

تعزيز الأمن السيبراني باستخدام التعلم الآلي دراسة مقارنة للأساليب التقليدية والتقنيات الذكية

د. إبراهيم بخي
جامعة ورقلة

ملخص:

يهدف المقال إلى استكشاف دور تقنيات التعلم الآلي في تعزيز فعالية الكشف عن الهجمات السيبرانية والتصدي للتهديدات الأمنية المتطورة، خاصة في ظل تصاعد وتيرة الهجمات وتعقيدها، حيث يناقش أهمية التعلم الآلي في تحليل البيانات واكتشاف الحالات الشاذة والتنبيه بالهجمات، مما يعزز القدرات الدفاعية، كما يستعرض التحديات المتعلقة بدمج التعلم الآلي في البنى التحتية للمؤسسات، مثل مخاوف الخصوصية وجودة البيانات.

بعد مراجعة وتحليل أدبيات الموضوع، أظهرت النتائج أن التعلم الآلي يوفر إمكانيات متقدمة للكشف عن التهديدات والاستجابة لها في الوقت الفعلي، ويتفوق على الأساليب التقليدية القائمة على التوقعات الثابتة، ومع ذلك يشدد المقال على ضرورة تطوير استراتيجيات تكيف متقدمة لمواجهة التحديات الناشئة وضمان الاستخدام الأخلاقي والفعال للتعلم الآلي في مجال الأمن السيبراني.

كلمات مفتاحية: أمن سيبراني، تهديدات أمنية، تعلم آلي، ذكاء اصطناعي، تعلم العميق، جودة البيانات.

Abstract:

The article aims to explore the role of machine learning techniques in enhancing the effectiveness of cyberattack detection and addressing evolving security threats, particularly in light of the increasing frequency and complexity of such attacks. It discusses the significance of machine learning in data analysis, anomaly detection, and attack prediction, thereby strengthening defensive capabilities. Additionally, the article examines challenges associated with integrating machine learning into organizational infrastructures, including privacy concerns and data quality issues.

Following a review and analysis of relevant literature, the findings indicate that machine learning offers advanced capabilities for real-time threat detection and response, surpassing traditional methods based on static signatures. Nevertheless, the article emphasizes the necessity of developing sophisticated adaptive strategies to address emerging challenges and ensure ethical and effective utilization of machine learning within cybersecurity.

Keywords: Cybersecurity, Security Threats, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Data Quality.

1. مقدمة:

يشهد الفضاء السيبراني تحولات متسارعة نتيجة تزايد حجم وتعقيد التهديدات الإلكترونية، لا سيما مع انتشار الحوسبة السحابية، إنترنت الأشياء، والتقنيات الرقمية الحديثة، في هذا السياق تواجه المؤسسات تحديات كبيرة في حماية أصولها المعلوماتية التي تستخدم أدوات تقليدية باتت محدودة الفعالية أمام هجمات متطورة مثل التهديدات المستمرة والمتقدمة وهجمات اليوم الصفر، وقد أدى ذلك إلى بروز الحاجة إلى اعتماد تقنيات ذكية ومرنة، وفي مقدمتها التعلم الآلي، كبديل فعال يتيح الكشف الاستباقي عن التهديدات والاستجابة لها في الزمن الحقيقي.

إشكالية الدراسة: رغم الوعود الكبيرة التي تقدمها خوارزميات التعلم الآلي في مجال الأمن السيبراني، لا تزال عملية دمجها ضمن الأطر الأمنية المؤسسية تواجه تحديات تقنية، أخلاقية، وتنظيمية. كما أن فعالية هذه التقنيات مقارنة بالأساليب التقليدية لم تحسم بعد بشكل قاطع في الأدبيات التطبيقية؛ انطلاقاً من هذا، تتمثل إشكالية الدراسة في التساؤل التالي: "إلى أي مدى يمكن لتقنيات التعلم الآلي أن تمثل بديلاً فعالاً للأساليب التقليدية في الكشف عن التهديدات السيبرانية والاستجابة لها".

أسئلة الدراسة: انطلاقاً من الإشكالية المطروحة، تسعى هذه الدراسة للإجابة عن مجموعة من التساؤلات المحورية التي تشكل الإطار المفاهيمي للتحليل، إذ تطرح بداية مسألة مدى قدرة الأساليب التقليدية للأمن السيبراني على مواجهة التهديدات المتقدمة والمتجددة، في ظل محدوديتها في الكشف عن الأنماط المعقدة أو التهديدات غير المعروفة. كما تستقصى الدراسة الكفاءة الفعلية لتقنيات التعلم الآلي في اكتشاف التهديدات السيبرانية والتنبؤ بها بدقة، من خلال تحليل الأداء التطبيقي لهذه الخوارزميات في البيئات المتغيرة. علاوة على ذلك، تتم دراسة مدى التفوق الكمي والنوعي الذي قد تحققه تقنيات الذكاء الاصطناعي مقارنة بالمقاربات التقليدية، لا سيما فيما يتعلق بسرعة الاستجابة، تقليل الإنذارات الكاذبة، والقدرة على المعالجة اللحظية. ولا تغفل الدراسة التحديات المتعددة التي تعيق عملية دمج هذه التقنيات، سواء من حيث البنية التقنية أو الاعتبارات الأخلاقية المتعلقة باستخدام البيانات الحساسة.

فرضية الدراسة: تُحسّن تقنيات التعلم الآلي بشكل جوهري من قدرات الكشف المبكر والاستجابة للتهديدات السيبرانية، مقارنة بالأساليب التقليدية، شريطة معالجة التحديات المتعلقة بجودة البيانات والتكامل البيئي والاعتبارات الأخلاقية.

أهداف الدراسة: تهدف هذه الدراسة إلى تقديم تحليل معمق لدور تقنيات التعلم الآلي في دعم وتعزيز الأمن السيبراني، وذلك من خلال تفكيك أوجه القصور التي تعاني منها الأساليب التقليدية المعتمدة في الكشف عن التهديدات السيبرانية، وتبسيط الضوء على مدى فعالية خوارزميات التعلم الآلي في تحسين قدرات الكشف المبكر والاستجابة الفورية للتهديدات السيبرانية، لا سيما في البيئات الرقمية الديناميكية والمعقدة، كما تسعى الدراسة إلى إجراء مقارنة منهجية بين المقاربات التقليدية والتقنيات الذكية من حيث الأداء والكفاءة والدقة في التصدي للهجمات المتقدمة، وإلى جانب ذلك، تسعى الدراسة إلى تحليل التحديات التقنية والتنظيمية والأخلاقية المرتبطة بتوظيف هذه التقنيات ضمن البنى التحتية الأمنية للمؤسسات، من حيث جودة البيانات، التحيزات الخوارزمية، وخصوصية المعلومات، ومن خلال هذا الإطار،

تسعى الدراسة إلى اقتراح مداخل بحثية وتطبيقية تعزز من فرص الدمج الآمن والفعال لتقنيات التعلم الآلي ضمن استراتيجيات الأمن السيبراني، بما يساهم في بناء منظومات دفاعية أكثر ذكاءً وتكاملاً.

1.1 الأمن السيبراني، وأهميته:

يشهد مجال الأمن السيبراني تطوراً متسارعاً بفعل تزايد التهديدات السيبرانية المتطورة والمتكررة، ومع انتشار التقنيات الرقمية وإنترنت الأشياء (IoT)، تواجه المؤسسات تحديات متزايدة لحماية أنظمتها المعلوماتية من مخاطر متنوعة تشمل البرمجيات الخبيثة، التصيد الاحتيالي، تسريبات البيانات، وهجمات تعطيل الخدمة؛ وفي المقابل يلجأ المهاجمون السيبرانيون إلى تطوير أساليبهم لاختراق الدفاعات التقليدية، مما يستدعي اعتماد حلول أمنية متقدمة تعتمد على الذكاء الاصطناعي والتحليلات التنبؤية لتعزيز قدرة المؤسسات على التصدي للهجمات وضمان حماية البنية التحتية الرقمية.

تواجه الأساليب التقليدية للأمن السيبراني، المعتمدة على القواعد الثابتة والكشف بالتوقيع، قصوراً واضحاً في التصدي للهجمات المتقدمة مثل هجمات اليوم الصفر (Zero-Day Attacks)، التي تُنفذ قبل الكشف عن الثغرات واستيعابها من قبل المصنعين، وفي هذا السياق يؤكد (Presswala et al., 2020, p. 375) أن هذه الأساليب تُعد غير فعالة أمام تهديدات غير معروفة مسبقاً، بينما تظهر تقنيات التعلم الآلي قدرة أفضل في رصد السلوكيات غير الطبيعية، كما تمثل التهديدات المستمرة المتقدمة (APTs: Advanced Persistent Threats) تحدياً بالغاً نظراً لطبيعتها التخريبية والخفية، مما يستلزم أنظمة دفاعية مرنة تعتمد على التعلم الذاتي، وهو ما تدعمه تقنيات الذكاء الاصطناعي، وفق ما بينه (Abaimov and Martellini (2022, pp. 4-5). ومن ثم أصبحت تقنيات الذكاء الاصطناعي، لا سيما التعلم الآلي، مكوناً محورياً في منظومات الدفاع السيبراني الحديثة، لما توفره من قدرات استباقية في كشف التهديدات والتعامل الفوري معها (Abaimov & Martellini, 2022, p. 5; Presswala et al., 2020, p. 376).

يساهم التعلم الآلي في إحداث تحول جذري في مجال الأمن السيبراني من خلال تمكين الأنظمة من استنتاج المعرفة من أنماط البيانات دون الحاجة إلى برمجة صريحة، فمن خلال تحليل كميات ضخمة من بيانات الشبكات، تستطيع خوارزمياته تحديد الحالات الشاذة والتنبؤ بالسلوكيات الضارة بدقة عالية، وتشير دراسة (Wasif, 2024) و (Shradha et al., 2024) إلى الدور الحاسم لهذه الخوارزميات في مواجهة التهديدات السيبرانية المتزايدة تعقيداً، كما تعد هذه التقنيات عنصراً رئيسياً في أنظمة كشف التسلل (IDS: Intrusion Detection Systems)، حيث تعتمد على تحليل حركة مرور الشبكة لرصد المؤشرات التي تكشف عن الهجمات المستمرة والجارية.

على الرغم من أن استخدام التعلم الآلي في الأمن السيبراني يعود إلى عدة عقود، فإن تطبيقه اكتسب شهرة في السنوات الأخيرة بفضل تحسين القدرة الحاسوبية وتوفر البيانات؛ سابقاً كان الاستخدام الأولي يركز على الكشف عن الشذوذات البسيطة، ولكن التقدم الحالي يعتمد على تقنيات التعلم العميق (DL) للتعرف على الأنماط المتطورة عبر

مجموعات بيانات متنوعة، ويعزز التعلم العميق القدرة على تحديد التهديدات غير المعروفة من خلال الكشف عن الأنماط الدقيقة التي تجاوزت الأساليب التقليدية.

علاوة على ذلك، تمتد تطبيقات التعلم الآلي لتشمل تصنيف البرمجيات الخبيثة وتصنيف رسائل البريد الإلكتروني المرسله بغرض التصيد؛ تسمح هذه المرونة للمؤسسات بتعزيز أوضاعها الأمنية بشكل ديناميكي، مما يساعد على تجنب الاعتماد على البروتوكولات الثابتة التي تتقادم بسرعة، وتشير التوقعات إلى نمو كبير في الاستثمار في حلول الأمن السيبراني المدفوعة بالذكاء الاصطناعي، باعتبار أن التعلم الآلي هو فرع أساسي من فروع الذكاء الاصطناعي، ورغم الإمكانيات الواعدة لتطبيق تقنيات التعلم الآلي في الأمن السيبراني، إلا أن دمجها مع البنى التحتية القائمة في المؤسسة يواجه تحديات تتطلب معالجة دقيقة، ومن أبرز هذه التحديات نذكر مخاوف الخصوصية، إذ يعتمد تدريب نماذج التعلم الآلي غالباً على بيانات حساسة يجب حمايتها من الوصول غير المسموح به (Abaimov & Martellini, 2022, p. 93; Khanna et al., 2020, p. 100)؛ إضافة إلى ذلك ينبغي الحفاظ على مستوى مرتفع من الشفافية في تصميم النماذج لضمان أن تكون آليات اتخاذ القرارات التلقائية مفهومة وقابلة للتدقيق، وهو ما يعد عنصراً حاسماً لتعزيز الثقة والمساءلة في استخدام الخوارزميات (Abaimov & Martellini, 2022, pp. 96–97).

تكمن خطورة هذه التهديدات في قدرتها على التموه داخل بيئة المؤسسة، حيث قد تتخذ شكل أنشطة تبدو مشروعة، مما يجعل عمليات الكشف عنها أكثر تعقيداً ويستدعي تطوير أساليب تحليلية متقدمة لتعزيز الاستجابة الأمنية الفعالة، للتصدي لها؛ ولذلك ينبغي على المؤسسات التي تعتمد بشكل متزايد على الحوسبة السحابية وتدمج تقنيات الذكاء الاصطناعي في استراتيجياتها الأمنية، أن تعتبر التعلم الآلي مكوناً جوهرياً في منظومتها الدفاعية، بدلاً من اعتباره مجرد أداة مساندة، فالتدابير الأمنية الفعالة لم تعد خياراً بل ضرورة حتمية، لا سيما في ظل التقديرات التي تشير إلى أن الجرائم السيبرانية قد تكبد المؤسسات بحلول سنة 2025، خسائر تصل إلى تريليونات الدولارات سنوياً (Carreiro, 2023 ; Salem et al., 2024).

تمثل الجريمة السيبرانية نشاطاً إجرامياً يستهدف الأنظمة والبيانات الرقمية لأغراض مثل الاحتيال، سرقة الأموال، الملكية الفكرية، البيانات الشخصية والمالية، تعطيل الأنظمة، أو تدمير البيانات؛ أما الهجمات السيبرانية فهي الأساليب المستخدمة لتنفيذها، كالبرمجيات الخبيثة، التصيد الاحتيالي، وبرامج الفدية؛ وبالتالي العلاقة بين الجريمة السيبرانية والهجمات السيبرانية هي علاقة الغاية بالوسيلة؛ وتتسبب هذه الجرائم بتكاليف كبيرة، كما يوضح الجدول التالي:

الجدول 1: توقعات لإحصائيات حول تكاليف الأمن السيبراني العالمي 2024 - 2031

الرقم	المؤشر الأمني	القيمة المتوقعة	ملاحظات
1	تكلفة الجرائم السيبرانية لسنة 2024	9.5 تريليون دولار	تعاادل مرتبة ثالث أكبر اقتصاد عالمي بعد الولايات المتحدة والصين
2	تكلفة الجرائم السيبرانية لسنة 2025	10.5 تريليون دولار	زيادة 15% مقارنة بسنة 2024
3	الإنفاق التراكمي على الأمن السيبراني بين 2021-2025	1.75 تريليون دولار	معدل نمو سنوي 15%
4	الوظائف الشاغرة في مجال الأمن السيبراني سنة 2024	3.5 مليون وظيفة	معدل البطالة في القطاع 0%
5	تكاليف أضرار برامج الفدية سنة 2021	20 مليار دولار	زيادة 57 ضعفا مقارنة بسنة 2015
6	تكاليف أضرار برامج الفدية سنة 2031	265 مليار دولار	هجوم كل 2 ثانيتين
7	حجم البيانات المطلوب حمايته سنة 2025	200 زيتابايت	50% منها مخزنة في السحابة
8	حجم سوق التأمين السيبراني سنة 2025	14.8 مليار دولار	معدل نمو سنوي مركب 15%
9	حجم سوق التأمين السيبراني سنة 2031	34 مليار دولار	
10	تكلفة الجرائم المشفرة سنة 2025	30 مليار دولار	زيادة بنسبة 15% سنويا

المصدر: (Morgan, 2024) مستخلص بتصرف.

تتضافر هذه البيانات الإحصائية معا، لترسم صورة شاملة تكشف عن سلسلة من الاستنتاجات الاستراتيجية التي تعكس التحولات العميقة الجارية في حقل الأمن السيبراني، ويتجلى هذا الواقع من خلال عدة محاور رئيسية تبرز تدريجيا عبر تحليل الظروف الحالية والمستقبلية.

في البداية، يظهر تحول جوهري في ميزان القوى داخل الفضاء السيبراني، حيث يميل ميزان السيطرة بشكل متزايد لصالح المهاجمين، إذ يتمتع هؤلاء بتفوق مستمر يتجسد في وفرة الموارد المالية والبشرية، إلى جانب القدرات التقنية المتطورة، مما يرسخ هيمنتهم ويضع المدافعين عن الأنظمة في موقف دفاعي صعب (Abaimov & Martellini, 2022, pp. 41-42).

وفي سياق متصل، تتجلى أزمة الموارد البشرية كعنصر عقبة بنوية تواجه القطاع، حيث يعاني المجال من عجز واضح في الكوادر المتخصصة ذات الكفاءة العالية (Abaimov & Martellini, 2022, p. 45)، وهو ما يستدعي استثمارات مكثفة في التعليم والتدريب المهني لتأهيل قوى عاملة قادرة على مواجهة التهديدات المتسارعة والمتغيرة (Mittal, 2023, p. 2)، علاوة على ذلك يشهد المجال انتقالا ملحوظا نحو نموذج إدارة مخاطر أكثر شمولية، متجاوزا بذلك الاستراتيجيات التقليدية المرتكزة حصريا على الوقاية، ليتضمن الكشف المبكر، والاستجابة للحوادث، وآليات الحد من المخاطر (Bhatt et al., 2020, pp. 326-327)، وفي الوقت ذاته، يفرض النمو الهائل في حجم البيانات، المصاحب بالتحول نحو الحوسبة السحابية، تحديات متزايدة في حماية البيانات، مما يتطلب حلولاً أمنية متقدمة قائمة على التشفير والتحكم في الوصول (Jordan & Mitchell, 2020, pp. 371-372)، وانطلاقا من هذه التحديات، تبرز الحاجة إلى إعادة تقويم الاستراتيجيات الحالية، من خلال تبني نهج شامل يدمج تقنيات حديثة مثل التعلم الآلي مع

كفاءات بشرية مدربة، ضمن أطر تنظيمية مرنة ومتلائمة (Abaimov & Martellini, 2022, p. 97)، وفي هذا السياق يشكل التعلم الآلي عاملاً محورياً في تشكيل بيئة الأمن السيبراني الحديثة، حيث يوفر إمكانيات متقدمة لتعزيز القدرات الدفاعية، لكنه في الوقت ذاته يطرح تحديات جديدة تتطلب استراتيجيات تكيف متقدمة عبر مختلف القطاعات.

2.1 مكانة التعلم الآلي في الأمن السيبراني:

لقد أصبح التعلم الآلي مكوناً حيوياً في الأمن السيبراني، حيث يعالج التهديدات السيبرانية المعقدة والمتزايدة التي تواجهها المنظمات، ومع تحسين المجرمين السيبرانيين لتكتيكاتهم، غالباً ما تفشل التدابير الأمنية التقليدية، مما يبرز ضرورة التقنيات المتقدمة مثل التعلم الآلي لتحسين اكتشاف التهديدات والاستجابة لها.

إن تزايد الجرائم السيبرانية أمر مضر بالمؤسسات والاقتصاد، حيث تشير التوقعات إلى أن التأثير المالي العالمي قد يرتفع من 9.22 تريليون دولار سنة 2024 إلى حوالي 13.82 تريليون دولار بحلول سنة 2028 (Tulsa, 2024)، هذا الاتجاه مدفوع بعدة عوامل، بما في ذلك الزيادة السريعة في أجهزة إنترنت الأشياء (IoT) التي توسع من ساحة الهجوم، حيث يستغل المهاجمون هذه الأجهزة المتصلة لتنفيذ هجمات على نطاق واسع، وغالباً ما تحاكي سلوك المستخدمين الشرعيين (Cassetto, 2020)، هذه التهديدات المتطورة تستدعي التحول من حلول الأمن الثابتة إلى حلول ديناميكية قادرة على التكيف مع التحديات الجديدة.

يتفوق التعلم الآلي في هذا البيئة بسبب قدرته على معالجة مجموعات من البيانات الضخمة بسرعة واكتشاف الأنماط التي تشير إلى تهديدات محتملة، على عكس الأساليب الأمنية التقليدية المعتمدة على القواعد الثابتة أو التوقعات التي تكون غالباً غير فعالة ضد الثغرات الجديدة، لأن أنظمة التعلم الآلي تستخدم البيانات التاريخية لاكتشاف الشذوذات الناشئة (Wasif, 2024) وتسمح تقنيات مثل التعلم الخاضع للإشراف وغير الخاضع للإشراف لهذه الأنظمة بتحسين قدراتها في اكتشاف التهديدات مع مرور الوقت.

من الفوائد الرئيسية للتعلم الآلي في الأمن السيبراني قدرته على التحليل في الوقت الفعلي، وهذا ما يمكن الخوارزميات الحالية من تقييم تدفقات البيانات الواردة وتقييم سلوك الشبكة على الفور، مما يسمح للمؤسسات بالاستجابة بسرعة لأي خروقات محتملة (Shah, 2022)، بالإضافة إلى ذلك يمكن لأنظمة الاستجابة التلقائية المدعومة بالتعلم الآلي تصنيف التهديدات وتحديد أولوياتها حسب شدة الخطر، مما يخفف من العبء على المحللين البشريين الذين يتعاملون مع بيانات معقدة وضخمة.

أصبح للتعلم العميق (وهو أحد فروع التعلم الآلي)، دور محوري في الأمن السيبراني، حيث يستخدم الشبكات العصبية (Neural Networks) المتخصصة في التعرف على الأنماط المعقدة عبر أنواع مختلفة من المدخلات مثل الصور أو النصوص، وتكمن قوة التعلم العميق في قدراته على استخراج الميزات، مما يكشف عن خصائص قد تكون غير

ملحوظة من قبل، والتي قد تشير إلى أعمال ضارة (Salem et al., 2024)، وهذا لا يعزز فقط اكتشاف البرمجيات الخبيثة، بل يساعد أيضا في التعرف على التهديدات الداخلية، التي تعتبر من التحديات الكبرى للمؤسسات في الوقت الحالي.

علاوة على ذلك، يدعم التعلم الآلي جهود استخبارات التهديدات من خلال تمكين المنظمات من تطوير نماذج تنبؤية تتوقع الهجمات المستقبلية إستنادا على الاتجاهات المتطورة والحوادث السابقة، إن القدرة على التنبؤ بالتهديدات المحتملة تسهم في اتخاذ تدابير استباقية، مما يعزز الدفاعات ضد مسارات الهجوم المتقدمة (Jada & Mayayise, 2024)، هذه الميزة الاستراتيجية تمكن المؤسسات من البقاء في صدارة مواجهة خصومها الذين يعملون على تحسين تكتيكاتهم باستمرار. يسهم تبني أطر التعلم الآلي في تعزيز الكفاءة التشغيلية من خلال الأتمتة، ويمكن تبسيط المهام الروتينية مثل مراقبة أنماط المرور في الشبكة أو تحليل سجلات النظام، باستخدام الخوارزميات المخصصة لهذه الوظائف، ونتيجة لذلك يمكن للفرق المكلفة بالأمن السيبراني التركيز على القضايا الأكثر تعقيدا والتي تتطلب البصيرة البشرية، بينما تتعامل التكنولوجيا مع العمليات الأقل أهمية بكفاءة.

ومع ذلك، توجد تحديات في دمج التعلم الآلي في البنى التحتية الحالية للأمن السيبراني، ومن القضايا الرئيسية الاعتماد على بيانات تدريب عالية الجودة، حيث يمكن أن تؤدي مجموعات البيانات المشوهة أو المتحيزة إلى إرباك النماذج، مما يؤدي إلى نتائج غير صحيحة في اكتشاف التهديدات، بالإضافة إلى ذلك قد يستهدف الخصوم أنظمة التعلم الآلي باستخدام تكتيكات لتجاوز هذه الخوارزميات، وهو ما يعرف بالهجمات المضادة.

تواجه المؤسسات تحديات متعددة عند تنفيذ حلول التعلم الآلي، تتراوح بين القيود المالية والاعتبارات الأخلاقية المتعلقة بالخصوصية، بالإضافة إلى تعقيد دمج هذه التقنيات ضمن البنية التحتية الحالية لأنظمة الأمن السيبراني؛ يتطلب هذا التكامل استثمارات كبيرة في الموارد البشرية والتكنولوجية لضمان تطبيق فعال ومستدام لهذه الحلول، ومع ذلك يصبح من الضروري أن تستثمر المؤسسات مواردها ورؤيتها الاستراتيجية في تطوير ممارسات أمن سيبراني قوية تعتمد على تقنيات متقدمة مثل التعلم الآلي، حيث يمكن لهذه التقنيات أن تحسن بشكل كبير من قدرة الأنظمة على اكتشاف التهديدات السيبرانية والاستجابة لها في الوقت الفعلي.

علاوة على ذلك فإن إدراك الدور الحاسم للتعلم الآلي في تعزيز الأمن السيبراني، يسهم في تمكين المؤسسات من التكيف مع التهديدات المتزايدة التي تستهدف الأصول الرقمية على نطاق عالمي، ويقتضي ذلك ليس فقط تحسين قدرة الأنظمة على تحليل الأنماط غير العادية، ولكن أيضا تطوير استراتيجيات استباقية يمكنها التنبؤ بالهجمات قبل وقوعها، مما يجعل التعلم الآلي تطورا جوهريا في استراتيجيات الحماية الحديثة، ومع استمرار تطور هذه التهديدات يصبح تعزيز الوعي الأمني والتدريب المستمر للعاملين في المجال ضرورة أساسية لضمان تحقيق أقصى استفادة من هذه التقنيات المتقدمة.

2. منهجية التحليل:

1.2 مراجعة الأدبيات:

أدى التزايد المستمر في تعقيد وتكرار التهديدات السيبرانية إلى تسليط الضوء على أهمية تطبيقات التعلم الآلي في مجال الأمن السيبراني، فقد أكد (Shah (2022 أن دمج تقنيات الذكاء الاصطناعي -التعلم الآلي- يعد عنصراً أساسياً في تطوير أنظمة أمنية قادرة على التكيف بفعالية مع التهديدات الناشئة، وتعتمد التدابير الأمنية التقليدية على أطر قائمة على قواعد صارمة، غالباً ما تكون غير كافية لمواجهة الأنواع الجديدة والمتطورة من الهجمات، وفي المقابل توفر منهجيات التعلم الآلي استجابات أكثر مرونة من خلال تحليل الأنماط الكامنة في كميات هائلة من البيانات، مما يسمح باكتشاف التهديدات التي قد لا تتمكن الأساليب التقليدية من رصدها بدقة.

يعتمد التعلم الآلي في الأمن السيبراني على قدرته الفائقة في كشف الشذوذات، مما يجعله أداة حيوية في رصد التهديدات الناشئة وتعزيز استراتيجيات الحماية الرقمية، إذ تعتمد هذه التقنيات على تحليل البيانات التاريخية لتحديد الأنماط الطبيعية ضمن الشبكة (Wasif, 2024)، مما يسمح باكتشاف أي انحرافات قد تكون مؤشراً على خروقات أمنية محتملة، فإذا كان أحد المستخدمين يصل عادة إلى مجموعة محدودة من الملفات، ثم قام فجأة بمحاولة تنزيل كميات كبيرة من البيانات الحساسة، فقد يشير ذلك إلى نشاط مشبوه يستدعي التدخل الفوري، ولتعزيز دقة وموثوقية عمليات الكشف، يتم تدريب نماذج التعلم الآلي باستخدام استراتيجيات تعتمد على التعلم الخاضع للإشراف وغير الخاضع للإشراف، مما يمكنها من التعرف بفعالية على الأنماط الشاذة وتقديم استجابات أمنية أكثر تكيفاً مع طبيعة التهديدات المتطورة (Alshathry et al., 2024).

تعزز الأبحاث الحديثة توظيف خوارزميات التعلم الآلي في الأمن السيبراني، حيث أثبت التعلم الآلي الخاضع للإشراف فعاليته في اكتشاف التسلل، بينما تكشف التقنيات غير الخاضعة للإشراف التهديدات غير المعروفة (Salem et al., 2024)، كما تبرز النماذج المتقدمة، مثل الشبكات العصبية البيانية والتعلم المعزز، في تحليل العلاقات المعقدة وتعزيز استراتيجيات الاستجابة للتهديدات (Alshathry et al., 2024)، مما يساهم في تطوير أنظمة أمنية أكثر ذكاءً ومرونة.

من خلال الاستفادة من تحليلات البيانات في الوقت الفعلي ودمج تدفقات استخبارات التهديدات، يمكن للمؤسسات مراقبة إشارات الاختراق بشكل نشط (AppOmni, 2024)، يساهم هذا الإشراف المستمر في تسريع التعرف على التهديدات الناشئة واتخاذ الإجراءات التصحيحية.

شدد Salem et al. على أهمية دمج خوارزميات التعلم العميق مع الاستراتيجيات الميتاهيرستيكية (Metaheuristic strategies) لتعزيز دقة اكتشاف التهديدات في مختلف سيناريوهات الهجمات السيبرانية، بما في ذلك البرمجيات الخبيثة والتسلل الشبكي، (Salem et al., 2024) كما أن الضرورة تستدعي تطوير أطر عمل منهجية

لتقييم فعالية تقنيات الذكاء الاصطناعي في مواجهة التهديدات السيبرانية المتطورة، مما يساهم في تحسين استراتيجيات الدفاع الرقمي وتكييفها مع المشهد الأمني المتغير.

تعتمد مؤسسات مثل CrowdStrike على استراتيجيات دفاع متعددة الطبقات، تدمج تقنيات التعلم الآلي عبر منصاتها المختلفة وتستخدم أنظمتها نماذج قائمة على الحوسبة السحابية وأخرى مدمجة في الأجهزة للكشف الديناميكي عن التهديدات والاستجابة لها، وذلك عبر جميع المراحل، ما قبل التنفيذ وأثناء التشغيل وما بعد التنفيذ (Stanham, 2023)، ويساعد هذا النهج في التعرف الفوري على التهديدات وتعزيز الدفاعات المستقبلية من خلال التدريب المستمر لمواجهة أساليب الهجوم الجديد، ومع ذلك، لا تزال هناك تحديات تواجه نشر هذه التقنيات المتقدمة، إذ تعد قضايا تحيز النماذج وجودة البيانات والاعتبارات الأخلاقية عوامل حاسمة عند دمج تقنيات التعلم الآلي في البنى التحتية الأمنية (Shah, 2022)، علاوة على ذلك قد يطور المهاجمون المتقدمون استراتيجيات للتحايل على نماذج التعلم الآلي، مما يؤكد الحاجة إلى دفاعات مرنة تتطور بمرور الوقت من خلال آليات التغذية الراجعة المستمرة في بيئات التعلم المعزز (Dunsin et al., 2024a).

بناءً على ما سبق من تحليل، لا تزال هناك فجوة بحثية تتعلق بالتحديات التشغيلية الأوسع التي تواجهها المؤسسات عند دمج الحلول المدعومة بالذكاء الاصطناعي (Kaur et al., 2023)، وتكشف الأدبيات عن موضوعات جوهرية تتعلق بفعالية تطبيقات التعلم الآلي الحالية، مما يسلط الضوء على القيود المرتبطة بعمليات النشر الفعلي، بما في ذلك مدى جاهزية البنية التحتية وإمكانية تطبيق هذه التقنيات عبر الهياكل التنظيمية المتنوعة (Salem et al., 2024), (Dixit & Silakari, 2021).

على الرغم من هذه التحديات، ستسهم التطورات التكنولوجية المستمرة في إعادة تشكيل أساليب الدفاع التي تعتمد عليها المؤسسات لمواجهة التهديدات السيبرانية المتزايدة التعقيد، وتوفر قدرة التعلم الآلي على معالجة كميات هائلة من البيانات رؤى معمقة حول نقاط الضعف الأمنية، مما يمكن المؤسسات من الاستجابة السريعة لإحباط الهجمات قبل تصاعدها، كما تتيح الابتكارات مثل التعلم المتحد (Federated Learning) - نموذج تعلم آلي لامركزي يتيح تدريب النماذج عبر أجهزة متعددة دون مشاركة البيانات الخام، حيث تبقى البيانات محلية، بينما يتم إرسال تحديثات النموذج إلى خادم مركزي لتحسينه - فرصاً واعدة من خلال تمكين النماذج من التدريب عبر شبكات موزعة مع الحفاظ على خصوصية المعلومات الحساسة، وهو عامل أساسي لضمان الامتثال للوائح حماية البيانات.

يطور الباحثون رؤى متعمقة حول هذه التكاملات، ويسعون إلى تحقيق توازن بين التقدم التكنولوجي والاعتبارات الأخلاقية، مما يعزز فرص تحقيق بيئات رقمية آمنة مدعومة بالذكاء الاصطناعي، ويتطلب دمج هذه التقنيات المتطورة في استراتيجيات الأمن السيبراني تزويد المتخصصين بالمهارات اللازمة لمواكبة التهديدات المتسارعة.

2.2 معايير اختيار دراسات الحالة:

عند اختيار دراسات الحالة لاستخدام التعلم الآلي في الأمن السيبراني، من الضروري إنشاء إطار عمل يعكس التفاعل بين كلا المجالين، تتضمن عملية الاختيار عدة معايير رئيسية لضمان أن الدراسات المختارة تظهر بفعالية أهمية التعلم الآلي في الأمن السيبراني، بينما تسمح بإجراء مقارنات ذات مغزى عبر المنهجيات والنتائج.

أولاً، يعد ارتباط الدراسات بمشاكل الأمن السيبراني المحددة أمراً بالغ الأهمية، يجب النظر في الحالات التي تعالج تهديدات أو ثغرات أمنية ملموسة فقط، ويتم إعطاء الأولوية للدراسات التي تركز على طرق الهجوم، تقنيات اكتشاف التهديدات، استراتيجيات الوقاية، أو منهجيات الاستجابة للحوادث، ويشمل ذلك مجموعة من الحوادث السيبرانية مثل هجمات البرمجيات الخبيثة، مخططات التصيد، هجمات تعطيل الخدمة، والتهديدات المستمرة المتقدمة (APTs)؛ كما ورد في (Salem et al., 2024)، فإن تصنيف هذه الحوادث يساعد في تحديد تطبيقات التعلم الآلي الفعالة المناسبة للتحديات الأمنية المختلفة.

ثانياً، من الضروري أن تتمتع دراسات الحالة المختارة بمنهجية صلبة، حيث يجب أن تعتمد الأبحاث على منهجيات رصينة في جميع مراحل التصميم والتنفيذ وتحليل النتائج، وتؤثر مصداقية هذه المنهجيات بشكل كبير على شرعية الاستنتاجات المتعلقة بفعالية التعلم الآلي في الحد من المخاطر السيبرانية، فقد أشار Dunsin et al. (2024b) أن استخدام خوارزميات قوية مثل مصنفات الغابات العشوائية (Random Forest classifiers) يعزز دقة الاكتشاف ويزيد من موثوقية النتائج.

يؤدي الوصول إلى بيانات عالية الجودة دوراً جوهرياً في عملية اختيار دراسات الحالة، يعتمد نجاح نماذج التعلم الآلي بشكل كبير على توفر مجموعات بيانات تدريبية عالية الجودة تمثل بدقة بيئات التهديد الحالية، وقد أشارت Stanham, (2023) إلى أن مجموعات البيانات الكبيرة تعد ضرورية لتدريب نماذج قادرة على اكتشاف التهديدات الجديدة دون الوقوع في نتائج إيجابية أو سلبية كاذبة، لذلك فإن الدراسات التي تطرح استراتيجيات فعالة للحصول على البيانات أو تقترح أساليب مبتكرة لإنتاج بيانات اصطناعية لغرض التدريب تستحق اهتماماً خاصاً.

تعتبر أيضاً مقاييس الأداء المستخدمة لتقييم تطبيقات التعلم الآلي في كل دراسة حالة ذات أهمية كبيرة، فمن الضروري أن تعتمد الدراسات على مقاييس موحدة إلى جانب التقييمات النوعية التي تعكس رضا المستخدمين عن الحلول المطبقة، ويؤدي الالتزام بمؤشرات الأداء المعترف بها، كما وضح سالم وآخرون (Salem et al., 2024) إلى تسهيل المقارنات الموضوعية بين التطبيقات المختلفة.

ومن المهم فحص مدى تكامل هذه الدراسات مع أطر الأمن السيبراني القائمة حالياً، إذ أن تقييم الحالات التي نجحت فيها أدوات التعلم الآلي في الاندماج مع الأنظمة التقليدية يوفر رؤى حول جاهزية هذه الأدوات من الناحية

التشغيلية وقدرتها على التكيف، وهو جانب رئيسي تم تسليط الضوء عليه ضمن التحديات المذكورة في تقرير (Sangfor, 2024).

تعد الشمولية الجغرافية والسياقية أمرا مهما عند إختيار دراسات الحالة، نظرا لاختلاف ممارسات الأمن السيبراني باختلاف المناطق الجغرافية نتيجة عوامل تنظيمية وثقافية متباينة (Shah, 2022) وبالتالي فإن التنوع الجغرافي في دراسات الحالة يعمق فهم المنهجيات المستخدمة في تطبيقات التعلم الآلي؛ كذلك، من الضروري مراعاة الاعتبارات الأخلاقية المتعلقة باستخدام البيانات لضمان الالتزام باللوائح وتعزيز الاستخدام العادل للذكاء الاصطناعي، فالدراسات التي تتناول قضايا الخصوصية أو شفافية الخوارزميات تساهم في تعزيز الثقة بين الأطراف المعنية، وهو أمر جوهري عند اعتماد التقنيات الحساسة مثل التعلم الآلي (Sangfor, 2024).

وأخيرا، يجب أن توثق دراسات الحالة بوضوح القيود والتحديات التي واجهتها أثناء التنفيذ، بهدف الكشف عن أي تحيزات محتملة في النماذج أو البيانات (Sangfor, 2024)، إن توضيح هذه القيود يوجه الأبحاث المستقبلية ويحافظ على واقعية التوقعات بشأن قدرات التعلم الآلي وحدوده، وبذلك يمكن تحديد المسار الأمثل لتطوير تقنيات التعلم الآلي في مواجهة التهديدات السيبرانية مستقبلا.

3.2 تقنيات تحليل البيانات:

تعتبر منهجيات تحليل البيانات في التعلم الآلي للأمن السيبراني، جد مهمة لاكتشاف ومعالجة التهديدات السيبرانية، عادة ما تتضمن الاستراتيجية الشاملة عدة مراحل: جمع البيانات، المعالجة المبدئية، اختيار الميزات، اختيار الخوارزميات، وتقييم النماذج، وتضمن كل مرحلة أن نماذج التعلم الآلي تتعلم بفعالية من البيانات التاريخية وتعمم على المدخلات الجديدة.

المرحلة الأولى هي جمع البيانات، والتي تتضمن جمع مجموعات البيانات التي تعكس الأنشطة الطبيعية والسلوكيات الشاذة في بيئات الشبكة، كما ورد في (Gottsegen & Urwin, 2023)، قد يكون من الصعب الحصول على بيانات عالية الجودة بسبب حساسية المعلومات المتعلقة بالأمن، وغالبا ما يعتمد خبراء الأمن السيبراني على السجلات التاريخية من حركة مرور الشبكة، أحداث النظام، إجراءات المستخدم، واستخبارات التهديدات لإنشاء مجموعات بيانات التدريب.

بعد ذلك تأتي المعالجة المبدئية، التي تقوم بتنظيف البيانات عن طريق إزالة الضوضاء والتفاصيل غير ذات الصلة التي قد تؤثر على أداء التعلم الآلي، وتضمن عملية تطبيع البيانات التناسق عبر الميزات من خلال تحجيمها إلى نطاق مشترك، بينما يتم أيضا استخدام تقنيات مثل إزالة القيم الشاذة (Palo Alto Networks, 2025a)، بعد ذلك تأتي هندسة الميزات، حيث يتم اختيار الميزات ذات الصلة التي تساهم في النمذجة التنبؤية، مما يقلل من الأبعاد (Shradha et al., 2024).

يعد اختيار الميزات أمراً بالغ الأهمية في أداء النماذج، ويهدف إلى تحديد الخصائص الموجودة ضمن مجموعة البيانات التي تتمتع بأكبر قدرة على التنبؤ بنتائج الأمن السيبراني، وقد تعتمد الطرق التقليدية في اختيار الميزات على تمثيل الخصائص في صورة متجهات مسطحة، ما قد يؤدي إلى إغفال العلاقات الهامة الكامنة في البنى الهرمية، نتيجة لذلك برزت الحاجة إلى استخدام تمثيلات متقدمة مثل الرسوم البيانية والبنى الرياضية متعددة الأبعاد التي تمثل البيانات المعقدة (Kaur et al., 2023).

وبعد اختيار الميزات، تأتي مرحلة اختيار الخوارزميات وتدريب النماذج، ويمكن تطبيق خوارزميات متنوعة من التعلم الآلي بحسب المهمة المطلوبة، مثل تصنيف التهديدات أو اكتشاف الحالات الشاذة (Sailpoint.com, 2023)، ويتطلب التعلم الخاضع للإشراف (Supervised Learning) مجموعات بيانات معنونة تتيح لخوارزميات الانحدار اللوجستي أو الغابات العشوائية أو غيرها، التعلم من الأمثلة التاريخية، أما التعلم غير الخاضع للإشراف (Unsupervised Learning)، فيبحث عن أنماط ضمن بيانات غير معنونة، وهو مفيد في تجميع السلوكيات المشابهة التي قد تشير إلى وجود تهديدات.

بعد اختيار الخوارزميات المناسبة وتدريبها، يجب تقييم أدائها بدقة ومن الضروري أيضاً ضمان قابلية تفسير النماذج لتعزيز ثقة المستخدمين، مع استمرار مراقبتها بعد النشر لمواجهة الطبيعة المتغيرة للتهديدات السيبرانية التي يقوم فيها المهاجمون بتعديل استراتيجياتهم استجابة للدفاعات التي تصادفهم؛ ومع تطور تطبيقات التعلم الآلي نحو الأنظمة اللحظية مثل تقنيات التعلم المعزز (Reinforcement Learning)، تزداد الحاجة إلى تقنيات مرنة تتكيف مع البيانات الجديدة، كاستخدام تقنيات الدمج التي تجمع بين عدة نماذج في نموذج تنبؤي قوي لتعزيز الدقة في اكتشاف التهديدات المختلفة بشكل فعال ودقيق، وهذا ما يمكن ملاحظته في دراسة (Shradha et al., 2024)، التي وضحو فيها أشكالاً من الهجمات كحجب الخدمة والتصيد وحقن البرمجيات الخبيثة؛ وفي النهاية يتطلب التنفيذ الناجح للتعلم الآلي في الأمن السيبراني إشرافاً بشرياً مستمراً يوفر سياقاً تحليلياً إضافياً يعزز الاستجابة السريعة للتهديدات المحتملة. ولتدعيم التحليل، نرى أنه من المستحسن، تقديم لمحة عامة عن استخدام خوارزميات التعلم الآلي لتعزيز الأمن السيبراني، من خلال سرد الأنواع، التطبيقات، المزايا والتحديات:

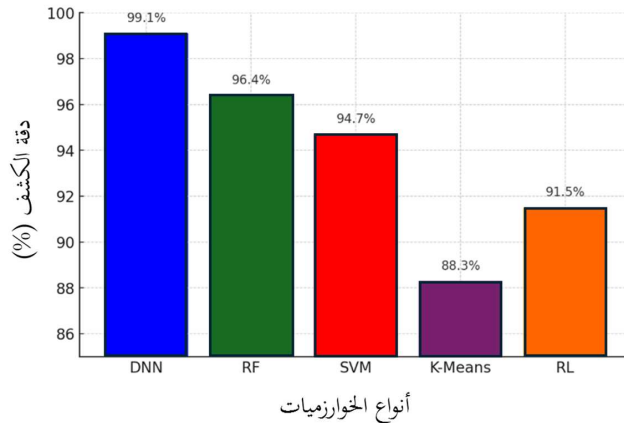
جدول 2: خوارزميات التعلم الآلي الشائعة في الأمن السيبراني وتطبيقاتها

نوع الخوارزمية	التطبيقات في الأمن السيبراني	مزاياها	تحدياتها
الغابات العشوائية RF	اكتشاف التسلل، تصنيف البرمجيات الخبيثة	دقة عالية، مقاومة للإفراط في الملاءمة	تحتاج موارد حاسوبية كبيرة
الشبكات العصبية العميقة DNN	اكتشاف الشذوذات، تحليل سلوك المستخدم	فعالة مع البيانات المعقدة، قدرة عالية على التعميم	تتطلب بيانات تدريب ضخمة، صعوبة التفسير
التعلم المعزز RL	الاستجابة الآلية للحوادث، التحسين المستمر	التكيف مع البيئات المتغيرة، التعلم المستمر	طويلة التدريب، غير مستقرة في بعض الحالات
خوارزمية التجميع k-means	اكتشاف التجمعات غير الطبيعية، تقسيم التهديدات	بسيطة، تعمل مع البيانات غير المصنفة	حساسة للقيم المتطرفة، تتطلب تحديد عدد المجموعات مسبقاً
آلات المتجهات الداعمة SVM	تصنيف البريد العشوائي، اكتشاف الاختراق	فعالة مع البيانات عالية الأبعاد، أداء جيد مع مجموعات صغيرة	تحتاج ضبط معلمات دقيق

المصدر: مستنبط من تحليل أدبيات المقال.

يوضح الجدول أعلاه، أن الخوارزميات المختلفة تخدم أغراضاً متباينة في الأمن السيبراني، وكل منها يتميز بخصائص تجعله أكثر ملاءمة لنوع معين من التهديدات، لكن لا توجد خوارزمية واحدة مثالية لكل السيناريوهات، لذا فإن دمج أكثر من خوارزمية في نظام أمني شامل قد يكون الحل الأمثل لمواجهة تعقيدات الجرائم السيبرانية الحديثة (Sagar et al., 2020)، بالإضافة إلى ذلك تطوير خوارزميات هجينة تجمع بين دقة التصنيف وكفاءة المعالجة والتكيف المستمر يمكن أن يعزز فعالية الحلول الأمنية في المستقبل (Salem et al., 2024).

شكل 1: مقارنة دقة خوارزميات التعلم الآلي في اكتشاف الهجمات السيبرانية



المصدر: مستنبط من تحليل (Salem et al., 2024)

يوضح الشكل السابق، أهمية اختيار الخوارزمية المناسبة لاكتشاف الهجمات السيبرانية وفقا لمتطلبات النظام الأمني، حيث توفر الشبكات العصبية العميقة (DNN) أعلى مستوى من الدقة، مما يجعلها الخيار الأفضل للأنظمة المتقدمة، لكنها تتطلب موارد حاسوبية كبيرة، في حين يمكن استخدام الغابات العشوائية (RF) وآلات المتجهات الداعمة (SVM) كبدايات موثوقة في البيئات ذات الإمكانيات المحدودة، نظرا لتوازنها بين الأداء وكفاءة الموارد، أما خوارزمية K-Means، فرغم بساطتها إلا أنها الأقل كفاءة في الكشف عن التهديدات السيبرانية، مما يجعلها غير مناسبة كأداة رئيسية، لكنها قد تكون مفيدة في تحليل البيانات غير المصنفة؛ ومن هذا المنطلق فإن الحل الأمثل هو دمج أكثر من خوارزمية في نظام أمني هجين للاستفادة من نقاط القوة لكل خوارزمية وتحقيق مستوى مرتفع من الحماية ضد الهجمات السيبرانية المتطورة.

3. النتائج:

1.3 فعالية أدوات التعلم الآلي:

أثبتت حلول التعلم الآلي فعاليتها في تعزيز الأمن السيبراني من خلال رفع معدلات اكتشاف التهديدات وتقليص أوقات الاستجابة في مواجهة التهديدات السيبرانية المعقدة، وتشير الدراسات إلى أن أدوات التعلم الآلي تعتمد على استراتيجيات مدعومة بالبيانات لتحديد الأنماط والشذوذ في مجموعات البيانات الضخمة التي غالبا ما تغفلها الأنظمة التقليدية، وتتسم هذه الخوارزميات بقدرتها على التعلم المستمر من مدخلات البيانات الجديدة، مما يمكنها من التعرف على التهديدات المعروفة ومتجهات الهجمات الجديدة باستخدام تقنيات اكتشاف الشذوذ (Shah, 2022). إحدى المزايا الأساسية للتعلم الآلي هي قدرته على معالجة البيانات غير المنظمة مثل حركة مرور الشبكة وسلوك المستخدمين، مما يؤدي إلى تحسين قدرات اكتشاف التهديدات والتحليلات التنبؤية للثغرات الأمنية، ويسمح ذلك للمؤسسات بتنفيذ دفاعات استباقية قبل وقوع الهجمات (Wasif, 2024)، ومن خلال توظيف أساليب التعلم الخاضعة وغير الخاضعة للإشراف، تتمكن نماذج التعلم الآلي من كشف التهديدات الخفية التي تتجنب الكشف التقليدي المستند إلى التوقع.

بينت التطبيقات العملية فعالية التعلم الآلي في الأمن السيبراني، حيث أثبتت تقنيات التعلم العميق، كفاءة عالية في التصدي لهجمات التصيد، محققة مستويات دقة تزيد عن 99% (Salem et al., 2024).

يمكن أن يتم توظيف التعلم الآلي في البيئات التطبيقية، ضمن مستويات متعددة، حيث يستخدم لاكتشاف التهديدات مسبقا عبر نماذج قائمة على السحابة، إضافة إلى تحليل سلوك الشبكة في الوقت الحقيقي (Stanham, 2023)، يساهم هذا النهج متعدد الأبعاد في تعزيز الأمن من خلال توفير معلومات فورية حول التهديدات المحتملة.

ساهم دمج الاستراتيجيات المبتاهيرستية مع منهجيات التعلم الآلي التقليدية بشكل ملحوظ في تعزيز كفاءة اكتشاف التهديدات السيبرانية؛ حيث تؤدي هذه الاستراتيجيات إلى تحسين عملية تدريب الشبكات العصبية، ما يزيد

من فعاليتها في تصنيف الأنشطة الخبيثة (Salem et al., 2024)، كما أثبتت النماذج العصبية المتقدمة، التي تعتمد على تقنيات التحسين الحديثة، تفوقا واضحا على الأنظمة التقليدية في تحديد التهديدات السيبرانية الناشئة والمعقدة؛ إضافة إلى ذلك تسعى أنظمة كشف التسلسل القائمة على التعلم الآلي بتحليل حركة مرور الشبكة بحثا عن الشذوذ الذي يشير إلى أنشطة خبيثة محتملة، ومن خلال إنشاء خطوط مرجعية للسلوك الطبيعي إستنادا على البيانات التاريخية، تخفض هذه الأنظمة من معدلات الإنذارات الكاذبة بشكل فعال مقارنة بالطرق التقليدية القائمة على القواعد (Carreiro, 2023).

تمتلك نماذج التعلم الآلي قدرة عالية على التكيف مع النمو المتزايد في حجم البيانات التي تنتجها المؤسسات، ما يجعلها قادرة على التوسع والاستجابة الفعالة للتهديدات السيبرانية المتغيرة باستمرار، ويعزز هذا التكيف المرونة في مواجهة التحولات السريعة في مشهد التهديدات الأمنية، كما أن اعتماد التحليلات السلوكية المدعومة بالتعلم الآلي يسمح بمراقبة شاملة لسلوك المستخدمين للكشف عن الأنشطة الداخلية المشبوهة أو الأنشطة غير المعتادة، التي قد يصعب اكتشافها باستخدام الدفاعات التقليدية (Wasif, 2024).

ومع هذه التطورات، تبرز تحديات إضافية تتعلق بالشفافية في نماذج التعلم الآلي، ومحاولات المهاجمين المستمرة للتلاعب بنتائجها أو التحايل عليها (Dunsin et al., 2024b)، لهذا يصبح من الضروري تطبيق ممارسات صارمة لإدارة البيانات وتحديث مجموعات التدريب بشكل منتظم، بما يضمن استدامة فعالية النماذج ضد التهديدات الناشئة.

2.3 المقارنة مع أساليب الاكتشاف التقليدية:

أحدث تبني تقنيات التعلم الآلي تحولا ملحوظا في أساليب كشف التهديدات والتصدي لها في مجال الأمن السيبراني مقارنة بالأساليب التقليدية، التي تعتمد على الكشف القائم على التوقيعات (Signature-based detection)، والذي يتطلب تحديثات مستمرة لقواعد البيانات لمواكبة التهديدات المعروفة، إلا أن هذا النهج يواجه صعوبات كبيرة في التعامل مع التهديدات المتقدمة المستمرة (APTs) ومتجهات الهجوم الجديدة التي لا تتوافق مع التوقيعات الحالية (Fichtner, 2022) وغالبا ما تجد الحلول التقليدية المضادة للبرمجيات الخبيثة صعوبة في التصدي للتقنيات المعقدة التي يستخدمها المهاجمون.

على النقيض من ذلك تستطيع نماذج التعلم الآلي، التعلم من البيانات التاريخية والتكيف مع أنماط سلوكية جديدة دون الحاجة إلى برمجة خاصة بكل حدث، حيث تقوم خوارزميات التعلم الآلي بتحليل مجموعات كبيرة من البيانات لرصد الشذوذات التي قد تدل على وجود تهديدات محتملة، وتظهر الأبحاث في (Salem et al., 2024) أن التعلم الآلي يستخدم التحليل السلوكي لفهم السلوك الطبيعي للمستخدمين، مما يسمح للأنظمة بالكشف عن أنشطة غير اعتيادية قد تشير إلى نية خبيثة أو أجهزة مخترقة.

من أبرز قيود الأساليب التقليدية أنها معرضة للهجمات ذات النكتيكات المتغيرة باستمرار، إذ يعمل المهاجمون السيبرانيون على تطوير أساليبهم باستمرار للتهرب من أنظمة الكشف التي تعتمد على التوقعات المسبقة، ومن بين

المساوئ البارزة لهذه الأنظمة، كما ورد في (AppOmni., 2024)، كثرة الإنذارات الكاذبة التي تؤدي إلى ما يعرف بإجهاد التنبيهات (alert fatigue)، مستنزفة موارد فرق الأمن التي تضطر للتعامل مع عدد كبير من الإنذارات غير المهمة.

بالمقابل، تتمتع نماذج التعلم الآلي بقدرة ديناميكية على التحسين والتكيف المستمر مع تراكم المزيد من البيانات حول سلوك المستخدمين وبيئات التهديد، مما يرفع من دقة كشف الحوادث الأمنية ويقلل بشكل ملحوظ من الإنذارات الكاذبة، وهو ما أكدته الباحثون (Shradha et al., 2024)، كما تسمح قدرات التحليلات التنبؤية التي يوفرها التعلم الآلي بتحديد الثغرات الأمنية قبل استغلالها، مما يعزز النهج الاستباقي الذي يصبح ضروريا في الأمن السيبراني المعاصر.

تصبح فعالية المقارنة بين هذين النهجين واضحة عند تقييم قدرتهما على مواجهة التهديدات السيبرانية المعقدة مثل هجمات حجب الخدمة أو التهديدات الداخلية، إذ تتطلب الدفاعات التقليدية تدخلا بشريا كبيرا للمراقبة بسبب اعتمادها على قواعد محددة مسبقا، ووفقا للدراسة التي قدمها (Sagar et al., 2020)، فإن الأنظمة الآلية التي يقودها التعلم الآلي تعزز كفاءة الاستجابة للحوادث من خلال المراقبة المستمرة لحركة مرور الشبكة، والكشف السريع عن أي انحراف عن القواعد الأساسية دون الحاجة إلى تدخل بشري مستمر.

إضافة إلى ذلك، يشكل توظيف تقنيات التعلم العميق تقدما مهما يفوق الأساليب التقليدية بشكل ملحوظ، وكما بين (Fichtner, 2022) فإن التعلم العميق يتميز بقدرته على تحديد الأنماط الدقيقة والمعقدة داخل البيانات، والتي يصعب على الطرق التقليدية رصدها، مما يجعله بالغ الأهمية لمواجهة المتغيرات المتقدمة للبرمجيات الخبيثة وأساليب التهرب المتطورة.

مما سبق، يمكن القول أن كلتا الطريقتين تواجهان تحديات تشغيلية مختلفة في بيئة التطبيق العملي؛ فالطرق التقليدية تتطلب إعدادا يدويا كثيفا وصيانة مستمرة بسبب طبيعتها الجامدة، أما نماذج التعلم الآلي فهي مرنة وفعالة، لكنها لا تخلو من القيود، مثل احتياجها العالي للموارد الحاسوبية، والمخاطر المتعلقة بالتحيزات المحتملة في مجموعات البيانات التدريبية، والتي قد تؤثر على فاعليتها في حال عدم إدارتها بشكل سليم (Salem et al., 2024)، فعدم كفاية البيانات قد يؤدي إلى زيادة الإنذارات الكاذبة.

على الرغم من هذه التحديات، تتضح مزايا دمج التعلم الآلي في الأمن السيبراني عند مقارنته بالطرق التقليدية؛ فقد برز على التكيف السريع مع التهديدات المتطورة وتحسين دقة الكشف ببررارة توجه المؤسسات نحو استخدام الحلول القائمة على التعلم الآلي والمصممة خصيصا لبيئات الأمن السيبراني، لذلك ينبغي على المؤسسات النظر بعناية في دمج أدوات التعلم الآلي ضمن استراتيجياتها للأمن السيبراني، مع إدراك كامل لإمكانات هذه الأدوات وحدودها مقارنة بالأنظمة التقليدية.

4. المناقشة:

1.4 التداعيات على استراتيجية الأمن السيبراني:

يُحدث إدماج تقنيات التعلم الآلي في الأمن السيبراني تحولاً جوهرياً في طرق حماية المؤسسات لأصولها الرقمية، ومع تزايد الهجمات السيبرانية من حيث التعقيد والتكرار، أصبحت التدابير الأمنية التقليدية غير كافية، فمن خلال قدرة التعلم الآلي على تحليل كميات هائلة من البيانات في الوقت الحقيقي، تعزز المؤسسات من قدراتها في الكشف والاستجابة، مما يدفع نحو تغيير استراتيجيات الأمن السيبراني بشكل جذري.

ومن أبرز هذه التحولات اعتماد موقف أمني استباقي، فعبر استخدام خوارزميات التعلم الآلي، يمكن للمؤسسات الكشف عن السلوكيات غير الطبيعية والتهديدات المحتملة قبل أن تتحول إلى اختراقات خطيرة، ويُعدُّ الاكتشاف المبكر لها بالغ الأهمية في تقليل الأضرار حيث أصبح بإمكان المؤسسات معالجة التهديدات بشكل استباقي بدلاً من الاكتفاء على ردود الفعل بعد وقوع الاختراق.

تسمح نماذج التعلم الآلي بمراقبة أنماط سلوك المستخدمين باستمرار للكشف عن الأنشطة غير المعتادة التي قد تشير إلى تهديدات ناشئة (Goodman, 2025)، هذا النهج الاستباقي يؤثر في طريقة توزيع الموارد داخل فرق الأمن السيبراني، فمن خلال أتمتة التعلم الآلي للمهام الروتينية كتحليل البيانات ومراقبة التهديدات التي قد ترهق العاملين في مجال تكنولوجيا المعلومات، يتمكن المختصون من التركيز على المبادرات الاستراتيجية، مما يرفع الكفاءة التشغيلية ويعزز التكامل بين الخبرة البشرية والتقنيات المتقدمة (Sailpoint.com, 2023)، إضافة إلى ذلك فإن دمج التعلم الآلي في بروتوكولات الأمان، يساعد على التحقق المستمر والرقابة الصارمة على الوصول، بما يتوافق مع قدرة التعلم الآلي على التعرف على الأنماط وتكييف الإجراءات الأمنية بشكل ديناميكي، وبهذا الاستخدام تستطيع المؤسسات تعزيز دفاعاتها ضد التهديدات المتغيرة، مع ضمان اقتصار الوصول إلى الموارد الحساسة على المستخدمين المصرح لهم فقط (Shah, 2022). تعتبر الأتمتة التي يوفرها التعلم الآلي من الجوانب المهمة في تحسين إجراءات الاستجابة للحوادث، حيث تتيح اتخاذ إجراءات سريعة بمجرد اكتشاف التهديدات، مثل عزل الأنظمة المصابة أو نشر التحديثات بشكل فوري لمعالجة نقاط الضعف، وهو أمر بالغ الأهمية نظراً لاستغلال المهاجمين السيبرانيين للثغرات فور ظهورها (Chishiri, 2024).

تتمتع المؤسسات المستخدمة للتعلم الآلي بدقة أكبر في تحديد التهديدات، نظراً لقدرة الخوارزميات على معالجة مجموعات بيانات ضخمة بسرعة، مما يقلل الإنذارات الكاذبة ويساعد على التركيز على التهديدات الحقيقية (Palo Alto Networks, 2025a)، وبما أن التعلم الآلي يدعم نظام الدفاع متعدد الطبقات، فإن هذا يعزز قدرة المؤسسات على مواجهة التهديدات السيبرانية من خلال التعلم المستمر من سلوك الشبكة وتعديل الدفاعات بشكل ديناميكي، هذه المرونة تضمن الاستعداد للثغرات المعروفة ومتجهات الهجوم الجديدة التي لم تحدث بعد (Venkatesan & Rahayu, 2024).

يؤدي التعلم الآلي أيضا، دورا أساسيا في تعزيز قدرات الاستقصاء الأمني، عبر تحليل الاتجاهات التاريخية للبيانات جنبا إلى جنب مع الحوادث الحالية، مما يساعد على توقع الهجمات المستقبلية وتمكين المؤسسات من إعداد دفاعاتها بشكل أفضل حسب ما أورده (Sangfor.com, 2024)، وبالرغم من مزاياه العديدة، فإن دمج التعلم الآلي في استراتيجيات الأمن السيبراني يفرض تحديات، خاصة مع استخدام المهاجمين السيبرانيين أيضا لأدوات الذكاء الاصطناعي، ما يستدعي تطوير استراتيجيات دفاعية متزامنة ومتجددة (Chishiri, 2024)، كذلك على المؤسسات مراعاة الأبعاد الأخلاقية عند تطبيق حلول تعتمد على الذكاء الاصطناعي والتركيز على شفافية استخدام البيانات لتعزيز الثقة بين أصحاب المصالح.

يتطلب اعتماد المؤسسات المتزايد على تقنيات متقدمة مثل التعلم الآلي في الأمن السيبراني تدريباً مستمرا وتطويراً لمهارات فرق الأمن، مما يمكنها من توظيف هذه التقنيات بفعالية لتعزيز النهج الاستباقي واتخاذ قرارات دقيقة مبنية على تحليلات البيانات اللحظية لمواجهة التهديدات المتجددة.

2.4 تحديات التعلم الآلي:

تواجه تطبيقات التعلم الآلي في مجال الأمن السيبراني تحديات بارزة تؤثر سلبا في فاعليتها وأدائها الأمني، ومن أهم هذه التحديات التنبيهات الكاذبة، التي ترهق فرق الأمن بكثرة الإنذارات وتشتت جهودها، بالإضافة إلى النتائج السلبية الخاطئة التي قد تؤدي إلى إغفال تهديدات حقيقية، كما تشكل الهجمات العدائية التي تستهدف نماذج التعلم الآلي تهديدا إضافيا يعرض دقة هذه النماذج وموثوقيتها للخطر، لهذا يجب معالجة هذه القيود لضمان فعالية هذه التطبيقات في حماية الأصول الرقمية.

أيضا، يؤدي نقص البيانات عالية الجودة أو التلاعب المتعمد فيها من قبل المهاجمين إلى إضعاف أداء نماذج التعلم الآلي في الأمن السيبراني، حيث يهدف المهاجمون من خلال تشويه البيانات إلى تضليل النماذج وتقليل فاعليتها (Dunsin et al., 2024b)، لذلك تبرز أهمية تطوير آليات دفاعية قوية للحماية من هذه الهجمات العدائية وتعزيز مقاومة النماذج السيبرانية.

تواجه المؤسسات كذلك تحديات تتعلق بتفسير نتائج خوارزميات التعلم الآلي المتقدمة، التي تتسم في كثير من الأحيان بعدم الشفافية، طبعاً هذا يجعل من الصعب على المحللين فهم كيفية التوصل إلى استنتاجات أو توقعات محددة، مما يقلل من مستوى الثقة في هذه التقنيات، ويستوجب تطوير أساليب تفسيرية واضحة.

تضاف إلى هذه الصعوبات مشكلات التكامل التقني بين حلول التعلم الآلي والبنى التحتية الأمنية القائمة، فمسألة التوافق بين الأدوات المدعومة بالذكاء الاصطناعي والأنظمة الحالية تتطلب جهوداً تقنية كبيرة، مما قد يسبب صعوبات في التواصل وتبادل البيانات بين مختلف هذه الأنظمة؛ كما تطرح الاعتبارات التنظيمية والأخلاقية المتعلقة باستخدام البيانات

تحديات إضافية، حيث تفرض التزاما صارما بمعايير حماية المعلومات الحساسة، وتزيد هذه الاعتبارات من تعقيد تطبيق نماذج التعلم الآلي، مما يتطلب من المؤسسات التأكد من التوافق مع اللوائح القانونية والشفافية في استخدام البيانات. إن نقص الموارد البشرية المؤهلة، يعرقل الاستخدام الفعال لأدوات التعلم الآلي في الأمن السيبراني، فالكثير من المؤسسات تعاني من نقص الكفاءات المدربة والقادرة على إدارة وتشغيل هذه التقنيات المتقدمة، مما يحد من قدرتها على الاستفادة الكاملة منها.

من خلال الأدبيات السابقة، تبرز الحاجة الملحة لوضع معايير موحدة لتقييم أداء نماذج التعلم الآلي في مجالات الأمن السيبراني المختلفة (Salem et al., 2024)، إذ يؤدي غياب هذه المعايير إلى إعاقه المقارنات الموضوعية بين النماذج وتقليل موثوقية النتائج، وبالتالي تظل هناك ضرورة لتطوير منهجيات تقييمية موحدة، بهدف تعزيز الثقة بفاعلية هذه النماذج وتمكين المؤسسات من استغلال إمكانات التعلم الآلي بشكل أفضل في مواجهة التهديدات السيبرانية المتجددة.

3.4 الاتجاهات المستقبلية للتعلم الآلي في الأمن السيبراني:

يتجه مسار التعلم الآلي في مجال الأمن السيبراني نحو نمو تحولي كبير، مدفوع بالتطورات التقنية المتسارعة، وتمثل زيادة تعقيد التهديدات الرقمية وتكرارها دافعا قويا لتبني هذه التقنيات وتطويرها، ويعزز دمج الذكاء الاصطناعي مع تقنيات مثل البلوكشين، من أمان الأنظمة، من خلال تطوير خوارزميات هجينة مما يتيح الكشف الفعال عن الهجمات ومنعها، وبالتالي حماية المعاملات الرقمية بصورة أفضل.

ومن المؤكد أن تعزيز صمود نماذج التعلم الآلي ضد الهجمات العدائية التي قد تؤثر على أدائها، يعتبر ضرورة لتحسين قوة النماذج، وهو عامل حاسم لمواجهة التهديدات المتطورة باستمرار (Sagar et al., 2024) وتتطلب مواجهة هذه التهديدات تطوير أساليب دفاعية قوية لحماية النماذج من الهجمات العدائية المحتملة، مع ضرورة التحديث المستمر لأساليب الدفاع.

تسهم النماذج الذكية القائمة على التعلم الآلي في تسريع عمليات اكتشاف التهديدات تلقائيا، حيث تعتمد المؤسسات بشكل متزايد على هذه النماذج لتسريع استجابتها عبر فحص مجموعات بيانات ضخمة عبر الشبكات، مما يؤدي إلى تقليص الوقت اللازم للكشف عن الحوادث والاستجابة لها؛ كما أن ضمان جودة البيانات يمثل تحديا كبيرا أمام فاعلية التعلم الآلي في الأمن السيبراني، وهذا ما يشجع على تبني آليات فعالة لجمع البيانات وتوحيدها بصورة منتظمة، مما يسمح للخوارزميات بتفسير المعلومات بدقة ويحد من المخاطر الناجمة عن البيانات المتباينة أو غير الموثوقة.

تستدعي التحديات المتعلقة بتفسير نماذج التعلم الآلي تعزيز شفافية هذه النماذج لزيادة ثقة المتخصصين في الأمن السيبراني الذين يعتمدون عليها لاتخاذ قرارات مدروسة وينبغي تطوير آليات ذكاء اصطناعي قابلة للتفسير لتوضيح آلية اتخاذ القرارات، مما يعزز من موثوقيتها لدى المختصين، ويجب أن تراعي المبادرات المستقبلية للتعلم الآلي التوافق مع

المتطلبات التنظيمية والقانونية، نظرا لأن المؤسسات التي تتعامل مع معلومات حساسة ملزمة بالامتثال للوائح حماية البيانات، ما يستلزم تضمين الأطر القانونية والتنظيمية ضمن مراحل تطوير النماذج والتطبيقات. تشير الدراسات الحالية إلى وجود صعوبات في التعامل مع التنبيهات الكاذبة في أنظمة الكشف عن الشذوذ، مما يستوجب توجيه البحوث المستقبلية نحو تطوير تقنيات مبتكرة تزيد من دقة الكشف، مثل خفض معدل التنبيهات الخاطئة من أجل تجنب إرباك فرق الأمن بالإشعارات غير الضرورية. إن توظيف التعلم الآلي يساهم في تعزيز استراتيجيات الأمن السيبراني من خلال تمكين المؤسسات من الاستجابة السريعة للتهديدات المكتشفة استنادا إلى الأتمتة القائمة على الخبرات السابقة، مما يحرر الموارد البشرية للتركيز على المهام الاستراتيجية، ويعزز مرونة المؤسسة أمام الهجمات المحتملة، مع ضرورة وضع الاعتبارات الأخلاقية في الحسبان، وتكثيف التعاون البحثي بين المختصين والصناعات لمواجهة التحديات واستغلال هذه التقنيات بصورة مثلى. علاوة على ذلك، توفر تطبيقات التعلم الآلي إمكانية اتخاذ قرارات استراتيجية مستنيرة، حيث تمكن صناع القرار من الاستفادة من تحليلات مفصلة حول المخاطر المحتملة وتقدير أفضل الطرق للتعامل معها، ما يؤدي إلى تحسين توزيع الموارد وجهود فرق الأمن السيبراني.

خاتمة:

يمثل دمج التعلم الآلي في الأمن السيبراني نقلة نوعية في استراتيجيات الحماية الرقمية، وذلك استجابة لتزايد تعقيد التهديدات الإلكترونية والقصور الذي تعاني منه أنظمة الكشف التقليدية، ويوفر التعلم الآلي حلولاً متقدمة لتعزيز قدرات الاكتشاف والاستجابة، حيث تعتمد خوارزمياته على تحليل البيانات والتكيف المستمر مع الأنماط الناشئة، مما يمكنها من رصد الأنشطة الضارة أو المشبوهة بدقة قبل حدوثها واتخاذ تدابير وقائية قبل وقوع أي ضرر محتمل.

توفر أدوات التعلم الآلي مزايا كبيرة مقارنة بأساليب الأمن السيبراني التقليدية، التي تعتمد على توقعات ثابتة أو قواعد استدلالية قد لا تتمكن من كشف أنماط الهجمات الجديدة أو التهديدات سريعة التطور، وعلى النقيض من ذلك يتميز التعلم الآلي بقدرته على التعلم المستمر من البيانات المستجدة، مما يمكنه من التكيف بفعالية مع بيئة التهديدات المتغيرة باستمرار، ووفقاً لما ورد في موقع (Sangfor.com, 2024)، فإن هذا النهج يساهم في تعزيز دقة وكفاءة الكشف عن التهديدات، مما يتيح لفرق الأمن التركيز على الحوادث الحرجة بدلاً من الانشغال بالتنبيهات الصادرة عن الأنظمة التقليدية الأقل تطوراً.

إن استخدام تقنيات متقدمة مثل الشبكات العصبية العميقة يمكن أن يعزز معدلات الكشف مع تقليل الإنذارات الكاذبة، وتعد هذه الميزة ضرورية في البيئة الحالية التي تتسم بهجمات متطورة التي غالباً ما تغفل عنها الطرق التقليدية؛ وكما هو مفصل في (Shradha et al., 2024) تستطيع نماذج التعلم الآلي تحليل كميات ضخمة من حركة مرور الشبكة وتحديد الأنماط التي تشير إلى وجود مخالفات، مما يجعلها مكوناً أساسياً في أنظمة كشف الاختراق (IDS) وتدابير الأمن الاستباقية وفقاً لما ورد في (Tanium, 2024)، ومع ذلك فإن الاعتماد على التعلم الآلي لا يخلو من التحديات، فقد تواجه المؤسسات مشكلات تتعلق بجودة البيانات والتحيز الخوارزمي والحاجة إلى موارد حاسوبية كبيرة لتدريب نماذج فعالة، وعلى الرغم من وجود جوانب سلبية محتملة مثل سوء تفسير البيانات أو الإفراط في ملاءمة النموذج، إلا أن الأبحاث مستمرة لمعالجة هذه المخاوف، ويبقى الهدف هو تحسين المنهجيات التي تعزز الأمن دون إدخال ثغرات جديدة.

إن استخدام التعلم الآلي ضمن استراتيجيات الأمن السيبراني يشير إلى فرص مبشرة في مواجهة التهديدات الأمنية المستمرة، كما تم بحثه بشكل مستفيض في (Salem et al., 2024)، حتى وإن كانت مليئة بالتحديات، فقد تؤدي التطورات المستقبلية إلى أنظمة أكثر تطوراً وكفاءة، وقادرة على التنبؤ بالهجمات وفقاً للاتجاهات الناشئة في سلوك المستخدمين ونواقل التهديدات، وستكون هذه القدرة التنبؤية حيوية لآليات الدفاع الاستباقية التي تخفف المخاطر قبل تحققها.

تعد الشراكة والتعاون بين القطاعات المختلفة أمراً حيوياً لتطوير مجموعات بيانات متنوعة تستخدم في تدريب نماذج التعلم الآلي، وتعتمد فعالية هذه الخوارزميات على بيانات مدخلة تعكس بدقة السيناريوهات الواقعية، ويمكن للجهود التعاونية أن تعزز موثوقية النماذج حسب ما ورد في (Shaukat et al., 2020)، ومن الضروري إعطاء الأولوية للشفافية عند بناء مجموعات البيانات وشموليتها فيما يتعلق بمختلف أنواع التهديدات الإلكترونية.

من خلال الأبحاث المستعرضة أعلاه، التي تشير إلى أن النماذج الهجينة، التي تمزج بين ممارسات الأمن السيبراني التقليدية وتقنيات التعلم الآلي المتقدمة، قادرة على تحقيق نتائج أفضل ضد الأنشطة الإجرامية الإلكترونية، ومن خلال تحديد مواطن القوة والضعف وتوجيه الموارد لمواجهة التحديات، يمكن تمهيد الطريق نحو مستقبل رقمي أكثر مرونة، وعلى الرغم من استمرار العقبات أمام دمج التعلم الآلي بفعالية ضمن الأطر القائمة، تظل إمكاناته في إعادة تشكيل الأمن السيبراني المعاصر ثابتة ؛ ولهذا، يوصى بدمج خوارزميات متعددة ضمن أنظمة هجينة للاستفادة من مزاياها، مما يحقق أداءً آمناً شاملاً، هذا النهج الهجين ليس ترفاً تقنياً، بل أصبح شرطاً أساسياً للحفاظ على المرونة الأمنية ؛ كذلك ينبغي تعزيز التعاون الدولي لمواجهة هذه الجرائم، إلى جانب زيادة الاستثمار في حماية البنية التحتية الرقمية للتصدي للهجمات السيبرانية المعقدة.

كأفاق للبحث المستقبلي، تكشف نتائج هذه الدراسة عن إمكانات واعدة لتقنيات التعلم الآلي في تعزيز فعالية الأمن السيبراني، غير أن المجال لا يزال بحاجة إلى مزيد من الدراسات المعمقة التي تأخذ في الحسبان عدة أبعاد إضافية، فمن جهة، تبرز الحاجة إلى تطوير نماذج هجينة أكثر قدرة على مواجهة الهجمات العدائية التي تستهدف آليات التعلم الآلي ذاتها، وهي ظاهرة تتطلب بحثاً تطبيقية في مجال التعلم الآلي المقاوم للهجمات (Adversarial ML)، ومن جهة أخرى تبقى قضايا الخصوصية والتحديات الأخلاقية أمر لا يستهان به، وهذا ما يستدعي مقاربات متعددة التخصصات تجمع بين علوم البيانات والقانون وأخلاقيات الذكاء الاصطناعي.

إضافة إلى ذلك، يمكن توسيع مجال الدراسة ليشمل تقييم الأداء الفعلي لتقنيات التعلم الآلي في بيئات تشغيل واقعية ضمن قطاعات مختلفة، مثل الصحة، الطاقة، المالية، وغيرها، مما يعزز من تعميم النتائج ويوفر نماذج قابلة للتنفيذ. كما يُوصى بتكثيف الجهود البحثية في تطوير آليات تحسين جودة البيانات وتوليد بيانات تدريب صناعية آمنة تضمن دقة النماذج دون المساس بالمعايير القانونية أو الأخلاقية، كما ينبغي تشجيع الدراسات المقارنة التي تعتمد على تجارب محاكاة أو دراسات حالة ميدانية، لفهم أفضل لتفاعل أنظمة الأمن السيبراني القائمة مع تقنيات الذكاء الاصطناعي، بما يتيح رسم خارطة طريق استراتيجية لتوظيف هذه التقنيات بفعالية واستدامة في بيئات متعددة التحديات.

قائمة المراجع:

- 1 Abaimov, S., & Martellini, M. (2022). Machine learning for cyber agents: Attack and defence. Springer.
- 2 Alshathry, N., Carare, A.-S., Galiveeti, S., Garg, R., & Mehta, D. (2024). Machine Learning Algorithms for Detecting and Preventing Cyber Threats. *Ox Journal* ; <https://www.oxjournal.org/machine-learning-algorithms-for-detecting-and-preventing-cyber-threats/> (consulté le 13/12/2024)
- 3 AppOmni.com (2024). A Comprehensive Guide to Threat Detection. <https://appomni.com/what-is-threat-detection> (consulté le 29/11/2024)
- 4 Bhatt, N., Presswala, F., & Thakkar, A. (2020). Cyber insurance and risk assessment. In *Machine learning for computer and cyber security: Principles, algorithms and practices* (pp. 326–327). CRC Press.
- 5 Carreiro, J. (2023). The Role of Machine Learning in Cybersecurity: Benefits and Applications. <https://www.ironhack.com/us/blog/the-role-of-machine-learning-in-cybersecurity> (consulté le 15/10/2024)
- 6 Cassetto, O. (2020). Machine Learning for Cybersecurity: Next-Gen Protection Against Cyber Threats. <https://www.exabeam.com/blog/infosec-trends/machine-learning-for-cybersecurity-next-gen-protection-against-cyber-threats/> (consulté le 29/01/2025)
- 7 Chishiri, V. (2024). AI and Cybersecurity: A Powerful Partnership. https://www.linkedin.com/posts/victor-chishiri-37221121_ai-cybersecurity-threatdetection-activity-7255507175760875522-qelj (consulté le 29/11/2024)
- 8 Dixit, P., & Silakari, S. (2021). Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. *Computer Science Review* ; Vol 39 ; <https://doi.org/10.1016/j.cosrev.2020.100317> (consulté le 29/11/2024)
- 9 Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V (2024a). Reinforcement Learning for an Efficient and Effective Malware Investigation during Cyber Incident Response. <https://dx.doi.org/10.48550/arXiv.2408.01999> (consulté le 22/12/2024)
- 10 Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V (2024b). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, Vol. 48, 1-21; <https://doi.org/10.1016/j.fsidi.2023.301675> (consulté le 22/12/2024)
- 11 Fichtner, E. (2022). 5 Amazing Applications of Deep Learning in Cybersecurity. <https://www.datto.com/blog/5-amazing-applications-of-deep-learning-in-cybersecurity/> (consulté le 15/10/2024)

- 12 Goodman, C. (2025). Understanding Machine Learning (ML) in Cybersecurity. <https://www.balbix.com/insights/machine-learning-in-cybersecurity/> (consulté le 18/02/2025)
- 13 Gottsegen, G., & Urwin, M. (2023). Machine Learning in cybersecurity: How it works and companies to know. <https://builtin.com/artificial-intelligence/machine-learning-cybersecurity> (consulté le 29/11/2024)
- 14 Jada, I., & Mayayise, T. O (2024). The impact of artificial intelligence on organisational cyber security: *An outcome of a systematic literature review. Data and Information Management*; Vol 8, Issue 2, <https://doi.org/10.1016/j.dim.2023.100063> (consulté le 07/12/2024)
- 15 Jordan, M., & Mitchell, C. (2020). A review of machine learning methods applied for handling zero-day attacks. In *Handbook of research on machine and deep learning applications for cyber security* (pp. 371–372). IGI Global.
- 16 Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, Vol 97, 1-29 ; <https://doi.org/10.1016/j.inffus.2023.101804> (consulté le 10/10/2024)
- 17 Khanna, R., & Singh, S. (2020). *Applications of machine and deep learning in cybersecurity*. In P. Ganapathi & D. Shanmugapriya (Eds.), *Handbook of research on machine and deep learning applications for cyber security* (pp. 95–102). IGI Global.
- 18 Mittal, S. (2023). A review of machine learning techniques in cybersecurity and research opportunities. In *Machine learning for cyber security* (p. 2). De Gruyter.
- 19 Morgan, S. (2024). Top 10 cybersecurity predictions and statistics for 2024. *Cybercrime Magazine*. <https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/> (consulté le 09/03/2025)
- 20 Palo Alto Networks (2025a). What Is the Role of AI in Threat Detection? <https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection> (consulté le 28/02/2025)
- 21 Palo Alto Networks (2025b). The Growing Role of Machine Learning in Cybersecurity <https://www.paloaltonetworks.com/cybersecurity-perspectives/the-growing-role-of-machine-learning-in-cybersecurity> (consulté le 28/02/2025)
- 22 Presswala, F., Thakkar, A., & Bhatt, N. (2020). A review of machine learning methods applied for handling zero-day attacks. In P. Ganapathi & D. Shanmugapriya (Eds.), *Handbook of research on machine and deep learning applications for cyber security* (pp. 374–381). IGI Global.

- 23 Sagar, R., Jhaveri, R., & Borrego, C. (2020). Applications in Security and Evasions in Machine Learning: A Survey. *Electronics* 9(1), 97; 1-42 <https://doi.org/10.3390/electronics9010097> (consulté le 29/11/2024)
- 24 Sailpoint.com (2023). Machine learning (ML) in cybersecurity. <https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity> (consulté le 12/11/2024)
- 25 Salem, A.H., Azzam, S.M., Emam, O.E. *et al.* (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data* 11:105 ; 1-38; <https://doi.org/10.1186/s40537-024-00957-y> (consulté le 12/02/2025)
- 26 Sangfor.com (2024). Machine Learning in Cybersecurity: Benefits and Challenges. <https://www.sangfor.com/blog/cybersecurity/machine-learning-in-cybersecurity-benefits-and-challenges> (consulté le 29/11/2024)
- 27 Shah, V. (2022). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. https://www.researchgate.net/publication/378396020_Machine_Learning_Algorithms_for_Cybersecurity_Detecting_and_Preventing_Threats (consulté le 15/10/2024)
- 28 Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. *Proceedings of the International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan, 2020, 1-6, <https://doi.org/10.1109/ICCWS48432.2020.9292388> (consulté le 17/10/2024)
- 29 Shradha, F., Rutuja, G., Sakshi, C., Khushi, A., & Srushti, K. (2024). Detection of cyber-attacks and network attacks using Machine Learning. *World Journal of Advanced Engineering Technology and Sciences*, 2(01), 128–132, <https://doi.org/10.30574/wjaets.2024.12.1.0184> (consulté le 29/11/2024)
- 30 Stanham, L. (2023). Machine Learning (ML) & Cybersecurity How is ML used in Cybersecurity? <https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/machine-learning/> (consulté le 19/10/2024)
- 31 Tanium.com (2024). Machine Learning in Cybersecurity: A Primer for Beginners. <https://www.tanium.com/blog/machine-learning-in-cybersecurity/> (consulté le 29/11/2024)
- 32 Tulsa (2024). What is Machine Learning in Cybersecurity?. <https://online.utulsa.edu/blog/what-is-machine-learning-cybersecurity/> (consulté le 29/11/2024)
- 33 Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. *NaturePortfolio*, 14:1149; <https://doi.org/10.1038/s41598-024->

[51578-7](#) (consulté le 29/11/2024)

- 34 Wasif, N. (2024). Revolutionizing Cybersecurity: Leveraging Machine Learning for Advanced Network Security and Information Security Infrastructure. <http://dx.doi.org/10.13140/RG.2.2.36563.18725> (consulté le 29/11/2024)