Journal of Al-Turath University College
Open Access Journal
ISSN : 2074-5621
https://jatuc.uoturath.edu.iq/

توظيف تقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني: تحليل معمّق للتحديات والفرص المستقبلية

دعاء علي نوري*

وزارة التربية ، مديرية تربية بغداد الكرخ الثانية ، بغداد ، العراق.

*Corresponding Author: aliduaa544@gmail.com

الملخص

يعتبر إدخال تكنولوجيا الذكاء الاصطناعي في صميم إجراءات الأمن السيبراني محركًا أساسيًا للتغيير، فهو يغير الطريقة التي تحدد بها الشركات المخاطر الرقمية وتتعامل معها. يسهم الذكاء الاصطناعي في تعزيز قدرات الأمن السيبراني بعدة طرق، منها تسريع عملية اكتشاف التهديدات، والحد من الإنذارات الخاطئة، وتسهيل إجراءات الاستجابة للحوادث، بالإضافة إلى تمكين التقييم الاستباقي للمخاطر قبل وقوعها. كما يعزز هذا الدمج من فعالية آليات التحقق من الهوية ويقلل من عمليات الاحتيال. بالرغم من الفوائد العديدة، يواجه دمج الذكاء الاصطناعي في الأمن السيبراني صعوبات كبيرة، مثل: شح البيانات اللازمة للتدريب، وتحيز الخوارزميات، والضعف أمام الهجمات المعادية، وظهور قضايا أخلاقية، ونقص الخبرات المتخصصة، وصعوبة التوافق مع البنى التحتية الحالية. تتوقع الدراسات المستقبلية دورًا أكبر للذكاء الاصطناعي التوليدي، وضرورة اتباع استراتيجيات تجمع بين الإنسان والآلة، وأهمية وضع أطر تنظيمية دولية شاملة، بالإضافة إلى تطوير أُطر ذكاء اصطناعي شفافة وجديرة بالثقة، وتعزيز التعاون بين الجامعات والقطاع الخاص والجهات الحكومية المختلفة. الاستخدام المسؤول لتقنيات الذكاء الاصطناعي أمر لا بد منه، للاستفادة القصوى من مزاياها مع معالجة المخاطر المحتملة، بهدف بناء بيئة رقمية آمنة وموثوقة للجميع.

الكلمات المفتاحية
الذكاء الاصطناعي, الامن السيبراني, التعلم الآلي, الامن التنبئي, الهجمات العدائية, اكتشاف الهجمات, التعاون بين الانسان والذكاء الاصطناعي, الذكاء الاصطناعي التوليدي.

Abstract

Placing AI at the heart of cybersecurity operations acts as a catalyst for transformation, reshaping how firms detect and handle digital threats. Machine-learning tools boost security functions in multiple dimensions: they speed up the identification of attacks, lower the incidence of false positives, streamline the steps taken during an incident, and allow for forward-looking risk evaluations before any breach materialises. This melding also strengthens identity-verification processes and curtails fraudulent activity. Even with these advantages, embedding AI within security frameworks encounters major obstacles, such as scarce training datasets, bias inherent in algorithms, susceptibility to adversarial manipulation, emerging moral dilemmas, a shortage of qualified professionals, and problems aligning with legacy systems. Looking ahead, researchers foretell an expanded presence of generative AI, the need for blended human-AI approaches, the creation of all-encompassing global regulatory schemes, the design of AI that is transparent and trustworthy, and deeper cooperation between academia, industry, and government. Using AI responsibly is crucial to reap its upside while mitigating its dangers, ultimately forging a secure and dependable digital landscape for all.

Keywords
Artificial Intelligence, Cybersecurity, Threat Detection, Machine Learning, Adversarial Attacks, Predictive Security, Human-AI Collaboration, Generative AI.

1. المقدمة

الذكاء الاصطناعي، أو ما يعرف بـ "الـAI"، هو تجسيد لعمليات معقدة تهدف لخلق آلات قادرة على محاكاة القدرات العقلية للإنسان. تُصنع هذه الآلات بهدف التفكير الذاتي، واكتساب المعرفة، وفي النهاية اتخاذ قرارات واعية عبر الاختيار من بين عدة بدائل متاحة. تتداخل في هذه التقنية تخصصات عدة، مثل "التعلم الآلي" و"معالجة اللغات الطبيعية" و"الرؤية الحاسوبية" و"علم الروبوتات". تمكن هذه التقنيات الأنظمة من تحليل مجموعات ضخمة من البيانات، وتحديد الأنماط المتكررة، وتكييف ردود أفعالها بشكل لحظي، حتى في غياب التعليمات الصريحة [1] .أما الأمن السيبراني، فهو بمثابة الدرع الذي يحمي الشبكات والأنظمة والبيانات الموجودة فيها. الهدف الأسمى للأمن السيبراني هو التصدي للاختراقات

الرقمية، ومنع الدخول غير المصرح به، أو أي نشاط ضار آخر. يشمل ذلك توظيف مختلف التقنيات، واتباع إجراءات عمل منظمة، وتطبيق التدابير الأمنية التي تساهم في الحفاظ على خصوصية المعلومات، وحمايتها من العبث، والتأكد من استمراريتها وتوفرها. [2]

في خضم التشابك المتصاعد والتغيرات المستمرة والتصاعد في حدة المخاطر السيبرانية، أثبتت الأساليب الأمنية التقليدية قصورها. يمثل إدخال الذكاء الاصطناعي نقلة نوعية، مقدمًا إجراءات حماية مؤتمتة، وذكية، وقابلة للتكيف بسهولة. يمكن للذكاء الاصطناعي أن يحدد بسرعة أي انحرافات، ويتنبأ بالمخاطر المحتملة، ويوفر ردود فعل سريعة، ويستخدم الحوادث الماضية لتحسين استراتيجيات الحماية المستقبلية. يُعتبر هذا الدمج ضروريًا ليس فقط لحماية البنى التحتية الهامة والمعلومات الحساسة، بل أيضًا لتقليل الأخطاء البشرية، وتحسين دقة الاكتشاف، وتسهيل التقييم الاستباقي للتهديدات. يمنح الذكاء الاصطناعي أنظمة الأمن السيبراني القدرة على التكيف والفعالية والمرونة في مواجهة مشهد التهديدات السيبرانية المتغيرة باستمرار.

2. منهجية البحث

بغية بلوغ الغايات التي رسمتها هذه الدراسة، والتي تتمحور حول تقصي فاعلية الذكاء الاصطناعي في دعم وتحسين مستوى الأمن السيبراني، سيتم اعتماد الأسلوب الوصفي التحليلي كإطار منهجي للبحث. يُعتبر هذا الأسلوب الأمثل لملاءمته طبيعة الاستقصاء، إذ يسعى إلى إيضاح الكيفية التي يتم بها دمج التقنيات الذكية ضمن المنظومات الأمنية وتحليل جوانبها المتعددة.

إن الخطة المنهجية المتبعة ترتكز على المراحل المحددة أدناه:

عملية استخلاص المعلومات (جمع البيانات):

التأسيس على المعطيات المتاحة عبر المصادر الثانوية ، بما في ذلك المؤلفات المتخصصة، والدوريات الأكاديمية الخاضعة للتحكيم العلمي، والتقارير التقنية الصادرة عن المؤسسات الرصينة المعنية بأمن المعلومات. إجراء مسح شامل لأحدث الإحصائيات والدراسات السابقة التي بحثت في مدى فعالية النماذج الخوارزمية المتعلمة آليًا في مهمة اكتشاف التهديدات.

عملية تحليل البيانات: الاستدلال عبر المقارنات: يتم إجراء موازنة بين الأساليب المتبعة تقليدياً في المجال السيبراني وتلك المستحدثة التي تستند إلى قدرات الذكاء الاصطناعي. **الاستنتاج والتوصيات :**بناءً على التحليل، سيتم استخلاص النتائج المتعلقة بفعالية هذه الأنظمة وتقديم توصيات عملية للمؤسسات الراغبة في تبني هذه التقنيات

3. اهداف البحث

يهدف هذا البحث بشكل أساسي إلى استكشاف كيفية دمج الذكاء الاصطناعي في الأمن السيبراني، مع تحليل الاستخدامات الحالية وتقييم التحديات والفرص الناتجة عن هذا الدمج. على وجه التحديد، يسعى البحث إلى:

- تقييم كيفية توظيف الذكاء الاصطناعي في الأمن السيبراني في الوقت الحالي.
- تحديد المزايا والعيوب الرئيسية لتطبيق أدوات الأمن المعتمدة على الذكاء الاصطناعي.
- تحليل الأمثلة العملية والأنظمة القائمة.
- تقديم توصيات لتعزيز الأمن السيبراني من خلال تطبيقات الذكاء الاصطناعي.
- صياغة مقترحات لرفع كفاءة آليات الدفاع ضد التهديدات الإلكترونية.

4. الدراسات السابقة

يُعد دمج الذكاء الاصطناعي (AI) في مجال الأمن السيبراني موضوعًا بحثيًا متناميًا نظرًا لقدرة هذه التقنية على معالجة حجم هائل من البيانات واكتشاف الأنماط المعقدة. تتناول الأدبيات الحالية جوانب متعددة لهذا التكامل، بدءًا من الكشف التنبؤي عن الهجمات وصولاً إلى أتمتة الاستجابة الأمنية.

1.4. الذكاء الاصطناعي في الكشف عن التهديدات (AI in Threat Detection)

لقد تبيَّن أن الطرق المعتمدة على البصمات (Signature-based systems) لم تعد كافية للتصدي للهجمات المتطورة والمستحدثة باستمرار (Zero-day attacks). في المقابل، تُقدِّم تقنيات تعلُّم الآلة (ML) والتعلُّم العميق (DL) إمكانات لا مثيل لها في رصد السلوكيات الخارجة عن المألوف (اكتشاف الشذوذ)، والتي قد تكون مؤشراً على محاولات اختراق لم تُسجَّل من قبل.

- **رصد محاولات التوغل (Intrusion Detection):** يتم توظيف خوارزميات تعلُّم الآلة، مثل اشجار القرار (Decision Trees) ونماذج المتجهات الداعمة (SVM)، لفرز تصنيفات تدفقات البيانات عبر الشبكة، والتمييز بين السلوكيات العدائية والسلوكيات المعتادة. علاوة على ذلك، أثبتت بنيات التعلم العميق ، ولا سيما الشبكات العصبية الالتفافية (CNN) والشبكات العصبية المتكررة (RNN)، كفاءة عالية في معالجة سلاسل البيانات المعقدة وتحديد مكان البرمجيات الضارة
- **فحص وتحليل البرمجيات الخبيثة (Malware Analysis):** يستند الذكاء الاصطناعي في هذا المجال إلى دراسة الخصائص الساكنة (الثابتة) والمتحركة (الديناميكية) للملفات بهدف اكتشاف السلالات الجديدة من البرمجيات الخبيثة. تتمتع هذه النماذج بالقدرة على استنتاج الهيكل المتوقع للملفات وسلوكها أثناء التشغيل لتحديد مدى اضرارها، مما يوفر سرعة استجابة يفوق ما يمكن تحقيقه بالوسائل التقليدية [3]

2.4 الأمن التنافسي والتحديات (Adversarial Security and Challenges)

يشكل استخدام المهاجمين للذكاء الاصطناعي تحديًا كبيرًا، وهو ما يُعرف بـ "الأمن السيبراني التنافسي(Adversarial Cybersecurity) "

- **الهجمات التنافسية على الذكاء الاصطناعي (Adversarial AI Attacks)** : يمكن للمهاجمين استخدام تقنيات إخفاء وإفساد البيانات (Evasion and Poisoning attacks)لخداع نماذج التعلم الآلي الأمنية. فمثلاً، قد يقومون بإجراء تعديلات طفيفة وغير محسوسة على البرمجيات الخبيثة (Adversarial Examples)لتصنيفها كنظام سليم من قِبل نظام الكشف المعتمد على الذكاء الاصطناعي .
- **التحديات الأخلاقية والخصوصية (Ethical and Privacy Challenges)**يتطلب تحليل كميات هائلة من بيانات المستخدمين لتغذية نماذج الذكاء الاصطناعي الأمنية مراعاة صارمة لمعايير الخصوصية. كما أن الاعتماد المفرط على الأنظمة المؤتمتة قد يؤدي إلى اتخاذ قرارات حاسمة دون تدخل بشري، مما يثير تساؤلات حول المسؤولية (Accountability)في حالة الفشل الأمني [4]

5. دور الذكاء الاصطناعي في الامن السيبراني

برز الذكاء الاصطناعي (AI) كأداة حاسمة في عالم الأمن السيبراني، مقدمًا حلولًا متطورة للتصدي للتحديات المتزايدة للتهديدات الرقمية، بدايةً من الكشف عنها وانتهاءً بمنعها والاستجابة لها بفعالية. النُظم التقليدية القائمة على القواعد غالبًا ما تظهر محدودية في التأقلم مع الهجمات الحديثة والمتطورة باستمرار [1]. في المقابل، يمتلك الذكاء الاصطناعي القدرة على معالجة كميات هائلة من البيانات لحظيًا، وتحديد الأنماط الشاذة التي قد تشير إلى سلوك ضار[2].

من أبرز مهام الذكاء الاصطناعي في الأمن السيبراني، الكشف عن التهديدات السيبرانية ومنعها. تعتمد الخوارزميات المستخدمة في التعلم الآلي على بيانات الهجمات السابقة للتعرف بدقة على البرامج الضارة، وحملات التصيد الاحتيالي، وبرمجيات الفدية، وكذلك الثغرات الأمنية المستحدثة [2]. يمكن لأنظمة كشف ومنع التسلل، المدعومة بالذكاء الاصطناعي، تحليل سلوك حركة المرور الشبكية وإطلاق التنبيهات تلقائيًا دون الحاجة لتدخل بشري [5]. إضافة إلى ذلك، يساهم الذكاء الاصطناعي في تحليل سلوكيات المستخدمين والأجهزة، حيث تقوم الأنظمة بدراسة السلوك الطبيعي، ثم تحديد أي انحرافات قد تشير إلى تهديدات داخلية أو حسابات تعرضت للاختراق. كما يعزز الذكاء الاصطناعي عملية الاستجابة للحوادث الأمنية من خلال أتمتة المهام المتكررة، وتصنيف التنبيهات بناءً على درجة خطورتها، وتحديد الأولويات للمحللين، وبالتالي تقليل الوقت اللازم للاستجابة [5]. بالإضافة إلى ذلك، يدعم الذكاء الاصطناعي الحصول على استخبارات التهديدات في الوقت الفعلي، من خلال جمع وتحليل البيانات بشكل مستمر من مصادر متنوعة (مثل الشبكات والنقاط النهائية والحوسبة السحابية)، مما يسمح للمؤسسات بالبقاء في صدارة أساليب المجرمين السيبرانيين [5]. علاوة على ذلك، يتم استخدام معالجة اللغة الطبيعية، كفرع من فروع الذكاء الاصطناعي، لتحليل البيانات غير المهيكلة مثل محادثات الويب المظلمة أو رسائل البريد الإلكتروني الخادعة، للكشف عن المخاطر المحتملة في مراحلها الأولى [6].

6. التطبيقات الرئيسية للذكاء الاصطناعي في الأمن السيبراني

يشهد الأمن السيبراني تحولاً عميقًا بفضل الذكاء الاصطناعي، الذي يفتح الباب أمام جيل جديد من أنظمة الحماية. تتميز هذه الأنظمة بالذكاء المتزايد، والسرعة الفائقة، والقدرة على التكيف مع التهديدات المتجددة باستمرار. تتجلى قوة الذكاء الاصطناعي في تطبيقات متنوعة وفعالة، تُظهر قدرته على تحديد التهديدات السيبرانية ومواجهتها ببراعة، وذلك قبل أن تتسبب في خسائر كبيرة([1] [2] [4]) ومن هذه التطبيقات :

1.6. تعزيز الأمن السيبراني: التعرف على التهديدات واحتواء التسلل باستخدام التعلم الآلي.

تُيسِّر خوارزميات التعلّم الآلي (ML) عمليات كشف التهديدات المتطوّرة ضمن الأنظمة الذكية. عبر تحليل كتل البيانات الضخمة المتعلّقة بحركة المرور الشبكية وسجلات النظام، تُمكن هذه البرمجيات من التعرّف على أنماط الهجمات بدقّة. وبخلاف الحلول التقليدية التي تعتمد على القواعد الصارمة، تستند نماذج التعلم الآلي إلى المعطيات التاريخية لتحديد التهديدات المستجدة والتعامل معها بفعالية، مما يعزّز إجراءات الكشف الاستباقي. وتساهم هذه التقنية بشكل ملحوظ في تخفيض الوقت اللازم للاستجابة الفورية عند وقوع أي اختراق أمني [2][7].

2.6. UEBA المراقبة المدعومة بالذكاء الاصطناعي للمستخدمين والأنظمة

يدعم الذكاء الاصطناعي أنظمة تحليل سلوك المستخدم والكيانات (UEBA)، مما يسمح بإنشاء نماذج سلوكية للمستخدمين والأجهزة والبرامج. من خلال المراقبة المستمرة للأنشطة، تكتشف هذه الأنظمة أي انحرافات يمكن أن تدل على تهديدات داخلية أو اختراقات للحسابات أو عمليات ضارة. على سبيل المثال، يمكن أن يؤدي وصول الموظفين إلى بيانات حساسة خارج ساعات العمل المعتادة أو من أجهزة غير مألوفة إلى إصدار تنبيهات آلية. [8]

3.6 الكشف عن هجمات التصيد وتصنيف البرمجيات الخبيثة

يعتمد الذكاء الاصطناعي على أدوات معالجة اللغة الطبيعية ورؤية الحاسوب لتحقيق كشفٍ فعال لرسائل البريد الإلكتروني التي تحمل طابع الاحتيال، وكذلك المواقع الإلكترونية المقلدة والمرفقات التي تحتوي على برمجيات ضارة. يتمثل ذلك في تحليل عناوين المواقع الإلكترونية، ومحتوى الرسائل، وكذلك سلوكيات المرسلين لتحديد الفروقات بين الاتصالات الآمنة وتلك الخبيثة. وفيما يخص تصنيف البرمجيات الضارة، يقوم الذكاء الاصطناعي بدراسة سلوك الملفات والبيانات الوصفية الخاصة بها، وذلك بهدف تحديد التهديدات المعروفة وغير المعروفة، بما في ذلك هجمات "zero-day" [9][10].

4.6. الأمن الاستباقي ورصد الحالات الشاذة الآنية

توظف النماذج التنبؤية، المدعومة بالذكاء الاصطناعي، المعطيات السابقة بهدف توقع المخاطر السيبرانية الآتية ومواطن الضعف المحتملة. تتفوق هذه الآليات في تحديد الاختلافات الطفيفة، والتي قد تدل على عمليات اختراق للبيانات، أو هجمات فدية، أو محاولات وصول غير مسموح بها، بشكل فوري. يعد التحول من الرد الدفاعي إلى الحماية الاستباقية، عبر الاعتماد على التوقعات، أمرًا بالغ الأهمية في ظل التهديدات السيبرانية المتجددة باستمرار [11][12].الذكاء الاصطناعي بدراسة سلوك الملفات والبيانات الوصفية الخاصة بها، وذلك بهدف تحديد التهديدات المعروفة وغير المعروفة، بما في ذلك هجمات "zero-day" [9][10].

5.6. الاستفادة من الذكاء الاصطناعي لتعزيز أمن إنترنت الأشياء (IoT)

يمكن أن تكون إجراءات السلامة في أجهزة إنترنت الأشياء عرضة للضعف في أغلب الأحوال، ما يحولها إلى أهداف رئيسية للكيانات ذات النوايا السيئة. باستطاعة الذكاء الاصطناعي فحص سلوكيات تفاعل أجهزة إنترنت الأشياء، واكتشاف أي أنشطة غير معتادة، ثم التجاوب سريعًا مع الأخطار المحتملة. بالتالي، تعتبر البنيات الأمنية المعتمدة على الذكاء الاصطناعي ضرورية لحماية البنية التحتية ذات الأهمية الحاسمة والبيئات الذكية المترابطة عبر شبكات إنترنت الأشياء [13].

عقب مناقشة النماذج الأبرز لتطبيق الذكاء الاصطناعي ضمن ميدان الأمن السيبراني، بات لزاماً أن نركز الاهتمام على الإمكانيات الكامنة التي يوفرها دمج هذه التقنيات الحديثة، وما يمكن أن تحققه من إضافة جوهرية وملموسة لمنظومات الدفاع الرقمي والحماية الإلكترونية.

7. فرص دمج الذكاء الاصطناعي في الأمن السيبراني

1.7. التخفيف السريع للتهديدات واتخاذ الإجراءات الفورية

من بين الفوائد الأساسية لدمج الذكاء الاصطناعي في منظومة الأمن السيبراني، تبرز القدرة على الرد السريع على التهديدات. إذ تتمكن الأنظمة المدعومة بالذكاء الاصطناعي من تحليل كميات هائلة من البيانات في وقت قياسي، مما يسهل تحديد الأنماط المشبوهة المحتملة وتفعيل آليات المواجهة بشكل آلي. وكنتيجة لذلك، يتقلص الوقت الفاصل بين اكتشاف التهديد والحد من آثاره بشكل ملحوظ، مما يقلل من حجم الأضرار المحتملة .[2] [13].

2.7. تقليل الإنذارات الكاذبة وتنقية نظام التنبيهات

تعتاد أنظمة الأمن السيبراني التقليدية على توليد عدد هائل من التنبيهات، غالباً ما تكون نسبة كبيرة منها غير دقيقة أو مجرد إنذارات كاذبة. هذا السيل من التنبيهات يمكن أن يثقل كاهل فرق الأمن ويعيق استجابتهم للتهديدات الحقيقية والوشيكة. بينما يساعد الذكاء الاصطناعي في غربلة هذه التنبيهات غير الضرورية، وذلك بالاعتماد على تقنيات متطورة لتحليل البيانات واكتشاف التهديدات الفعلية. وهذا بدوره يتيح لمتخصصي الأمن تركيز جهودهم على الحوادث الأمنية ذات الأولوية القصوى، والتعامل معها بكفاءة. [9]

3.7. رصد التهديدات واكتشاف المخاطر

بإمكان المؤسسات تبني منهجية أمنية استباقية بفضل الذكاء الاصطناعي. عبر استغلال البيانات التاريخية مع معلومات التهديدات، يستثمر الذكاء الاصطناعي في خوارزميات التعلم الآلي للتنبؤ بمسارات الهجوم المحتملة وتحديد مواطن الضعف قبل استغلالها. تعزز هذه القدرة التنبؤية تطبيق التدابير الوقائية وتصميم استراتيجية دفاعية متينة. [14]

4.7. **تعزيز الاستجابة للحوادث وقدرات الأتمتة**

يمكن الاستفادة من أدوات الأتمتة، المدعومة بالذكاء الاصطناعي، لتسهيل عمليات الاستجابة للحوادث الأمنية. تتضمن هذه العمليات عزل الأجهزة المتضررة، وحظر الاتصالات من عناوين بروتوكولات الإنترنت (IP) المشبوهة، أو الشروع في تحقيقات جنائية معمقة. تساهم أتمتة المهام الروتينية التي تستهلك الوقت، في تحسين الكفاءة التشغيلية، مما يسمح لخبراء الأمن بالتركيز على المشكلات الأكثر تعقيدًا وتطوير الخطط الاستراتيجية اللازمة. [14] [15]

مع أن الإمكانيات الهائلة التي تبدو عليها استخدامات الذكاء الاصطناعي والفرص المتاحة بفضلها، يبقى لزامًا استعراض كافة الزوايا، بما في ذلك العقبات التي قد تعترض طريق دمج هذه التقنيات في مختلف الحقول والمجالات الإلكترونية.

8 . تحديات الذكاء الاصطناعي في الأمن السيبراني

- **قيود البيانات: قلة، دقة، ووضع العلامات**

تعتمد كفاءة الذكاء الاصطناعي بشكل أساسي على توفر بيانات واسعة النطاق وذات جودة عالية. ومع ذلك، غالبًا ما تعاني مجموعات بيانات الأمن السيبراني من صعوبات عدة، مثل محدودية الإتاحة، أو عدم الدقة، أو التحيز. بالإضافة إلى ذلك، يمثل وضع العلامات الدقيقة على بيانات الأمن السيبراني تحديًا كبيرًا بسبب التغيرات السريعة التي تطرأ على سلوكيات التهديدات، مما يصعب الحفاظ على تحديث مجموعات التدريب. [16]

- **النزعات الخوارزمية وتخصيص النموذج بشكل مفرط**

قد تحمل نماذج الذكاء الاصطناعي، دون قصد، تحيزات متأصلة في البيانات التي تعتمد عليها، الأمر الذي قد يفضي إلى نتائج مضللة أو غير منصفة. تعرف بـ"زيادة التخصيص" بأنها تحقيق النموذج على أداء متميز مع بيانات التدريب، لكن مع ضعف قدرته على تطبيق هذه المعرفة على بيانات جديدة، مما يؤدي إلى تراجع موثوقية أنظمة الذكاء الاصطناعي، خاصة في بيئة الأمن السيبراني دائمة التغير. [17]

- **مدخلات خبيثة وخداع النموذج**

تتعرض نماذج الذكاء الاصطناعي لهجمات يمكن أن يطلق عليها "العدائية". يقوم المهاجمون بابتكار مدخلات مصممة بدقة بهدف "خداع" هذه الأنظمة. عبر استغلال نقاط الضعف الكامنة، يصبح بمقدورهم إحداث نتائج غير دقيقة، ما يؤدي إلى توليد "إيجابيات كاذبة" أو، الأهم، "سلبيات كاذبة". هذه التلاعبات الخادعة، في جوهرها، تقوض الثقة في موثوقية الإجراءات الأمنية المعتمدة على الذكاء الاصطناعي. [18]

- **المعضلات الأخلاقية: السرية، التتبع، والشفافية**

إن توظيف الذكاء الاصطناعي في مجال الأمن السيبراني يجلب معه اعتبارات أخلاقية هامة. فعملية جمع وتحليل كميات هائلة من البيانات قد تُعرّض سرية المستخدم للخطر. بالإضافة إلى ذلك، قد يُستغل التتبع المدعوم بالذكاء الاصطناعي بصورة سلبية. ولغرض تعزيز الثقة والمسؤولية، تُعد الشفافية في الإجراءات وتقديم تفسيرات واضحة للقرارات التي ينتجها الذكاء الاصطناعي أمرًا حيويًا. [19]

- **نقص المهارات والفجوات التعليمية**

إن القصور في توافر الخبراء في مجال الأمن السيبراني المتمكنين في الذكاء الاصطناعي وتعلّم الآلة يشكّل عقبةً كبيرة. هذا النقص في المهارات يجعل عملية تطوير وتنفيذ وصيانة الحلول الأمنية المعتمدة على الذكاء الاصطناعي أكثر صعوبة. لذا فإن البرامج التدريبية الدائمة والدورات التعليمية تُعد ضرورية للتقليل من هذه الفجوة في الكفاءات. [20]

- **العقبات في دمج البنى التحتية القديمة**

تتمثل إحدى التحديات الشائعة في دمج أنظمة الذكاء الاصطناعي المتقدمة مع البنى التحتية لتكنولوجيا المعلومات القائمة. فقد تفتقر الأنظمة القديمة إلى الدعم الضروري. كما أن قضايا عدم التوافق، ونقص المعايير، والمقاومة للتغيير يمكن أن تعيق أو تجعل تبني حلول الذكاء الاصطناعي في الأمن السيبراني أكثر صعوبة. [19]

8. دراسة حالة وتطبيقات عملية

- **حلول الذكاء الاصطناعي في الأمن السيبراني(مثل IBM Watson وDarktrace)**

تستفيد منصات الأمن السيبراني التي تستخدم الذكاء الاصطناعي، مثل **IBM Watson** و**Darktrace** ، من تقنيات تعلّم الآلة والتحليلات المتقدمة لأداء مهام تتعلق بالكشف عن الانتهاكات الأمنية الرقمية، وفحصها، والتفاعل معها. يدمج **IBM Watson** معالجة اللغة الطبيعية مع قاعدة بيانات واسعة للمعلومات الأمنية، ما يسهل توفير رؤى استخباراتية عن التهديدات ويدعم فرق الأمن لاتخاذ القرارات الحرجة بسرعة. من ناحية أخرى، يستخدم **Darktrace** التعلم غير المراقب لإنشاء نماذج سلوكية للشبكات، مما يتيح الكشف عن الشذوذات التي قد تشير إلى هجمات محتملة، مع تقديم اكتشاف ذاتي للتهديدات واستجابة آلية في الوقت الفعلي. [19]

- **الذكاء الاصطناعي في كشف تهديدات البريد الإلكتروني والدفاع ضد التصيّد الاحتيالي (Phishing)**

يُعَدُّ التصيّد الاحتيالي من أكثر أساليب الهجمات رواجًا، ويتطلب اتخاذ تدابير مضادة. تستقصي حلول الذكاء الاصطناعي رسائل البريد الإلكتروني بدقة، وتشمل عملية التحليل البيانات الوصفية، نص الرسالة، وتصرفات المرسِل. تعتمد هذه الأنظمة على تقنيات مثل معالجة اللغة الطبيعية وتحديد الأنماط لاكتشاف الرسائل المشكوك فيها والروابط الخبيثة. تستغل منصات مثل(**Microsoft Defender** و**Gmail AI Filters**) إمكانيات الذكاء الاصطناعي للحد من محاولات التصيّد، وذلك لحماية المستخدمين من سرقة بيانات الدخول وانتشار البرمجيات الضارة. [21]

- **تطبيقات الأمن القومي والحماية السيبرانية على المستوى العسكري**

تسعى الحكومات والجهات الدفاعية بشكل متزايد إلى دمج تقنيات الذكاء الاصطناعي في برامج الأمن السيبراني، لتأمين البنى التحتية الحيوية وحماية الأصول الوطنية الحساسة من الأخطار الرقمية. تتميز أنظمة الذكاء الاصطناعي بقدرتها على فحص كميات ضخمة من البيانات لاكتشاف محاولات التجسس السيبراني، وهجمات الفدية، والتهديدات المستمرة المتقدمة. على سبيل المثال، تستعين **وزارة الدفاع الأمريكية** بآليات مدعومة بالذكاء الاصطناعي لتحديد التهديدات وتلقائيًا الاستجابة لانتهاكات الأمن، مما يضمن سرية المعلومات والحفاظ على تفوقها السيبراني المستمر. [19] [22]

9.المناقشة

إن إدخال آليات الذكاء الاصطناعي ضمن أنظمة الحماية الإلكترونية يمثل نقلة نوعية جذرية في المقاربة المتبعة للتصدي للأخطار المستجدة والاعتداءات المتقنة. النصوص التي تناولناها قدمت أساسًا مفاهيميًا وعمليًا يوضح سبب ضرورة هذا التكامل، ويسلط الضوء على مدى نجاحه، مع استعراض العقبات التكنولوجية وتلك المتعلقة بالجوانب غير التقنية. بناءً على هذا، تسعى هذه المداولة العلمية إلى فحص محتوى تلك المراجع فحصًا تحليليًا متعمقًا، ومواءمتها مع الأوضاع البحثية الحالية في مجال الامن السيبراني.

1.9 **منهجية التحليل**

ارتكزت عملية التحليل هذه على أسلوب التحليل المنهجي المنظم (Systematic Comparative Analysis)، الذي يقوم على تجزئة المدخلات النصية إلى عناصرها النظرية وأخرى عملية، سعيًا لكشف الصلة بين الركائز الإجرائية لتوظيف الذكاء الاصطناعي، والمخرجات الواقعية الناجمة عن هذا الإدماج. ولإنجاز هذا التحليل، تم الاستعانة بأدوات ثلاث أساسية:

- **تحليل المضمون** : تم عبر عملية فحص المحتوى من خلال استخلاص المحاور الأساسية التي تكررت في المواد المقروءة، ومن أبرزها: تقنيات التعلم الآلي والتعلم العميق ، رصد الاستثناءات أو الانحرافات، التهديدات الأمنية غير المسبوقة (هجمات يوم الصفر)، صراع الذكاء الاصطناعي التنافسي. هذا التحليل أتاح تأسيس فهم متكامل للكيفية التي يساهم بها الذكاء الاصطناعي في دعم وتقوية الإمكانات الدفاعية.
- **الإطار المنهجي** : تمت المقارنة بين المبادئ المطروحة في السطور المذكورة مع النموذج الفكري المهيمن في مجال حماية الفضاءات الرقمية، الذي يشدد على الانتقال من أساليب الحماية القائمة على رد الفعل إلى منهجيات وقائية متقدمة، الأمر الذي تستدعيه وتدعمه استخدام الذكاء الاصطناعي في تعميق الفهم للسلوكيات المشبوهة والتنبؤ بالمخاطر المقبلة.
- **التحليل ثنائي الأبعاد(Bipolar Analysis)** : تم النظر إلى هذا الموضوع من منظورين رئيسيين:
  - الجانب الإيجابي (الفرص): يتمثل في إمكانية رفع كفاءة الكشف، وتسريع وتيرة الاستجابة، وزيادة مستوى التشغيل الآلي.
  - الجانب السلبي (المعوقات): يبرز في صعوبة فهم العمليات، والمخاطر المتعلقة بالميزة التنافسية، ومشكلة تحيز البيانات، والجوانب المتعلقة بالأخلاقيات.

ومن خلال هذا التحليل ، تجلّى أن إدماج تقنيات الذكاء الاصطناعي يعد بمثابة معضلة ذات حدين؛ فهو يفتح آفاقاً دفاعية لم يسبق لها مثيل، ولكنه يولد في الآن ذاته تهديدات مستجدة ومتشابكة.

2.9 توافق النتائج مع الدراسات السابقة

1. **تحديات المناهج الدفاعية المعتادة:** الأساليب الكلاسيكية للحماية، المرتكزة على مطابقة البصمات المعروفة، تظهر عجزاً متزايداً في التصدي للتهديدات المستجدة التي لم تُكتشف بعد، والمعروفة باسم "هجمات اليوم صفر"
2. **الريادة للتحليل السلوكي (كشف الشذوذ):** لقد برهنت خوارزميات متقدمة، ومن ضمنها الشبكات الالتفافية (CNN) والمتكررة (RNN)، على قدرتها الفائقة في رفع مستوى دقة وكفاءة الاستجابات الأمنية. [3]
3. **التحديات الأمنية للذكاء الاصطناعي (الذكاء الاصطناعي الخصامي):** نماذج الذكاء الاصطناعي نفسها باتت عرضة للاستهداف من قبل تكتيكات هجومية تهدف إلى التضليل وتلويث البيانات
4. **معضلات الشفافية والمسؤولية الأخلاقية:** إن الطبيعة الصندوقية المغلقة لتقنيات التعلم العميق تعيق الوصول إلى فهم واضح لآلياتها الداخلية، مما يصعب مهمة التحقق والمساءلة، ويتنافر مع المتطلبات التنظيمية المعاصرة كاللائحة العامة لحماية البيانات (GDPR). [4]

10.الاتجاهات المستقبلية والتوصيات [19] [23] [24]

- **البيئة المتقلبة للتقنيات التوليدية للذكاء الاصطناعي داخل مجال الأمن السيبراني**

يتزايد دمج تقنيات الذكاء الاصطناعي التوليدي في أنشطة الأمن السيبراني، لاسيما عبر الاعتماد على نماذج اللغات الضخمة (SLMs) مثل GPT-4. تُستغل هذه الأدوات في صقل قدرات جمع معلومات التهديدات، وتلقيم عمليات الاستجابة للوقائع، وتفصيل تحليل الثغرات الأمنية. ومع هذا التقدم، فإن هذه النماذج قد تُسهم في ظهور تهديدات جديدة، بما فيها إمكانية توظيفها كأداة للعداوة وإنتاج محتوى ضار.

التوصيات:

- ❖ **التركيز على تنفيذ إجراءات أمنية مشددة لضمان سلامة أنظمة الذكاء الاصطناعي من أي هجمات.**
- ❖ **تطبيق صيانة دورية وتحديثات مستمرة للنماذج القائمة لضمان كفاءتها في التصدي للتهديدات السيبرانية المتصاعدة.**
- ❖ **إعداد وتطبيق إرشادات أخلاقية لاستخدام أدوات الذكاء الاصطناعي التوليدي ضمن عمليات الأمن السيبراني.**

- **دمج الفطنة البشرية مع تقنيات الذكاء الاصطناعي**

التكامل بين أنظمة الذكاء الاصطناعي وخبرة الأفراد يولّد نماذج مختلطة، تُحسّن من كفاءة اتخاذ القرار في ميدان الأمن السيبراني. إذ يتفوق الذكاء الاصطناعي في تحليل كمية هائلة من البيانات واكتشاف الانحرافات، بينما يضيف المتخصصون البشريون البعد السياقي والتقييم الأخلاقي. هذا التفاعل يُعزّز دقة وقوة بروتوكولات الأمن السيبراني.

التوصيات:

- ❖ **إطلاق مبادرات تعليمية تهدف إلى تمكين المتخصصين في الأمن السيبراني من مهارات الذكاء الاصطناعي.**
- ❖ **تعزيز التعاون بين مهندسي الذكاء الاصطناعي وخبراء الأمن السيبراني لتطوير موارد ذكاء اصطناعي متاحة وسهلة الاستخدام.**
- ❖ **حث المؤسسات على اعتماد استراتيجيات هجينة تستفيد من نقاط القوة لكل من قدرات الذكاء الاصطناعي والوعي البشري.**

- **بناء حلول ذكاء اصطناعي متينة، قابلة للتفسير، ومحافظة على الأمان**

تُعد القدرة على شرح سلوك الذكاء الاصطناعي (**Explainable AI – XAI**) من الركائز المهمة في مجال الأمن السيبراني، حيث يلزم أن يكون العاملون البشريون قادرين على استيعاب وثقة القرارات التي ينتجها الذكاء الاصطناعي. تُوفر منهجياتXAI ، بما فيها تقنيات التعرف على السمات الأكثر تأثيرًا والتحليل السببي، وسيلة قيمة لتوضيح استنتاجات نماذج الذكاء الاصطناعي، وتوصيل الأخطار المحتملة.

التوصيات:

- ❖ **تخصيص ميزانية لاستكشاف أحدث حلول XAI المصممة خصيصًا لتلبية متطلبات الأمن السيبراني.**
- ❖ **ضمان أن تُصمم أطر عمل الذكاء الاصطناعي مع مراعاة الأمان كشرط أساسي للحد من فرص التلاعب.**
- ❖ **تشجيع دمج تقنيات XAI لرفع مستويات الثقة والمسائلة في أنظمة الأمن السيبراني المعتمدة على الذكاء الاصطناعي.**

- **انشاء منصات مشتركة بين الجامعات والشركات الامنية والهيئات الحكومية لاجراء نماذج AI ضد الهجمات العدائية**

يُعتبر التنسيق بين الكيانات الأكاديمية، الصناعة، والقطاع العام عاملًا أساسيًا في مواجهة التحديات المتنوعة التي يفرضها الذكاء الاصطناعي على ميدان الأمن السيبراني. ويسهم التعاون المتبادل في إبداع حلول جديدة، وتطبيق أنجح الممارسات، كما يتيح صياغة استراتيجيات ذات فائدة ملموسة.

التوصيات:

- ❖ **تكوين تحالفات تجمع بين المؤسسات الأكاديمية، قادة الأعمال، والجهات الحكومية لتعزيز تبادل المعرفة وتعزيز الإبداع.**
- ❖ **تعزيز برامج البحث المشتركة التي تدمج خبرات الذكاء الاصطناعي، الأمن السيبراني، وصنع السياسات العامة.**
- ❖ **تشجيع المشاريع المتداخلة بين القطاعين العام والخاص بجهد ملحوظ لتسريع تطوير وتطبيق تقنيات الذكاء الاصطناعي الآمنة.**

10.الاستنتاج

لقد أوضحت هذه الدراسة التي تعتمد على التحليل العميق أن إدماج أدوات الذكاء الاصطناعي في مجال الامن السيبراني ، لا سيما التعلم العميق وقدرات تعلم الآلة، يشكل تحولاً جذرياً لا مفر منه في قطاع الأمن الإلكتروني. النتيجة الأساسية التي توصلنا إليها هي أن استغلال الذكاء الاصطناعي يعزز بشكل ملحوظ فعالية الدفاعات في اكتشاف التهديدات الجديدة بشكل استباقي وتسريع آليات التعامل معها، متجاوزاً بهذا القصور الواضح في الطرق الكلاسيكية التي تعتمد على قوائم الاكتشافات المعروفة مسبقاً.

على الصعيد الآخر، كشف البحث عن أن هذا التوجه نحو التبني تواجهه ثلاث عقبات أساسية تتطلب معالجة متكاملة:

العائق التقني: يتمثل في سرعة تطور أساليب الاختراق، التي تتجاوز قدرة النماذج المدربة على البيانات التاريخية، إضافة إلى نقطة الضعف المتعلقة بالهجمات المعادية المصممة خصيصاً لخداع نماذج الذكاء الاصطناعي نفسها.

التحدي المنهجي: ينبع من مشكلة "الصندوق الأسود"، وهي حالة تقلل من الثقة في القرارات الصادرة عن الأنظمة وتزيد من صعوبة مهمة الخبراء البشريين في فحص الإشعارات وإثبات صحتها.

العائق التشريعي والأخلاقي: يرتكز على المعضلات الأساسية المتعلقة بضمان خصوصية المعلومات وتفادي التحيز في الخوارزميات، وهي عوامل تعرقل التطبيق الواسع والآمن للذكاء الاصطناعي.

وختاماً، يمكن الاستنتاج بأن تحقيق التقدم المأمول في حماية الأنظمة الرقمية لا يكمن في الاعتماد المطلق على الأتمتة، بل في وضع خطة واعية ومسؤولة تحقق التوازن بين المكاسب التكنولوجية والمحاذير الأخلاقية. يجب أن تقوم هذه الخطة على تطوير نماذج ذكية تتمتع بالقدرة على الشرح والتحقق، مع ضرورة ربطها بشكل دائم ومحكم بخبرة وحس المحللين البشريين، ضمن أطر تنظيمية محددة بدقة لضمان الوضوح الكامل والمساءلة.

Appendix (الملحق)

"**الملحق (أ):** جدول مقارنة خوارزميات الذكاء الاصطناعي في الأمن السيبراني"

نوع الخوارزمية	الوصف المختصر	الاستخدامات	المزايا	العيوب
Machine Learning	يعتمد على بيانات سابقة لاستخراج أنماط	اكتشاف البرمجيات الخبيثة، تصنيف الترافيك	دقة جيدة وسريع	يعتمد على جودة البيانات
Deep Learning	شبكات عصبية متعددة الطبقات	كشف التهديدات المتقدمة	دقة عالية	يحتاج بيانات ضخمة
Supervised Learning	يعتمد على بيانات مصنّفة	كشف البرمجيات الخبيثة	نتائج دقيقة	غير فعال للهجمات الجديدة
Unsupervised Learning	يكتشف الأنماط الشاذّة	كشف الشذوذ	مناسب للهجمات الجديدة	نتائج خاطئة محتملة
Reinforcement Learning	يتعلم بالمكافأة والعقاب	الدفاع الذاتي	تعلم مستمر	يحتاج وقت تدريب
NLP	فهم النصوص البشرية	كشف البريد الاحتيالي	دقيق في كشف التصيّد	قد يخطئ في النصوص الغامضة
Genetic Algorithms	تحسين الحلول عبر محاكاة التطور	تحسين إعدادات الدفاع	تحسين مستمر	بطيء نسبياً
Graph Algorithms	تحليل العلاقات بين العقد	كشف البوت نت	ممتاز للسلوك الجماعي	معقد
Anomaly Detection	تمييز السلوك الطبيعي عن غير الطبيعي	IDS/IPS	يكشف هجمات Zero-day	نتائج خاطئة محتملة

" **الملحق (2)** : جدول التحديات والحلول في استخدام الذكاء الاصطناعي في الأمن السيبراني"

التحديات	الشرح	الحلول
هجمات التلاعب بالذكاء الاصطناعي (Adversarial Attacks)	باستطاعة المعتدين زرع معلومات غير صحيحة بغرض تضليل نماذج الذكاء الاصطناعي، مما يجعل ظهور المخاطر وكأنها تصرفات اعتيادية.	صنع تركيبات قادرة على الصمود أمام الاعتداءات، توظيف أساليب التدريب الخصم (Adversarial Training)، وإجراء تحسينات دورية على تلك التركيبات.
نقص البيانات عالية الجودة	قديُسفراستطلاع وتحليل المعلومات الهائلةعن اختراق لحرمة الأفراد المتمثلة في خصوصيتهم.	يتطلب الأمر تبني أسس الخصوصية منذ المراحل التخطيطية الأولى، بالإضافة إلى صياغة منظومة قانونية محكمة تضع حدوداً لاستغلال هذه البيانات.

التعقيد والتكلفة العالية	تشييد وتشغيل المنظومات الذكية المتطورة في مجال الحماية يتطلب استثمارات مالية ضخمة ويتطلب كفاءات متخصصة يصعب العثور عليها.	الاعتماد على نماذج متاحة للعامة ومفتوحة المصدر، واعتماد هياكل حوسبة سحابية قابلة للتكيف، وتأهيل موظفين ذوي مهارات خاصة.
الاعتماد الكلي على الذكاء الاصطناعي	ربما تتخلى بعض الهيئات عن الرصد التقليدي للأنظمة وتعتمد كلياً على التقنيات الذكية، وهذا الأمر قد يفتح ثغرات أمنية.	من الضروري دمج قدرات الذكاء الاصطناعي مع المعرفة البشرية عبر تبني نموذج "الإنسان في الحلقة" (Human-in-the-loop).
الإنذارات الكاذبة(False Positives)	قد تنتج عن الأنظمة تحذيرات غير صحيحة، مما يضع عبئاً كبيراً على كاهل فرق الأمن.	يتطلب ذلك الارتقاء بخوارزميات تحديد الحالات الشاذة، تطبيق منهجية تحليل السياق (Contextual Analysis).
تطور الهجمات بسرعة اكبر من النماذج	بإمكان بعض التهديدات المكتشفة حديثًا (Zero Day) تجاوز قدرات نماذج الذكاء الاصطناعي التي لم تتلق تدريبًا على هذا النوع من التكتيكات المستجدة.	يتطلب الأمر مواصلة صقل وتدريب النماذج المعتمدة، والتوظيف الفعال للتعلم غير المراقب (Unsupervised Learning) بهدف استبانة وتحديد الأنماط غير المألوفة.
النماذج غير القابلة للتفسير	تُصنَّف نماذج التعلّم العميق على أنها "صندوق أسود"، مما يُعقِّد عملية فهم المبررات وراء القرارات الأمنية المتخذة.	يتم اللجوء إلى توظيف تقنيات الذكاء الاصطناعي القابل للتفسير (XAI) بهدف تعزيز الوضوح ودعم فعالية عملية صنع القرار.

الاختصارات

AI : Artificial Intelligence
ML: Machine Learning
DL : Deep Learning
CNN : Convolutional Neural Network
RNN : Recurrent Neural Network
GDPR : General Data Protection Regulation
UEBA : User and Entity Behavior Analytics
IOT: Internet Of Things
IP : Internet Protocol
IBM Waston : IBM هو نظام ذكاء اصطناعي من شركة
XAI: Explainable Artificial Intellige

المراجع

[1] Rjoub, G., Al-Ebbini, O., Al-Fuqaha, A., Alomari, A., Krounbi, T., Al-Azawei, A., & Ahmad, N. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. IEEE Transactions on Network and Service Management, 20(4), 4811–4828.

[2] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.

[3] فضل الله، ه. ر .(2025). دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني: دراسة تحليلية للتحديات والحلول المستقبلية. *المجلة المصرية للدراسات المتخصصة*, *13*(46), 1341–1362.

[4] الغامدي، ع. س .(2025). الأمن السيبراني والذكاء الاصطناعي: حلول لإدارة أزمات البنية التحتية الرقمية. *Journal of the Association of Arab Universities for Research in Higher Education*, *45*(2), Article 5. https://doi.org/10.36024/1248-045-997-005

[5] Agarwal, S., Gupta, S., & Kumar, P. (2020). Natural language processing for cybersecurity: A review. *Journal of Cybersecurity Research*, *3*(2), 45–60.

[6] Shone, N., Balasingham, M., Al-Khateeb, B., & Al-Qurashi, M. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50.

[7] Dlamini, M. T., & Modiba, M. (2021). User and Entity Behavior Analytics (UEBA) Using Machine Learning for Insider Threat Detection: A Review. *Computers & Security*, *107*, 102319.

[8] Moradi, M., & Zulkernine, M. (2018). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50.

[9] Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2017). Classifying Phishing URLs Using Recurrent Neural Networks. *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, 1291–1300.

[10] Sahu, S. K., Singh, G., Sharma, A., & Goyal, N. (2020). Malware detection using machine learning techniques: A review. *Journal of Information Security and Applications*, *55*, 102597.

[11] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. *ACM Computing Surveys*, *41*(3), 15.

[12] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A Survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications*, *60*, 19–31.

[13] Nguyen, T. T., & Kim, J. (2020). Artificial Intelligence-Based Intrusion Detection and Prevention for IoT Security: A Survey. *IEEE Access*, *8*, 114011–114028.

[14] Ferrag, M. A., Friha, O., Moungla, K., Hamouda, O., & Dhelim, S. (2020). Deep learning-based intrusion detection systems: A systematic review. *Computer Communications*, *163*, 218–245. https://doi.org/10.1016/j.comcom.2020.08.012

[15] Sobh, T., & Elleithy, K. (2018). *Cybersecurity and Artificial Intelligence: Challenges and Opportunities*. Springer.

[16] Sourav Kumar Bhoi, Pani, S. K., Rath, M., & Mukherjee, A. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*.

[17] Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions. *Frontiers in Big Data*, *7*, Article 1497535.

[18] Alhajjar, E., Maxwell, P., & Bastian, N. D. (2020, April). *Adversarial Machine Learning in Network Intrusion Detection Systems*. arXiv. http://arxiv.org/abs/2004.11898

[19] Ferrag, M. A., Friha, O., Moungla, K., Hamouda, O., & Dhelim, S. (2020). Deep learning-based intrusion detection systems: A systematic review. *Computer Communications*, *163*, 218–245. https://doi.org/10.1016/j.comcom.2020.08.012

[20] Oladimeji, S., Egon, A., & Broklyn, P. (2024). *Bridging the skills gap in the age of automation*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4904939

[21] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

[22] جودة، ل. م. ع. س .(2024). ضوابط استخدام الذكاء الاصطناعي في مجال التسليح العسكري في ضوء مبادئ القانون الدولي الإنساني .*مجلة الدراسات القانونية والاقتصادية*.2326–2264 ,*10*(4), **العمري، ف. خ** .(2024) .تطبيقات الذكاء الاصطناعي في الأمن القومي للدول العربية: الفرص والتحديات .*المجلة العربية للعلوم الأمنية*.210–189 ,*40*(4),

[23] Sourav Kumar Bhoi, Pani, S. K., Rath, M., & Mukherjee, A. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*.

[24]Chan, K. C., Gururajan, R., & Carmignani, F. (2025). A Human–AI Collaborative Framework for Cybersecurity Consulting in Capstone Projects for Small Businesses. *Journal of Cybersecurity and Privacy*, *5*(2), 21.