2022).

تحسين توزيع المفاتيح الكمومية (QKD)

التعمية الكمومية طريقة من طرق الاتصال عالية الأمان، مبنية على مبادئ ميكانيكا الكم. إنها تعتمد على طريقة توزيع المفاتيح الكمومية (QKD)التي تتيح لطرفين تبادل مفتاح عشوائي سري مشترك لتشفير رسائلهما وفك تشفيرها. ويُعدّ

بروتوكول "BB84" [المشار إليه أعلاه] من الأمثلة المعروفة لهذه الطريقة (Shamshad et al., 2022).

يُعدّ توزيع المفاتيح الكمومية طريقةً عالية الأمان، ولكنها ليس بمنأى عن الأخطاء والاختراقات الأمنية. وهنا نلاحظ أن للذكاء الاصطناعي القدرة على تحسين توزيع هذه المفاتيح بطرقٍ متعددة.

أولاً، يُمكن للذكاء الاصطناعي المساعدة في تصحيح الأخطاء، وهو أمرٌ لا مفرّ منه في أي نظام واقعي لهذا التوزيع. فمن خلال التنبؤ بالأخطاء وتصويبها، يستطيع الذكاء الاصطناعي ضمان سلامة المفتاح الكمومي، وهو أمرٌ أساسيٌّ للحفاظ على أمان قناة الاتصال.

ثانيًا، تستطيع التقنيات المدعومة بالذكاء الاصطناعي مراقبة نظم توزيع المفاتيح الكمومية باستمرار للكشف عن أي خروقات أمنية محتملة أو محاولات تنصت. وهذا يُحسّن تحليل العوامل الأمنية ويحمي النظام من الدخلاء والمندسين.

أخيرًا، يمكن لخوارزميات الذكاء الاصطناعي تحسين معدل توليد المفاتيح الكمومية (Ying, 2010) من خلال مراعاة العوامل البيئية وأداء الأجهزة. ويساعد ذلك على توليد أسرع لكمية من المفاتيح تكون أحسن أداء، وهو أمر بالغ الأهمية لقنوات الاتصال عالية السرعة. ومن خلال استغلال تقنيات الذكاء الاصطناعي، يمكن أن يصبح توزيع المفاتيح الكمومية أكثر أمانًا وموثوقية، مما يمهد الطريق لمستقبل واعد في مجال الاتصالات الآمنة.

التعمية الكمومية في الذكاء الاصطناعي: تأمين نظم الذكاء الاصطناعي

في عالمنا اليوم المتطور تكنولوجيًا، يجب على الصناعات التي تعتمد على الذكاء الاصطناعي إعطاء الأولوية لأمن خوارزمياتها والبيانات التي تعالجها. يمكن أن تُسفر خروقات البيانات عن عواقب وخيمة تشمل الحاق الضرر بالسمعة والخسائر المالية. إن إحدى طرق تعزيز أمن نظم الذكاء الاصطناعي هي استخدام تقنيات التعمية الكمومية. تستخدم هذه التقنيات مبادئ ميكانيكا الكم لحماية البيانات من

المهاجمين المحتملين، مما يجعل اختراق النظام معلوماتيا مستحيلًا. بتطبيق هذه التدابير الأمنية المتقدمة، يمكن للصناعات ضمان سلامة نظم الذكاء الاصطناعي الخاصة بها، وكذا أمن البيانات الحساسة التي تعالجها.

المبادئ الكمومية في خوارزميات الذكاء الاصطناعي

تختلف المبادئ التي تحكم عالم فيزياء الكم اختلافًا كبيرًا عن مبادئ الفيزياء الكلاسيكية. يمكن أن تكون هذه المبادئ مصدر إلهام وابتكار لتصميم خوارزميات متقدمة للذكاء الاصطناعي. ومن هذه التقنيات في الحوسبة الكمومية تقنية التشابك الكمومي التي يمكنها تحسين تلك الخوارزميات، وخاصةً في تدريب الشبكات العصبية (Ying, 2010). ويؤدي ذلك إلى إنشاء نماذج للذكاء الاصطناعي أكثر كفاءة وسرعة. كما اكتشف العلماء أنه يمكن الاستفادة من التشابك الكمومي -حيث تتشابك الجسيمات- لتطوير نماذج ذكاء اصطناعي قادرة على معالجة المعلومات بطرق كانت مستحيلة في الماضي. يستطيع هذا التقدم التكنولوجي إحداث ثورة في مجال الذكاء الاصطناعي وتمهيد الطريق لتطبيقات أكثر تطورا.

المشهد التنظيمي والمعايير

طرح دمجُ تقنية الذكاء الاصطناعي مع التعمية الكمومية تحديات جديدة (Kop, 2023) تخص الامتثال للأنظمة والمعايير (Ying, 2010) ولمعالجة هذا الأمر، اجتمعت منظمات دولية مختلفة لوضع إرشادات وبروتوكولات شاملة لضمان موثوقية وأمان نظم التعمية الكمومية. وتهدف هذه الجهود إلى إرساء إطار عمل موثوق لدعم التطوير المستمر ونشر حلول تعتمد على التعمية الكمومية المتقدمة.

تم تحقيق تقدم ملحوظ في خصوصية البيانات والأمان بمساعدة المنظمات البارزة مثل:

"ISO/IEC) "ISO 2022, 2017, 2023; NIST 2023a, b, c, d, e, 2001, f, g, 2022a, b, 2018, 2014, 2011; Tabassi 2023; SWID 2023; Petrov 2021; Udroiu et al. 2022; Catril Opazo 2021; NIST 2020; NIST 800-53 2020; NIST Advanced Manufacturing Office 2013; Johnson et al.2016;https://advisera.com/27001academy/what-is-iso-27001/;

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11- its- popular-cybersecurity-framework; https://csrc.nist.gov/Projects/block-cipher-techniques; https://csrc.nist.gov/Projects/post-quantum-cryptography;
https://csrc.nist.gov/Projects/lightweight-cryptography;
https://csrc.nist.gov/Projects/pec; https://www.nist. gov/cyberframework/getting-started

و. EU/UK GDP" (GPDR, 2023 ; ICO 2023) "قد قدمت هذه الجهات رؤى وإرشادات قيّمة لحماية المعلومات الحساسة، وهو ما عزز ثقة المستخدمين. وبفضل هذه المساهمات، أصبح القطاع مجهزا بشكل أفضل لمواجهة التهديدات والتحديات الناشئة، الأمر الذي مهّد الطريق لمشهد رقمي أكثر أمانًا.

تولّت المنظمة الدولية للمعايير (ISO) واللجنة الكهرو تقنية الدولية (IEC) مهمةً بالغة الأهمية تتمثل في إطلاق مشاريع تهدف إلى توحيد معايير بروتوكولات التعمية الكمومية. ويشمل ذلك إجراءات التأسيس الأساسية التي تضمن النقل الآمن للمعلومات الحساسة والسرية. تضمن هذه المشاريع قبول التعمية الكمومية على نطاق واسع كطريقة موثوقة للاتصال الآمن في مختلف القطاعات، بما في ذلك القطاع المالي والرعاية الصحية والقطاع الحكومي. ومع توحيد معايير هذه البروتوكولات، يمكن للمؤسسات تعزيز ثقتها بأمن أنظمة اتصالاتها، وهو أمرٌ بالغ الأهمية في عالمنا اليوم الذي يشهد تزايدًا في الترابط والتواصل بين الأنظمة.

قام المعهد القومي للمعايير والتكنولوجيا (NIST, 2023a, b) -وهو وكالة اتحادية تابعة لوزارة التجارة الأمريكية- بتطوير معايير ومقاييس شاملة لنظم التعمية الكمومية. تستجيب هذه النظم لمتطلبات أمنية صارمة لحماية المعلومات الحساسة في عصر الحوسبة الكمومية. وتهدف جهود المعهد إلى تعزيز إطار عمل آمن وموثوق للاتصالات والتعمية الكمومية التي ينبغي أن تؤدي دورًا حيويًا في مستقبل الأمن السيبراني.

يُمثل تنظيم الذكاء الاصطناعي مجموعة من التحديات فريدة من نوعها. فبينما تُطرح قضايا التقييس في عالم الكم، يواجه الذكاء الاصطناعي عقبات تنظيمية. وتشمل هذه المخاوف انشغالات بشأن خصوصية البيانات، والاعتبارات

الأخلاقية، والشفافية في صنع القرار. وتتطلب معالجة هذه المخاوف حوارات عالمية حول أفضل السبل لتنظيم الذكاء الاصطناعي. على سبيل المثال، تُوفر اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي إرشادات دقيقة لعمليات صنع القرار المتعلقة بالذكاء الاصطناعي. وهذا يضمن الشفافية وتحمل المسؤولية، وبالتالي الاستخدام المسؤول للذكاء الاصطناعي. إن تحديات تنظيم الذكاء الاصطناعي معقدة ومتعددة الأوجه، ولكنها ضرورية لضمان تطوير هذه التكنولوجيا واستخدامها بشكل آمن ومسؤول.

يُلوّح دمج الذكاء الاصطناعي والتعمية الكمومية بمستقبل واعد، إلا أن هناك عقبات تحول دون نجاح تنفيذه وتطويره والالتزام بالمتطلبات القانونية. إنه من الضروري اعتماد منهجية تعاونية تضمّ الباحثين وصانعي السياسات والمتخصصين في هذا المجال حتى نتمكن من الاستغلال الأمثل للإمكانات التي يتيحها هذا الدمج. لا بد من التعرّف على التحديات والعمل معًا للتغلب عليها ونحن نمضي قدما في تحقيق أهدافنا.

التحديات والفرص السانحة: دمج الذكاء الاصطناعي والتعمية الكمومية

يقدم تقاطع الذكاء الاصطناعي والتعمية الكمومية إمكانيات واعدة. ومع ذلك، فإن تقاطع هذين المجالين الرائدين أمر بالغ التعقيد. دعنا نتحدث هنا عن التحديات والفرص الكبيرة الناتجة عن تكاملهما. على سبيل المثال، أظهر الذكاء الاصطناعي القائم على الشبكات العصبية إمكانيات كبيرة في تحسين نظم التعمية، مع بروز عديد التطبيقات العملية التي تثبت سعة إمكاناته. يعدّ توظيف الشبكات العصبية مثالا بارزا على نجاح تطوير خوارزميات التعمية نفسها. ومن الأمثلة الأخرى، استخدام تقنيات التعلم الآلي لتصميم وتحسين "صناديق الابدال" في التعمية ذات المفتاح المتماثل. تمثل هذه الصناديق مكونات أساسية في العديد من خوارزميات التعمية مثل معيار التشفير المتقدم (AES) حيث تُدخل عاملي اللاخطية والارتباك في عملية التشفير. تستطيع الطرق التي تعتمد على الذكاء الاصطناعي تحليل خصائص صناديق الابدال، مثل اللاخطية والتوحيد التفاضلي، لتطوير خوارزميات أكثر أمانًا وكفاءة في مجال التعمية.

هناك تطبيق آخر في مجال تحليل الشفرات: استُخدمت خوارزميات الذكاء الاصطناعي ونماذج التعلم العميق لإجراء تحليل تشفير آلي على خوارزميات تعمية متنوعة. من خلال تدريب الشبكات العصبية بأمثلة من النص العادي والنص المشفر المقابل، يمكن لهذه النماذج تعلم التنبؤ بالمفتاح أو فك تشفير الرسائل بدون المفتاح، وبذلك يتم استكشاف مواطن الضعف المحتملة في خوارزميات التعمية.

يؤدي الذكاء الاصطناعي القائم على الشبكات العصبية -فضلا عن تعزيز نظم التعمية التقليدية- دورًا محوريًا في مواجهة تحديات الحواسيب الكمومية. تستغل هذه الحواسيب ثغرات أمنية محددة في خوارزميات التعمية واسعة الاستخدام. على سبيل المثال، تستفيد خوارزمية شور Shor من قدرة الحواسيب الكمومية على تفكيك الأعداد الكبيرة إلى عوامل أولية بكفاءة، مما يُضعف تشفير "RSA" الذي يعتمد على صعوبة تفكيك حاصل ضرب عددين أوليين كبيرين. وبالمثل، تستطيع الحواسيب الكمومية حلّ مشكلة اللوغاريتم المتقطع بفعالية، وهو ما يُضعف أمان تبادل مفاتيح " ECC " ومفاتيح "ديفي-هيلمان" "Diffie-Hellman".

تنجُم هذه الثغرات من المبدأ الكمومي الخاص بالتراكب (الذي يسمح للحواسيب الكمومية بتقييم احتمالات متعددة في آنٍ واحد) ومن التشابك الكمومي (الذي يُمكّنها من ربط خصائص الجسيمات المنفصلة). تتيح هذه الخصائص للحواسيب الكمومية إجراء حسابات خاصة أسرع بكثير من الحواسيب التقليدية، مما يجعل طرق التعمية الحالية عُرضةً للخطر.

يُعد دمج الذكاء الاصطناعي مع أبحاث التعمية المقاومة للحوسبة الكمومية أمرًا بالغ الأهمية لتطوير خوارزميات جديدة قادرة على مواجهة قدرات الحواسيب الكمومية. على سبيل المثال، يُمكن للذكاء الاصطناعي محاكاة الهجمات الكمومية على خوارزميات التعمية، وهذا ما يُساعد الباحثين على فهم نقاط الضعف والحد منها. وعلاوة على ذلك، يُمكن لتقنيات التحسين المُعتمدة على الذكاء الاصطناعي أن تُساعد في إنشاء خوارزميات تعمية أكثر كفاءة وأمانًا لما بعد الكمّ، مما يضمن استمرار حماية المعلومات الرقمية في عصر الكم.

التحديات: القيود التكنولوجية

توفّر النظم الكمومية قدرات لا تضاهى في موضوع قوة إجراء العمليات الحسابية، إلا أن العديد من القيود التكنولوجية تجعل الاستفادة من هذه القدرات أمرا صعبا (Gill et el. , 2022). وأحد التحديات الرئيسية في هذا المجال هو تصميم نظم كمومية موزعة، الأمر الذي يتطلب تقدمًا كبيرًا في صناعة الأجهزة الكمومية وفي تطوير تقنيات تصحيح الأخطاء (Awan et al. , 2022). لكن، على الرغم من هذه التحديات، لا يزال الباحثون عازمين على استكشاف إمكانات الحوسبة الكمومية وتطوير استراتيجيات جديدة للتغلب على العقبات التي تعترض طريق التقدم.

تحديات البيانات في الذكاء الاصطناعي والانتقال إلى التعمية ما بعد الكم

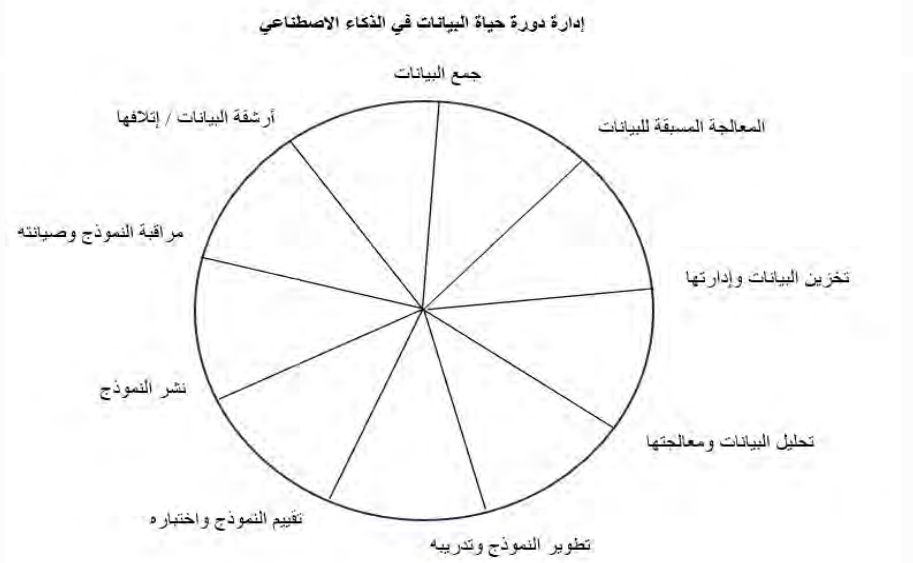
يعدّ دمج نظم الذكاء الاصطناعي مع نظم التعمية الكمومية عملية معقدة مرتبطة بجودة البيانات وحجمها وخصوصيتها وأمانها والانحيازات المحتملة.

تواجه تطبيقات الزمن الفوري[xi] العديد من التحديات في تطبيق التعمية الكمومية التي يديرها الذكاء الاصطناعي. ولا تزال قابلية التوسع والأداء لهذه التقنيات تُمثل تحديًا، خاصةً لتشفير البيانات واسعة النطاق واتصالات الإنترنت. تتطلب نظم التعمية الكمومية بنية تحتية مهمة، وقد تستدعي كما كبيرا من الموارد، وهذا يعقّد عمليات النشر واسعة النطاق. يُعد دمج طرق التعمية الكمومية المتقدمة في نظم الاتصالات الحالية -دون التسبب في اضطرابات على مستوى الخدمات الجارية- أمرًا معقدًا. إنه من الأهمية بمكان أن يتم ضمان التشغيل السلس أثناء الانتقال إلى نظم آمنة كميًا. تتطلب تطبيقات الزمن الفوري مدة استجابة قصيرة جدا، علما أنه من الجائز أن تُسبب خوارزميات الذكاء الاصطناعي المُدمجة مع عمليات التعمية الكمومية في إطالة مدة الاستجابة، وهو ما يؤثر على أداء نظم الزمن الفوري وعلى سهولة استخدامها. تُعدّ نظم التعمية الكمومية حساسة للعوامل البيئية، مما يؤدي إلى ارتفاع معدلات الخطأ، ويُصعّب ضمان الموثوقية والدقة في بيئات مختلفة.

يُعد دمج الذكاء الاصطناعي مع التعمية الكمومية أمرًا ممكنًا، وذلك ما

سيؤدي إلى تطورات كبيرة في أمن التعمية. إن خوارزميات الذكاء الاصطناعي تُحسّن التعمية الكمومية، ومن ثمّ تجعلها أكثر مرونة وأحسن أداء. لقد خففت المقاربات المعتمدة على الذكاء الاصطناعي من الخطر الكمومي بشكل فعال، ففتحت الباب لتطوير وتحسين خوارزميات تعمية مقاومة للظواهر الكمومية. وعلى الرغم من التحديات، فإن نجاح تطبيقات الذكاء الاصطناعي وتطبيقاته المحتملة في تحسين نظم التعمية الكمومية تُنبئ بمستقبل واعد. وتشمل هذه التنبؤات قنوات اتصال آمنة، وسريّة أكثر للبيانات، وحلول أمنية فعّالة لقطاعات مختلفة.

إن الاستمرار في البحث وتطوير هذه الأدوات أمر بالغ الأهمية لمواجهة تحديات تطبيقات الزمن الفوري، وتحسين قابلية التوسع، وتقليص مهلة الاستجابة، وضمان التوافق مع النظم الحالية. وتُؤكد النتائج على ضرورة وضع السياسات وإشراك القطاع الصناعي لتسهيل الانتقال إلى نظم تعمية كمومية آمنة. ويشمل ذلك توحيد الممارسات وسبل العمل، والاستثمار في البنية التحتية، وتعزيز التعاون بين الأوساط الأكاديمية والقطاع الصناعي وصانعي السياسات. يوضح الشكل 3 هذه العملية.



الشكل 3. التحديات المرتبطة بالتعمية الكمومية

في إدارة دورة حياة بيانات الذكاء الاصطناعي

يوضح الشكل 3 التطبيق الناجح للذكاء الاصطناعي في هذا السياق، وهذا يتطلب استخدام طرق تعمية ما بعد الكم، لا سيما مع اقتراب ظهور الحواسيب الكمومية (Aldoseri et al. , 2023). ومع ذلك، يجب دراسة الانتقال إلى هذه الطرق بعناية والتحضير له إذ قد يطرح التوحيد القياسي والقبول الواسع النطاق تحديات كبيرة. ولذلك، فمن الضروري إعطاء الأولوية لتطوير حلول متينة وموثوقة تُعالج هذه المسائل بفعالية وتضمن سلامة البيانات الحساسة وأمنها.

فرص تعزيز آليات الأمن والنظم الكمومية المعتمدة على الذكاء الاصطناعي

قد يؤدي التكامل المحتمل بين قدرات الذكاء الاصطناعي المذهلة في معالجة البيانات مع الأمان المنيع للتعمية الكمومية، إلى ظهور قنوات اتصال فائقة الأمان، ومقاومة للتهديدات الكلاسيكية والكمومية. فنظرا إلى التطورات السريعة في الحوسبة الكمومية، تشير الأدلة المتزايدة إلى أن النظم الكمومية ستتفوق قريبًا على النظم الكلاسيكية من حيث القدرات الحسابية (Ayoade et al. , 2022). يمتلك الذكاء الاصطناعي القدرة على تحسين النظم الكمومية بشكل كبير، وهذا ما يؤدي إلى خوارزميات أسرع وبروتوكولات تعمية مبسطة ذات آثار بعيدة المدى. يمكن لهذه التطورات أن تُحدث ثورة في الاتصالات الآمنة ونقل البيانات. يوفر اندماج المفاهيم الكمومية مع الذكاء الاصطناعي إمكانات عديدة لمجالات بحثية جديدة تجذب تمويلات أكبر في التعمية الكمومية، وتوسع نطاق هذين المجالين إلى آفاق جديدة.

هناك تحديات معتبرة عند دمج الذكاء الاصطناعي والتعمية الكمومية، لكن المكاسب المحتملة هائلة. يستطيع الباحثون استغلال ثروة من الإمكانيات التي تُرسي أسسا لتطورات جديدة في الحوسبة والأمن. كما يمكن لهذه التطورات أن تُحدث ثورة في كيفية تعاملنا مع هذه المجالات، وأن تُؤثر بقوة على المجتمع.

تؤدي التعمية ذات المفتاح العمومي (PK) دورًا حيويًا في هذا الجهد. تستخدم التعمية غير المتماثلة (أو التعمية ذات المفتاح العمومي) مفتاحين مرتبطين

رياضياتيا: مفتاح عمومي ومفتاح خاص. هذه التعمية تختلف عن التعمية المتماثلة، إذ تعتمد على مفتاح واحد للتشفير وفك التشفير. تستخدم التعمية ذات المفتاح العمومي مفاتيح منفصلة لكل عملية. ذلك ما يعزز الأمان ويضمن بقاء البيانات الحساسة آمنة، حتى في حال اعتراض أي جهة للمفتاح العمومي. تتيح التعمية ذات المفتاح العمومي إجراء اتصالات آمنة وميزات تعمية مثل التبادلات الحرجة والتوقيعات الرقمية وتشفير البيانات. يمثل ذلك عنصرا أساسيا في نظم التعمية الحديثة حيث يوفر أمانًا معززًا وقابلية للتوسع والتكيّف عبر مختلف التطبيقات.

يُعدّ توليد التوقيع الرقمي مفهومًا بالغ الأهمية في التعمية. فلتوليد توقيع رقمي، يجب على المُوقّع أولًا إنشاء مفتاحين يتكون من مفتاح خاص ومفتاح عمومي. يُحفظ المفتاح الخاص سرًا ولا يعلم به أحدا أبدًا، بينما يُتاح المفتاح العمومي للجميع. يتم توليد تلبيد (hash) [xii] فريد للوثيقة أو الرسالة المراد توقيعها باستخدام دالة التلبيد (أو دالة البصمة). وتمثل هذه القيمة للتلبيد محتوى الوثيقة بشكل فريد. يتم التوقيع عبر التلبيد عندما يقوم الموقّع بتشفير قيمة التلبيد المُولّدة باستخدام مفتاحه الخاص. بهذه الكيفية يرتبط توقيعه بوثيقة محددة. يولّد تشفير قيمة التلبيد توقيعًا رقميًا مُعَمّى يكون خاصًا بالوثيقة والموقّع.

يُتيح الجمع بين الذكاء الاصطناعي والتعمية الكمومية فرصًا واعدة. ورغم التحديات الكبيرة التي يجب التغلب عليها فإن المكاسب المحتملة هائلة، ومن المتوقع أن تكون آثارها بعيدة المدى. ويمكن لدمج هذين المجالين أن يفتح آفاقًا واسعة تُرسي أسسًا لتطورات جديدة في الحوسبة والأمن. ومن شأن هذا الدمج أن يُحدث ثورة في الاتصالات الآمنة ونقل البيانات، مما يُفضي إلى مجالات بحثية جديدة، ويدفع بآفاق كلا الحقلين إلى آفاق جديدة.

التعمية الكمومية

تمثّل التعمية الكمومية تقنية ثورية قادرة على توفير تدابير أمنية لا مثيل لها تعتمد على مبادئ ميكانيكا الكم. فعلى عكس التعمية التقليدية التي تعتمد على مسائل رياضية معقدة، تستخدم التعمية الكمومية الخصائص التي تتميز بها

الجسيمات الكمومية لإنشاء طريقة تشفير غير قابلة للاختراق. ومن أهم مكونات هذه المقاربة توزيع المفاتيح الكمومية (QKD)الذي يسمح لطرفين بإنشاء مفتاح عشوائي سري ومشترك يمكن استخدامه للاتصال الآمن. وعلاوة على ذلك، يتم كشف أي محاولة للتنصت على الاتصال الكمومي لأن أي اختراق سيؤدي إلى اضطراب في المراسلات الكمومية كاشفًا بذلك عن وجود متسلل. تدعم هذه الميزة الأمان وتزيد في حماية الاتصال بين الطرفين.

دور الذكاء الاصطناعي في الأمن

ازداد دور الذكاء الاصطناعي في الأمن السيبراني أهميةً في الآونة الأخيرة بفضل قدرته على الاستفادة من التعلم الآلي والخوارزميات المتقدمة التي تتعرّف بسرعة على التوجهات العامة والتشوّهات والتهديدات المحتملة ضمن مجموعات البيانات الضخمة. تُعدّ هذه القدرة بالغة الأهمية في عالم تتطور فيه التهديدات السيبرانية باستمرار وتزداد تعقيدًا. لا يقتصر دور الذكاء الاصطناعي على تحديد التهديدات السيبرانية آنيًا فحسب، بل يوفر أيضًا تحليلات تنبؤية لتوقّع نقاط الضعف المحتملة، مما يُمكّن من اتخاذ تدابير أمنية استباقية. وعلاوةً على ذلك، يُمكن للنظم المعتمدة على الذكاء الاصطناعي تحسين عمليات المصادقة، وتبسيط العمليات الأمنية، وتسهيل المواجهة السريعة للتهديدات التي يتم التعرّف عليها. وهكذا، يُحدث الذكاء الاصطناعي اليوم ثورةً في مجال الأمن السيبراني من خلال توفير أداة فعّالة لمكافحة التهديدات السيبرانية وحماية البيانات الحساسة.

دراسات سابقة حول الذكاء الاصطناعي والتعمية الكمومية

هناك بحوث قيد الإنجاز حول العلاقة بين الذكاء الاصطناعي والتعمية الكمومية، وهو مجال دراسة يزداد أهمية يوما بعد يوم. وفي هذا السياق، أظهرت دراسة أجراها أولوالِ آيُوادِ وآخرون (Ayoade, 2022) القدرات الرائعة للحوسبة الكمومية مقارنة بالنظم التقليدية، وهو ما يثبت أهمية إمكانات الذكاء الاصطناعي على المستوى الكمومي. كما تستكشف بحوث غوبتا (Gupta Gupta et al. , 2023) كيف يمكن للذكاء الاصطناعي والتعلم الآلي مساعدة الحوسبة الكمومية في قطاع

الرعاية الصحية. في عام 2019، تناولت مناقشة الطرق التي يستخدمها للتشفير الكمومي لحماية الاتصالات بين طرفين متعارفين من المستمعين الدخلاء، مما يشير إلى صلات محتملة مع التدابير الأمنية التي تعتمد على الذكاء الاصطناعي. تسلّط هذه الدراسات الضوء على أهمية مواصلة الاستكشافات في هذا المجال متعدد التخصصات حيث يمكن للذكاء الاصطناعي والتعمية الكمومية وضع تصميم لمستقبل الأمن السيبراني.

الذكاء الاصطناعي في التعمية

نبذة عن تقنيات الذكاء الاصطناعي في التعمية

لقد أحدث الذكاء الاصطناعي نقلة نوعية في العديد من المجالات، بما في ذلك التعمية. فباستخدام تقنيات التعلم الآلي، يُقدم الذكاء الاصطناعي طرقًا جديدة لمعالجة مسائل التعمية القديمة والجديدة. ويُعدّ الذكاء الاصطناعي القائم على الشبكات العصبية مفيدًا بشكل خاص في تحسين طرق التعمية وتحليل الشفرات (Nitaj & Rachedi, 2023). إن قدرة الذكاء الاصطناعي على تحليل كميات هائلة من البيانات بسرعة تجعله أداة أساسية من شأنها أن تتعرف على أنماط البيانات والتنبؤ بالتهديدات التشفيرية المحتملة، مما يُسهم في تعزيز إجراءات الأمن.

الذكاء الاصطناعي في التعمية التقليدية

في التعمية التقليدية، يُستخدم الذكاء الاصطناعي بشكل رئيسي لتحليل الشفرات. فمن خلال تدريب خوارزميات التعلم الآلي على التمييز بين أنماط البيانات والتشوّهات في البيانات المشفرة، يمكنها توقع مفاتيح التشفير المحتملة وفك تشفير النصوص المشفرة دون الحاجة إلى المفتاح. وعلاوة على ذلك، تُعزز الطرق التي يستخدمها الذكاء الاصطناعي تقنيات التعمية التقليدية، مما يجعلها أكثر مقاومة "لهجمات القوة الغاشمة" [xiii] وغيرها من أساليب فك التشفير التقليدية. وقد شهد دمج الذكاء الاصطناعي والتعمية التقليدية تقدمًا ملحوظًا حيث تُسهم التعمية في تطوير تقنيات الذكاء الاصطناعي، والعكس بالعكس.

الذكاء الاصطناعي في التعمية الكمومية

تنجم عن دمج التعمية الكمومية والذكاء الاصطناعي تحديات وفرص سانحة (Kop, 2023). ومع تقدم تكنولوجيا الحوسبة الكمومية، من الجائز أن تظهر مواطن ضعف في خوارزميات التعمية. ورغم ذلك، يُمكن للقدرات التنبؤية للذكاء الاصطناعي أن تُساعد في التعرّف على تلك الثغرات، وكذا في إنشاء خوارزميات مقاومة للحوسبة الكمومية (Zolfaghari et al.). وفضلا عن ذلك، يُمكن لتقنيات الذكاء الاصطناعي أن تُحسّن إجراءات التوزيع الكمومي الأساسية، مما يضمن اتصالات آمنة في الشبكات الكمومية. نلاحظ أن هذا المجال لا يزال في مراحله الأولى، إلا أنه يمتلك القدرة على إحداث تحولات سريعة في حقل الاتصالات الآمنة.

التعمية الكمومية

مبادئ التعمية الكمومية

يعتمد أمان التعمية الكمومية على مبادئ ميكانيكا الكم، وهو مجال فيزيائي يدرس سلوك الجسيمات تحت الذرية[xiv]. ويعتمد هذا الأمان على مبدأ استحالة نسخ البيانات المحفوظة في الحالات الكمومية أو الوصول إليها دون إحداث اضطراب في حالتها الأصلية. يُعدّ هذا المفهوم الأساسي، المعروف باسم "نظرية عدم الاستنساخ" (no-cloning theorem)، أساسيًا لحماية شبكات التعمية الكمومية (Shapna Akter, 2023).

توزيع المفاتيح الكمومية

يمثل توزيع المفاتيح الكمومية (QKD) طريقة آمنة تستخدم مفاهيم ميكانيكا الكم لإنشاء وتوزيع مفاتيح التعمية على طرفين (Gyongyosi & Imre, 2020 ; Tsai et al. , 2021). ويُعد بروتوكول "BB84" السالف الذكر أحد أكثر البروتوكولات استخدامًا في هذا النوع من المفاتيح التي تكمن ميزتها الأساسية في قدرتها على اكتشاف أي محاولات للتنصت: إذا ما حاول طرف ثالث اعتراض المفاتيح الكمومية المتبادلة، فسيحدث اضطراب في الحالات الكمومية المرسلة. ذلك ما سيؤدي إلى تنبيه الطرفين المتواصلين فورًا باحتمال حدوث خرق أمني (Diamanti et al. , 2016).

بروتوكولات التعمية الكمومية

هناك تطبيقات متنوعة لبروتوكولات التعمية الكمومية إلى جانب تقنية التوزيع الكمومي للمفاتيح. نشير، على سبيل المثال، إلى التوقيعات الرقمية الكمومية، والسحب العشوائي الكمومي[xv]، والاتصال الكمومي المباشر الآمن. تستخدم هذه البروتوكولات ميكانيكا الكم لأداء مهام يستحيل تنفيذها باستخدام التعمية التقليدية، وهو ما يضمن إجراءات أمنية أكثر متانة (Broadbent et al. , 2015).

تحديات وحلول

يُقدم مفهوم التعمية الكمومية إمكانيات جديدة للاتصال الآمن، ولكنه يُواجه أيضًا مجموعة من التحديات الخاصة. من الناحية العملية، يُعدّ استخدام توزيع المفاتيح الكمومية صعبًا بسبب ظهور بعض العقبات، مثل فقدان القنوات الكمومية، والضوضاء، ومحدودية الأدوات التكنولوجية (Lovic, 2020). ومع ذلك، يعمل الباحثون بنشاط على تجاوز هذه الثغرات. وفي هذا السياق، تُوفر التعمية ما بعد الكمومية (PQC) [xvi] خوارزميات قادرة على الصمود أمام التحديات الكمومية، وهو ما يُسهم في سدّ الفجوة بين تقنيات التعمية الكلاسيكية والكمومية (Tsai et al. , 2021).

تقاطع الذكاء الاصطناعي والتعمية الكمومية

النهج التآزري

يُتيح التقارب بين الذكاء الاصطناعي والتعمية الكمومية فرصًا سانحة غير مسبوقة لإجراء عمليات حسابية آمنة وتحسين بروتوكولات التعمية. ومع تزايد تعقيدات نماذج الذكاء الاصطناعي، تكتسب الخوارزميات الكمومية الآمنة أهمية بالغة. كما تُوفر الحوسبة الكمومية منصةً لخوارزميات الذكاء الاصطناعي قادرة على معالجة كميات هائلة من البيانات خلال مدة حدودياتية[xvii]، ذلك ما يُمكّن من تنفيذ عمليات الذكاء الاصطناعي بسرعة وفعالية أكبر.

الذكاء الاصطناعي لتحسين بروتوكولات التعمية الكمومية

يمكن تحسين بروتوكولات التعمية الكمومية، مثل بروتوكول"BB84"،

باستخدام قدرات التعلم الآلي للذكاء الاصطناعي (Shor, 1994). ومن خلال تحليل الحالات الكمومية والتنبؤ باحتمال التنصت، بمقدور الذكاء الاصطناعي أيضا تعديل عوامل توزيع المفاتيح الكمومية ديناميكيًا لتحسين الأمان. وبالإضافة إلى ذلك، يستطيع الذكاء الاصطناعي المساعدة في تطوير خوارزميات تعمية ما بعد الكمومية ضامنا بذلك مقاومة هجمات الحواسيب الكمومية.

الحوسبة الكمومية لأمن نماذج الذكاء الاصطناعي

يمكن إدخال تقنيات تشفير جديدة عند دمج الحوسبة الكمومية مع الذكاء الاصطناعي، مما يجعل نماذج الذكاء الاصطناعي أكثر أمانًا (Bennett & Brassard, 2020). كما أن البِتّات الكمومية (كيوبتات (qubits تستطيع تمثيل حالات متعددة في آنٍ واحد، مما يوفر مساحة حسابية أوسع للذكاء الاصطناعي يمكن استخدامها من ترقية نظم تشفير تتطور باستمرار. ومن جهة أخرى، بمقدور هذا النوع من التشفير الديناميكي أن يعرقل عمل المهاجمين المحتملين. (Mallow & al. , 2022)

المخاطر المحتملة والتخفيف منها

يُبشّر دمج الذكاء الاصطناعي والتعمية الكمومية بالخير، ولكنه ليس خاليًا من المخاطر. فنظام التشفير الذي يُتطوَّر باستمرار لا يُستبعَد أن تنشأ عنه ثغرات أمنية جديدة أو صعوبات في إدارته. ولذا، من الضروري الموازنة بين الابتكار وإدارة المخاطر، وضمان بقاء الاعتبارات الأخلاقية والأمنية في صلب تطور التكنولوجيات الكمومية.

التطبيقات والتداعيات

حقق التقارب بين الحوسبة الكمومية والذكاء الاصطناعي تقدمًا ملحوظًا في العديد من الحقول العلمية، بما في ذلك مجال التعمية. وقد حسّنت قوة الحوسبة الكمومية منهجيات تشفير خوارزميات الذكاء الاصطناعي، وهو الأمر الذي جعل هذه الطرق أكثر مناعة. وعلاوة على ذلك، يتطوّر التشفير مع ظهور توزيع المفاتيح الكمومية الذي يستغل السمات الفريدة من نوعها التي تتمتع بها ميكانيكا الكم.

وبالإضافة إلى التعمية، تُحدث الحوسبة الكمومية ثورةً في مجال البحوث

الكيميائية الحيوية من خلال توفير إمكانات حسابية متطورة. ذلك أن الحواسيب الكمومية قادرة على محاكاة تفاعلات كيميائية حيوية معقدة، مما يُسهم في تحقيق تقدم طبي كبير.

يحمل دمج الحوسبة الكمومية والذكاء الاصطناعي إمكانات هائلة بمقدورها أن تحدث ثورة في مختلف الصناعات. ومع ذلك، فإن التطوير المستمر لهذه التقنيات يُبرز أيضًا معضلات أخلاقية. فقد تقوم القدرات الكمومية بفكّ شفرة البيانات الحساسة، وهذا ما يُشكّل مخاطر على الحياة الخاصة للبشر، وبالموازاة مع ذلك من الجائز أن يُؤدي التقارب المتزايد بين الذكاء الاصطناعي والتعمية الكمومية إلى تبعات يُمكن استغلالها استغلالًا ضارًا.

للاستفادة القصوى من إمكانات تكامل التعمية الكمومية والذكاء الاصطناعي مع الحد من المخاطر المرتبطة به، يتعيّن على صانعي السياسات إدراك تعقيدات هذه التقنيات بشكل استباقي. ويجب على الهيئات التنظيمية ضمان خصوصية البيانات وأمنها مع حماية حقوق الأفراد ورفاه المجتمع. وتكمن الصعوبة المنتظرة في الموازنة بين الفوائد والمخاطر المحتملة لهذه التكنولوجيات.

وخلاصة القول إن الجمع بين الحوسبة الكمومية والذكاء الاصطناعي يوفر إمكانيات هائلة في مختلف المجالات العلمية والصناعية. لكنه من الضروري مراعاة الاعتبارات الأخلاقية والتداعيات التنظيمية لهذه التكنولوجيات للاستفادة من إمكاناتها على أكمل وجه. ينبغي على أصحاب القرار السياسي والهيئات التنظيمية ضمان خصوصية البيانات وأمنها مع حماية حقوق الأفراد ورفاه المجتمع.

حالات دراسية: تقاطع الذكاء الاصطناعي والتعمية الكمومية

تطبيق الذكاء الاصطناعي في نظم التعمية الكمومية

لقد مهّد التقارب بين الذكاء الاصطناعي وميكانيكا الكم الطريق لأساليب تشفير مبتكرة تعالج بكفاءة سبل مواجهة مخاطر الأمن المتغيرة باستمرار والمعقدة بشكل متزايد (Awan et al. , 2022). فمن خلال الجمع بين قوة الحوسبة الكمومية

وخوارزميات الذكاء الاصطناعي، يمكن لهذه التقنيات حماية البيانات الحساسة بشكل فعال ومنع أي اختراق، مما يضمن أعلى مستوى من الحماية للمعلومات الهامة (Taylor, 2020).

التطبيقات والنتائج الملموسة

لقد حسّن الذكاء الاصطناعي الكمومي حماية البيانات وأمن المعاملات بشكل ملحوظ في القطاع المصرفي. وهكذا غيّرت أساليب الذكاء الاصطناعي تقنيات التشفير فأدى ذلك إلى اعتماد تدابير أمنية أكثر تطورًا لمواجهة التهديدات التي يطورها أهلها باستمرار. غير أن التدابير الأمنية التقليدية لها حدودها، ولذا فإن اكتشاف التهديدات المتقدمة والداخلية بات أمرا صعبًا. وقد استخدم المهاجمون السيبرانيون الذكاء الاصطناعي، وتزييف البيانات، وسرقة النماذج لأتمتة هجماتهم، وهذا ما يضطرنا إلى استخدام تقنيات الأمن السيبراني القائمة على الذكاء الاصطناعي.

من هذه الطرق طريقة CS-FSM"[xviii]" وخوارزمية"[xix] "KNN. تستخدم طريقة "CS-FSM" خوارزمية "معيار التعمية المعزز" (EES) [xx] لتشفير البيانات وفك تشفيرها ضامنة بذلك أمن المعلومات في القطاع المالي. أما خوارزمية "KNN"فتكتشف هجمات البرمجيات الخبيثة وتمنعها من خلال التنبؤ باستخدام بيانات التدريب. كما تُحسّن هذه الطرق أداء نظم الأمن السيبراني فينتج عن ذلك تحسين مقاومتها للهجمات السيبرانية، وتعزيز سرية البيانات، وقابلية التوسع، والتقليل من المخاطر، والمزيد من حماية البيانات، والوقاية من الهجمات.

تم اعتماد الذكاء الاصطناعي الكمومي في قطاع البيع بالتجزئة لتوفير معاملات أكثر أمانًا وفعالية. ومن خلال الاستفادة من قوة هذا النوع من الذكاء، يمكن لتجّار التجزئة حماية بيانات الزبون وضمان معاملات سلسة. كما توفر هذه التقنية حلاً

عالي الموثوقية لحماية معلومات الزبائن الحساسة.

يمكن أن يُفضي دمج الذكاء الاصطناعي وميكانيكا الكم إلى تطورات كبيرة في نظم التعمية. وعلى الرغم من أن التحول إلى نظم التعمية الكمومية له فوائد

عديدة، فإنه لا يخلو من التحديات في التنفيذ نستطيع التغلب عليها بالتخطيط والتنفيذ الدقيقين. إن فوائد دمج الذكاء الاصطناعي الكمومي مع التعمية جلية، لا سيما في قطاعات مثل قطاع البيع بالتجزئة حيث تحسنت حماية بيانات العملاء وأمن المعاملات بشكل ملحوظ.

مناقشة

يوفّر دمج الذكاء الاصطناعي وميكانيكا الكم في نظم التعمية إمكانات هائلة لإحداث ثورة في حماية البيانات وأمن المعاملات في مختلف القطاعات. يُنشئ هذا الدمج نظما أكثر متانة وأمانًا قادرة على مواجهة التهديدات السيبرانية المتطورة، وهو أمر بالغ الأهمية لحماية المعلومات الحساسة. كما يُتيح تطوير تكنولوجيات مبتكرة خاصة بالتعمية وكذا خوارزميات تقاوم التحديات الكمومية.

وحتى نرتقي بهذا المجال، يجب على الباحثين مواصلة الابتكار واستكشاف التداعيات ذات الطابع الأخلاقي لهذه التقنيات، كما يتعيّن البحث في استدامتها. أما صناع القرار السياسي فينبغي عليهم دعم البحث العلمي في هذا الحقل مع ضمان خصوصية البيانات وأمنها من خلال وضع سياسات تُعزز أفضل الممارسات. من جهة أخرى، يجب على المتخصصين في هذا القطاع الاستثمار في البحث والتطوير، ومواكبة أحدث التطورات، وتدريب القوى العاملة على التكيّف مع هذه التكنولوجيات الجديدة. كما ينبغي عليهم المشاركة في صياغة السياسات وتحديد المعايير التي تؤثر على انتشار هذه التقنيات.

إن الفوائد المحتملة الناجمة عن دمج الذكاء الاصطناعي والتعمية الكمومية هائلة وواعدة. إنها تعد بإنشاء بيئة حوسبية آمنة في عصرٍ من المتوقع أن تصبح فيه الحوسبة الكمومية لاعبًا أساسيًا. ومن خلال تعزيز أمن البيانات، يمكن للقطاعات الصناعية زيادة ثقة المستهلكين، وإحداث نقلة نوعية في المعاملات المصرفية الإلكترونية، والتجارة الإلكترونية، والرعاية الصحية، والأمن القومي، والاتصالات.

بشكل عام، يمثّل تقاطع الذكاء الاصطناعي والتعمية الكمومية مجالًا ديناميكيًا متطورًا، يُمكنه أن يُؤمّن نظم التعمية في المستقبل ويعزز الأمن الرقمي العالمي. وبفضل التعاون الدولي في وضع معايير وممارسات عالمية، يُمكننا استكشاف كمّ كبير من الإمكانات التي توفرها هذه التكنولوجيات والارتقاء بأمن البيانات إلى مستوى أعلى.

مستقبل التعمية الكمومية المدعومة بالذكاء الاصطناعي

يجب علينا التعمق في مختلف القطاعات التي تستخدم التعمية الكمومية المدعومة بالذكاء الاصطناعي. وبذلك، يُمكن للباحثين اكتساب فهم أفضل للتحديات والمزايا العملية المرتبطة بكل قطاع. وهذا الوضع يُمكّن، بدوره، من تطوير تطبيقات أكثر فعالية وكفاءة للتعمية الكمومية المدعومة بالذكاء الاصطناعي.

نلاحظ، على ضوء التقدم التكنولوجي الحديث، أنه من الضروري إجراء تحليل شامل للاعتبارات الأخلاقية، لا سيما فيما يتعلق بخصوصية البيانات وإمكانية إساءة استخدامها. يجب أن نأخذ هذه المخاوف على محمل الجدّ، وأن نضمن اتخاذ تدابير وقائية ضد أي عواقب سلبية محتملة لاستخدام التكنولوجيات المتطورة. لذا، من الأهمية بمكان دراسة تداعيات أي تطورات جديدة والتعامل معها بحذر، مع مراعاة تأثيرها المحتمل على الأفراد والمجتمع.

إنه يتحتم علينا التدقيق مليّا في استدامة هذه الآليات ومرونتها، لا سيما في ظل التطورات المستمرة في كلٍّ من الذكاء الاصطناعي وميكانيكا الكم. سيمكننا هذا الفحص الدقيق من ضمان فعاليتها على المدى الطويل وقدرتها على التكيّف مع التطورات المستقبلية.

يمكّن التعاون بين خبراء الذكاء الاصطناعي والفيزياء الكمومية من تعزيز القدرات البحثية. فبدمج خبرات هؤلاء الباحثين، نستطيع تبني مقاربة أكثر شمولا للنهوض بالبحث العلمي. إن إمكانات الذكاء الاصطناعي والتعمية الكمومية تعد بالكثير. كما أن البحث المركز في هذا التخصص، سيمكننا مستقبلا من استغلال هذه التكنولوجيا استغلالا كاملا.

الخاتمة

استكشف نقاشنا العلاقة المعقدة القائمة بين الذكاء الاصطناعي والتعمية الكمومية، موضحا أن دمج هذين المجالين يُمكن أن يحسّن من أداء نظم التعمية ويعزز إجراءات الأمن بفعالية. وقد أدى دمج الذكاء الاصطناعي والتعمية الكمومية إلى تطورات حاسمة في قطاعات مختلفة، مثل الخدمات المصرفية والتجارة الإلكترونية، مما سهّل تطوير بروتوكولات أمنية قوية وعزز ثقة المستخدمين في هذه القطاعات.

يشهد مجال التعمية الكمومية الذي يديره الذكاء الاصطناعي تطورًا سريعًا. فبمقدور الأبحاث قيد الانجاز والتطورات المتوقعة إحداث ثورة في هذا الحقل. وفي هذا السياق، نشير إلى أن نظم التعمية الهجينة، وتصميم بروتوكولات التعمية الآلية، وتحسينات توزيع المفاتيح الكمومية، وتطوير التعمية ما بعد الكمومية، والتعلم الآلي الكمومي لتحليل الشفرات، والحوسبة متعددة الأطراف الآمنة [xxi] (MPC) من أبرز أقطاب الابتكار والتقدم التكنولوجي.

يستكشف الباحثون بنشاط دمج الخوارزميات المقاومة للكم التي يمكن أن تتعرض إليها طرق التعمية التقليدية. وفي هذا السياق، يمكن أن يكون التحسين والتحليل المدعوم بالذكاء الاصطناعي حاسمين في تطوير هذه النظم الهجينة وضبطها بدقة لتحقيق أقصى قدر من الكفاءة والأمان. وتستغل هذه النظم الهجينة نقاط قوة التعمية الكمومية والتقليدية، مما يوفر أمانًا معززًا ضد التهديدات الكلاسيكية والكمومية على حد سواء.

في مجال التصميم الآلي لبروتوكولات التعمية، يُعد الذكاء الاصطناعي، وتحديدًا التعلم الآلي والشبكات العصبية، اتجاهًا بحثيًا واعدًا. تستطيع خوارزميات الذكاء الاصطناعي تحليل كميات هائلة من البيانات لتحديد التوجهات والثغرات المحتملة في بروتوكولات التعمية، وهذا ما يؤدي إلى تصميم نظم أكثر متانة وأمانًا. كما تسمح هذه المقاربة باكتشاف طرق تعمية جديدة مقاومة بطبيعتها للهجمات الكمومية.

نلاحظ أن الأبحاث جارية حاليًا لاستخدام الذكاء الاصطناعي في موضوع

تحسين أداء وموثوقية نظم توزيع المفاتيح الكمومية (QKD). تستطيع خوارزميات الذكاء الاصطناعي القيام بتحسين عملية توزيع هذه المفاتيح، وتقليل الأخطاء، وزيادة معدلات توليد المفاتيح. ويشمل ذلك استخدام الذكاء الاصطناعي في التوزيع التكيّفي للمفاتيح الكمومية حيث تُعدّل عوامل نظام تلك المفاتيح ديناميكيًا استجابةً للظروف البيئية المتغيرة والتهديدات الأمنية المحتملة.

من المتوقع أن يُسرّع الذكاء الاصطناعي تطوير خوارزميات التعمية ما بعد الكمومية. فمن خلال محاكاة الهجمات الكمومية، بمقدور الذكاء الاصطناعي المساعدة في تحديد مواطن الضعف المحتملة في الخوارزميات الحالية والعمل على تصميم نظم تعمية جديدة مقاومة للكم. وقد يؤدي هذا الوضع إلى إنشاء جيل جديد من خوارزميات التعمية القادرة على تأمين البيانات ضد التهديدات الحاسوبية التقليدية والكمومية.

ينطوي مجال التعلم الآلي الكمومي الناشئ، الذي يجمع بين الحوسبة الكمومية وخوارزميات التعلم الآلي، على تطبيقات واعدة في تحليل الشفرات. يمكن للتعلم الآلي المعزز كموميًا تحليل البيانات المشفرة بكفاءة أكبر، مما يؤدي إلى تحليل أسرع وأكثر فعالية للشفرات. كما تستطيع مثل هذه البحوث الاسهام في تقديم إضاءات حول قدرة خوارزميات التعمية في مواجهة تقنيات الحوسبة الكمومية المتقدمة.

نلاحظ، مع التقدم في الذكاء الاصطناعي والتعمية الكمومية، أنه من المتوقع أن تصبح الحوسبة الآمنة متعددة الأطراف (MPC) أكثر متانة وكفاءة. وبوسع الذكاء الاصطناعي أن يساعد في تحسين البروتوكولات والخوارزميات المستخدمة في نوع الحوسبة السابق الذكر، وهو ما يضمن حوسبة آمنة وتعاونية بين أطراف متعددة دون الكشف عن مدخلات بيانات الأفراد.

ورغم ذلك، ينبغي علينا -مع تطور هذه المجالات البحثية- مراعاة التبعات الأخلاقية وضمان توافق تطورات التعمية الكمومية المعتمدة على الذكاء الاصطناعي مع معايير حماية البيانات العالمية والانشغالات ذات الصلة بجانب الخصوصية. وفي هذا السياق، يعدنا مستقبل التعمية الكمومية المعتمدة على هذا الذكاء بتحسين

الأمن وبمزيد من الفعالية في الأداء، لكنه يطرح تحديات ومسؤوليات تتعلق بالاستخدام الأخلاقي وباللوائح التنظيمية العالمية.

حتى نعزّز فهمنا للتعمية الكمومية التي يديرها الذكاء الاصطناعي، ينبغي على الشركات التي يرتبط مصيرها بالنقل الآمن للبيانات تخصيص تمويلات للبحث والتطوير الذي يجمع بين الذكاء الاصطناعي وميكانيكا الكم. فمن شأن ذلك أن يؤدي إلى نظم تعمية أكثر مرونة وقابلية للتكيف. ومن ثمّ، يتم في نهاية المطاف تحسين أمن البيانات. وبالإضافة إلى ذلك، ينبغي على المؤسسات إعطاء الأولوية لتدريب موظفيها على التكيف مع هذه التكنولوجيات المتطورة.

في الختام، يُعدّ الجمع بين الذكاء الاصطناعي والتعمية الكمومية مجالًا واعدًا ذا إمكانات كبيرة في تعزيز أمن البيانات وخصوصيتها. ومن المتوقع أن تُحدث الأبحاث والتطورات الجارية في نظم التعمية الهجينة، وتصميم بروتوكولات التشفير الآلية، وتحسينات توزيع المفاتيح الكمومية، وتطوير التعمية ما بعد الكمومية، والتعلم الآلي الكمومي لتحليل الشفرات، والحوسبة الآمنة متعددة الأطراف، ثورةً في هذا المجال. ومع ذلك، من الضروري مراعاة التبعات الأخلاقية وضمان توافق التطورات في التعمية الكمومية التي يديرها الذكاء الاصطناعي مع معايير حماية البيانات العالمية، ومع المخاوف التي تمليها الخصوصية.

شكر وتقدير

نعرب عن امتناننا العميق لمشروع الباحث الزائر في برنامج فولبرايت.

الإحالات :

1. https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices
2. https://csrc. nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon.
3. https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics.

تعليقات المترجم:

[i] نشرت القائمة النهائية للفائزين، أنظر الرابط:

https://csrc.nist.gov/Projects/lightweight-cryptography/finalists

[ii] في هذا الرمز يشير الحرف B المكرر إلى الحرفين الأولين لاسمي الباحثين و 84 إلى سنة 1984.

[iii] مصطلح Photonics يُترجم أيضا" ضوئيات".

[iv] لفظRSA مكوّن من الحروف الأولى لأسماء الباحثين الثلاثة الذين اخترعوا هذه الخوارزمية وهمRivest – Shamir – Adleman . وقد تم تطوير خوارزمية RSA عام 1977..

[v] تم تطوير خوارزمية شور عام 1994 من قبل العالم بيتر شور**Peter Shor** ، وهي تعمل على **الحواسيب الكمومية دون غيرها.**

[vi] في الذكاء الاصطناعي يشير مصطلح الأنطولوجيا إلى تمثيل لمجموعة من المفاهيم داخل مجال معين، والعلاقات بين هذه المفاهيم. .

[vii] هو الحروف الأولى لكلمات: CYBEX " Cybersecurity Information Exchange Framework". **إطارتبادل معلومات الأمن السيبراني.**

[viii] الرمز ANP-TOPSIS هو الحروف الأولى للعبارة-Analytic Network Process " Technique for Order Preference by Similarity to Ideal Solution"عملية الشبكة التحليلية- طريقة الترتيب حسب التشابه مع الحل المثالي. يتعلق الأمر بنموذج **هجين** يستخدم الشبكة التحليلية"**ANP**"، ثم يطبق طريقة الترتيب "**TOPSIS**" لاختيار أو ترتيب البدائل. هذا النموذج شائع في دراسات اتخاذ القرار، كإدارة المشاريع، واختيار الموردين، والتقييم البيئي، وغيرها.

[ix] S-Box تعني"Substitution box"، وهي مكونات تُستخدم في خوارزميات نوع من التعمية، وظيفتها الرئيسية إجراء **تحويل غير خطي** على البيانات، أي استبدال المدخلات بقيم أخرى بطريقة معقدة يصعب عكسها دون معرفة المفتاح. .

[x] نسبة إلى عالم المنطق البريطاني جورج بول(1815-1864) Boole . أما الدوال الشعاعية فهي أداة من أدوات التحليل الرياضي.

[xi] المقصود بـ"تطبيقات الزمن الفوري "أو" التطبيقات الزمنية الفورية "أو" تطبيقات الوقت الفعلي (Real-time applications) "اتلك التطبيقات التي ينبغي أن تستجيب فورا أو خلال وقت قصيرة جدا مثل المكالمات الصوتية عبر الإنترنت أو بث فيديوهات مباشرة.

[xii] التلبيد (أو" الهاش "hash أو التقطيع أو التجزئة) يعني هنا تحويل وثيقة أو رسالة بأي حجم إلى بصمة رقمية ذات حجم ثابت، باستخدام دالة رياضية تسمى دالة البصمة أو دالة التلبيد.

[xiii] "هجمات القوة الغاشمة (Brute-force attacks) "هي طريقة اختراق تعتمد على تجريب جميع الاحتمالات الممكنة للوصول إلى كلمة مرور، أو مفتاح تشفير، أو حل لمسألة أمنية.

[xiv] الجسيمات تحت الذرية (subatomic particles)هي الجسيمات الأصغر من الذرات، مثل الإلكترونات، وتعد اللبنة الأساسية لجميع المواد في الكون.

[xv] السحب العشوائي الكمومي(quantum coin tosses) هو عملية يُتّخذ فيها قرار عشوائي باستخدام قوانين ميكانيكا الكم بدلاً من استخدام مولّد أرقام عشوائية تقليدي أو قطعة نقدية حقيقية ورميها لمعرفة ما سيظهر (الوجه أو الظهر).

[xvi] التعمية ما بعد الكمومية (Post-quantum cryptography) هو جيل جديد من خوارزميات التشفير، تم تطويره بهدف استبدال أو تعزيز نظم التشفير الحالية التي ستكون عرضة للخطر عند ظهور الحواسيب الكمومية القوية.

[xvii] مدة حدودياتية (Polynomial time) "مصطلح يُستخدم في المعلوماتية والخوارزميات لوصف مدى تعقيد خوارزمية. وهذا الوصف يطلق على المسائل التي تُحل في عدد من الخطوات تكون محدودة بواسطة كثير حدود (Polynomial)، بمعنى أنه كلما زاد حجم المدْخلات، زادت مدة التنفيذ بشكل معقول، وليس بشكل أسّي (exponentially)الذي يدل على عكس ذلك.

[xviii] CS-FSM اختصار لعبارة" طريقة التعمية والأمن- استخدام الآلة ذات الحالات المحدودةFinite State Machine – Cryptography and Security) ".

[xix] الخوارزمية "KNN" اختصار لعبارة" الجيران K الأقرب.(K-Nearest Neighbors) "

[xx] EES اختصار Enhanced Encryption Standard.

[xxi] في المعلوماتية، تشير الحوسبة متعددة الأطراف (Multi-Party Computation=MPC)الآمنة غالبًا إلى فرع من التعمية يهدف إلى تمكين عدة أطراف من التعاون في إجراء عملية حسابية على بيانات خاصة، دون أن يكشف أي طرف بياناته للآخرين).

قائمة المراجع:

Advisera, "What is the meaning of ISO 27001?". https://advisera. com/27001 academy/what-is-iso-27001/

Agrawal A, et al. Software security estimation using the hybrid fuzzy ANP- TOPSIS approach: design tactics perspective. Symmetry. 2020; 12(4): 598. https://doi. org/10. 3390/SYM12040598.

Aldoseri A, Al-Khalifa KN, Hamouda AM. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Appl Sci. 2023; 13(12): 7082. https://doi. org/10. 3390/APP13127082.

Alyami H, et al. The evaluation of software security through quantum computing techniques: a durability perspective. Appl Sci. 2021; 11(24): 11784. https://doi. org/10. 3390/APP112411784.

Awan U, Hannola L, Tandon A, Goyal RK, Dhir A. Quantum computing challenges in the software industry. A fuzzy AHP-based approach. Inf Softw Technol. 2022; 147: 106896. https://doi. org/10. 1016/J. INFSOF. 2022. 106896.

Ayoade O, Rivas P, Orduz J. Artificial intelligence computing at the quantum level. Data. 2022; 7(3): 28. https://doi. org/10. 3390/DATA7030028.

Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2020; 560(P1):7–11. https://doi. org/10. 1016/j. tcs. 2014. 05. 025.

Braverman M, Ko YK, Weinstein O. Approximating the best Nash equilibrium in no (1ogn)-time breaks the exponential time hypothesis. Proc West Mark Ed Assoc Conf. 2015; 2015-Janua(January): 970–82. https://doi. org/10. 1137/1. 9781611973730. 66

Broadbent A, Schaffner C, Broadbent Abroadbe BA, Uottawaca B, Schaffner C. Quantum cryptography beyond quantum key distribution. Des Codes Cryptogr. 2015; 78(1):351-82. https://doi. org/10. 1007/S10623-015-0157-4.

Catril Opazo JE, NIST cybersecurity framework in South America: Argentina, Brazil, Chile, Colombia, and Uruguay (2021)

Diamanti E, Lo HK, Qi B, Yuan Z. Practical challenges in quantum key distribution. Npj Quantum Inf. 2016;2(1):1-12. https://doi. org/10. 1038/npjqi. 2016. 25.

Diffie W, Hellman ME. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6): 644–54. https://doi. org/10. 1109/TIT. 1976. 1055638.

Eisenhardt KM. Building theories from case study research. Acad Manag Rev. 1989; 14(4): 532. https://doi. org/10. 2307/258557.

Elaziz A, Raheman F. The future of cybersecurity in the age of quantum computers. Fut Internet. 2022; 14(11): 335. https://doi. org/10. 3390/FI14110335.

Feistel H, Block cipher cryptographic system (1971).

GDPR, What is GDPR, the EU's new data protection law?-GDPR. eu. Accessed 07 Jul 2023. https://gdpr. eu/what-is-gdpr/

Gill SS, et al. AI for next generation computing: Emerging trends and future directions. Internet of Things. 2022; 19:100514. https://doi. org/10. 1016/J. IOT. 2022. 100514.

Gupta S, Modgil S, Bhatt PC, Chiappetta Jabbour CJ, Kamble S. Quantum computing led innovation for achieving a more sustainable Covid-19 healthcare industry. Technovation. 2023;120:102544. https://doi. org/10. 1016/J. TECHNOVATION. 2022. 102544.

Gyongyosi L, Imre S. Secret key rate adaption for multicarrier continuous-variable quantum key distribution. SN Comput Sci. 2020;1(1):1-17. https://doi. org/10. 1007/s42979-019-0027-7.

ICO, Information Commissioner's Office (ICO): The UK GDPR, UK GDPR guidance and resources. Accessed 08 July 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/

ISO, "ISO/IEC 27035–1:2016-Information technology-Security techniques-Information security incident management-Part 1: Principles of incident management. " Accessed 25 July 2023. https://www. iso. org/standard/60803. html.

ISO, "ISO - International Organization for Standardization. " Accessed 26 Dec 2017. https://www. iso. org/home. html.

ISO, "ISO/IEC 27001 and related standards Information security management 2022

ISO, "ISO/IEC DIS 42001 - Information technology-Artificial intelligence—Management system. " Accessed 06 April 2023. https://www. iso. org/standard/81230. html.

Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C. Guide to cyber threat information sharing. NIST Spec Publ. 2016. https://doi. org/10. 6028/NIST. SP. 800-150.

Kop M. Quantum-ELSPI: a novel field of research. Digit Soc. 2023; 2(2):1–17. https://doi. org/10. 1007/S44206-023-00050-6.

Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. 2022; 15:100242. https://doi. org/10. 1016/J. ARRAY. 2022. 100242.

Liddell HG. A greek-english lexicon. Cape Palmas: Harper; 1894.

Lovic V, Quantum key distribution: advantages, challenges and policy 2020. https://doi. org/10. 17863/CAM. 58622.

Mallow GM, Hornung A, Barajas JN, Rudisill SS, An HS, Samartzis D. Quantum computing: the future of big data and artificial intelligence in spine. Spine Surg Relat Res. 2022; 6(2):93. https://doi. org/10. 22603/SSRR. 2021-0251.

NIST, "Advanced Encryption Standard (AES), 2001. Accessed 19 March 2023. https://web. archive. org/web/20170312045558/http://nvlpubs. nist. gov/nistpubs/FIPS/NIST. FIPS. 197. pdf

NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2014. Accessed 24 Dec 2017. https://www.nist. gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214. pdf

NIST, "Cybersecurity Framework Version 1. 1", 2018.

NIST, "Product Integration using NVD CVSS Calculators," 2022. https://nvd.nist. gov/Vulnerability-Metrics/Calculator-Product-Integration

NIST, "Key Management - Symmetric Block Ciphers, Pair-Wise Key Establish- ment Schemes," 2022, [Online]. https://csrc.nist.gov/projects/key-management/key-establishment

NIST, "Artificial intelligence | NIST. " Accessed 06 April 2023. https://www. nist. gov/artificial-intelligence

NIST, "AI Risk Management Framework | NIST," National Institute of Standards and Technology. Accessed 18 April 2023. Available: https://www.nist.gov/itl/ai-risk-management-framework

NIST, "Software Security in Supply Chains: Software Bill of Materials (SBOM) | NIST," National Institute of Standards and Technology. Accessed 18 April 2023. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

NIST, "Post-Quantum Cryptography | CSRC | Competition for Post-Quantum Cryptography Standardisation," 2023. Accessed 06 Sept 2023. https://csrc.nist. gov/projects/post-quantum-cryptography

NIST, "SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC. " Accessed 25 July 2023. https://csrc.nist.gov/pubs/sp/800/61/r2/final

NIST, "Post-Quantum Cryptography | CSRC | Selected Algorithms: Public-key Encryption and Key-establishment Algorithms," 2023. Accessed 06 Sept 2023. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

NIST, "NVD-CVSS v3 Calculator," CVSS Version 3. 1. Accessed 03 Jan 2023. https://nvd. nist. gov/vuln-metrics/cvss/v3-calculator

NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations 2020.

NIST Advanced Manufacturing Office, "Advanced Manufacturing Partnership," 2013. Accessed 04 May 2020. https://www.nist.gov/amo/programs

NIST C, Cybersecurity Framework | NIST. 2016. https://www.nist. gov/cyberframework.

NIST, "Block Cipher Techniques." https://csrc.nist.gov/Projects/block-cipher-techniques

NIST, "Post-Quantum Cryptography PQC." https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST, "Privacy-Enhancing Cryptography PEC. " https://csrc.nist.gov/Projects/pec

NIST, "Lightweight Cryptography." https://csrc.nist.gov/Projects/lightweight-cryptography

NIST, "Cybersecurity Framework." https://www.nist.gov/cyberframework/getting-started

NIST, "Hash Functions," 2020. https://csrc. nist. gov/Projects/Hash-Functions

NIST, "NIST Special Publication 800-128," 2011. https://nvlpubs.nist. gov/nistpubs/SpecialPublications/NIST. SP. 800-128. pdf

NIST, "NIST Version 1. 1," National Institute of Standards and Technology, U. S. Department of Commerce. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Nitaj A, Rachidi T. Applications of neural network-based AI in cryptography. Cryptography.2023;7(3):39.https://doi.org/10.3390/CRYPTOGRAPHY7030039.

Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners. Berlin: Springer; 2009.

Petrov M, Adapted SANS cybersecurity policies for NIST cybersecurity framework.

Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120-6.

Rutkowski A, et al. CYBEX. ACM SIGCOMM Comput Commun Rev. 2010;40(5):59–64. https://doi.org/10.1145/1880153.1880163

Sahu K, Srivastava RK, Kumar S, Saxena M, Gupta BK, Verma RP. Integrated hesitant fuzzy-based decision-making framework for evaluating sustainable and renewable energy. Int J Data Sci Anal. 2023;16(3):371–90. https://doi. org/10. 1007/S41060-023-00426-4

Sevilla J, Moreno P, Implications of quantum computing for artificial intel- ligence alignment research 2019.

Shamshad S, Riaz F, Riaz R, Rizvi SS, Abdulla S. An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy. Sensors (basel). 2022;22(21):271-6. https://doi. org/10. 3390/S22218151

Shapna Akter M Quantum cryptography for enhanced network security: a comprehensive survey of research. Developments, and Future Directions 2023.

Shor PW, Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings—annual IEEE symposium on foundations of computer science, FOCS, 1994. Pp. 124-134. https://doi. org/10. 1109/SFCS. 1994. 365700

SWID, "Software Identification (SWID) Tagging | CSRC | NIST," National Institute of Standards and Technology. Accessed 19 April 2023. [Online]. https://csrc.nist. gov/projects/Software-Identification-SWID

Tabassi E, AI risk management framework | NIST. (2023) https://doi.org/10. 6028/NIST. AI. 100-1

Takahashi T, Kadobayashi Y. Reference ontology for cybersecurity operational information.ComputJ.2015;58(10):2297-312. https://doi.org/10.1093/COMJNL/BXU101

Taylor RD. Quantum artificial intelligence: a 'precautionary' U. S. approach? Telecomm Policy. 2020;44(6):101909. https://doi. org/10. 1016/J. TELPOL. 2020. 101909

Tsai CW, Yang CW, Lin J, Chang YC, Chang RS. Quantum key distribution networks: challenges and future research issues in security. Appl Sci. 2021;11(9):3767. https://doi. org/10. 3390/APP11093767

Udroiu A-M, Dumitrache M, Sandu I, Improving the cybersecurity of medical systems by applying the NIST framework. In 2022 14th international conference on electronics, computers and artificial intelligence (ECAI). IEEE, 2022, pp 1–7.

Yin KR, Case study research: design and methods (2009) Accessed 25 April 2023. https://books.google.com/books?hl=en&lr=&id=FzawIAdilHkC&oi=fnd&pg=PR1&dq=Yin,+R.+K.+(2009).+Case+study+research:+Design+and+methods+(Vol.+5).+sage.&ots=l_5Q4fkSYt&sig=fICdRmFfBrFKJIHQRApE252vNhQ#v=onepage&q&f=false

Yin RK. Case study research: design and methods, vol. 5. Newcastle upon Tyne: Sage; 2009b.

Ying M. Quantum computation, quantum theory and AI. Artif Intell. 2010; 174(2):162-76. https://doi.org/10.1016/J.ARTINT.2009.11.009.

Ying M. Quantum computation, quantum theory and AI ☆. Artif Intell. 2010; 174:162-76. https://doi. org/10. 1016/j. artint. 2009. 11. 009.

Zolfaghari B, Rabieinejad E, Yazdinejad A, Parizi RM, Dehghantanha A, Crypto makes AI evolve

التمويل :

تم دعم هذا البحث من قبل المركز القومي البريطاني "بتراس" (PETRAS) للتميز في أمن نظم إنترنت الأشياء السيبراني، الممول من قبل مجلس بحوث الهندسة والعلوم الفيزيائية (EPSRC) في المملكة المتحدة تحت منحة رقم EP/S035362/1، ومن قبل مجلس"ESRC " تحت منحة رقم ES/V003666/1.

التعريف بالمؤلف :

الدكتور بيتر رادانليف هو مشرف مشاريع ماجستير في قسم علوم الحاسب بجامعة أكسفورد وباحث ما بعد الدكتوراه في جامعة باث. حصل على درجة الدكتوراه عام 2014/2013، ومنذ ذلك الحين، عمل باحثا في ما بعد الدكتوراه في عديد المؤسسات البحثية المرموقة، بما في ذلك إمبريال كوليدج لندن، وجامعة كامبريدج، ومعهد ماساتشوستس للتكنولوجيا (MIT)، وقسم هندسة العلوم بجامعة أكسفورد لمدة 7 سنوات، قبل أن ينتقل إلى قسم علوم الحاسب. لديه خبرة واسعة في الذكاء الاصطناعي، والأمن السيبراني، والحوسبة الكمومية، وتقنية البلوكشين. قبل مسيرته الأكاديمية، عمل لمدة عقد من الزمن مديرا للأمن السيبراني في بنك RBS، بالإضافة إلى 5 سنوات خبيرا في اختبارات الاختراق بوزارة الدفاع البريطانية.

Petar Radanliev, Department of Computer Sciences, University of Oxford, Oxford, UK

2 School of Management, University of Bath, Bath, UK.

ملخص المقال :

شهدت التطورات التكنولوجية الحديثة، لا سيما في مجالي الذكاء الاصطناعي (AI) والحوسبة الكمومية، تحولات جذرية في مجال التكنولوجيا. وقد أثرت هذه التطورات بشكل كبير على التعمية الكمومي حيث يحمل الذكاء الاصطناعي إمكانات هائلة لتعزيز كفاءة وقوة أنظمة التعمية. ومع ذلك، فإن ظهور الحواسيب الكمومية خلق تحديًا جديدًا أمام خوارزميات الأمان الحالية، يُعرف عادة باسم "التهديد الكمومي". وعلى الرغم من هذه التحديات، هناك آفاق واعدة لدمج الذكاء الاصطناعي القائم

على الشبكات العصبية في التعمية، وهو ما قد يكون له تأثيرات كبيرة على مستقبل أمن المعلومات الرقمي. نستعرض هذه الدراسة المحاور الرئيسية لتقاطع الذكاء الاصطناعي والتعمية الكمومية، بما في ذلك الفوائد المحتملة والتحديات التي يجب مواجهتها وآفاق البحث المستقبلي في هذا المجال متعدد التخصصات.

الكلمات الدالة : الذكاء الاصطناعي، الخوارزميات الكمومية، الشبكات العصبية، تكامل الذكاء الاصطناعي والكم، التهديدات الكمومية، الأمان المعزز بالذكاء الاصطناعي، معالجة المعلومات الكمومية.