

إطار قائم على التعلم الآلي لتقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية.

مشروع خطة أطروحة للتسجيل لدرجة الدكتوراه

إعداد الباحث:

٢٠٢٥ / ١٤٤٦ هـ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

المحتويات

٤	المقدمة:
٥	مشكلة الدراسة :
٧	أهمية الدراسة
٩	أهداف الدراسة
١٠	فرضيات الدراسة
١١	نموذج الدراسة:
١٣	مصطلحات الدراسة وتعريفاتها الإجرائية:
١٦	منهج الدراسة :
١٧	أداة الدراسة
١٧	مجتمع الدراسة:
١٩	عينة الدراسة
١٩	مصادر البيانات في الدراسة
٢٠	المعالجات الإحصائية المقترحة:
٢١	حدود الدراسة
٩٠	الدراسات السابقة :
١٠٥	الفجوة البحثية
٢٣	قائمة المراجع:

المقدمة:

يشهد العالم المعاصر تحولات جذرية في بنية أنظمتها الاقتصادية والتقنية، مدفوعة بالتقدم السريع في مجال الذكاء الاصطناعي وما يتفرع عنه من تقنيات حديثة أبرزها التعلم الآلي (Machine Learning). وقد أسهمت هذه التطورات في إحداث نقلة نوعية في طريقة تحليل البيانات، واتخاذ القرارات، وإدارة الموارد في المؤسسات المعاصرة، فلم تعد البيانات تُعامل كمخرجات ثانوية للأنشطة البشرية، بل أصبحت تُعدّ مصدرًا رئيسًا للقيمة المضافة ومحركًا أساسيًا للتنافسية العالمية، خاصة في ظل اقتصاد المعرفة الذي يقوم على التحليل الذكي والتعلم من الخبرة السابقة (بن التركي وآخرون، ٢٠٢١).

يُعد التعلم الآلي أحد أهم فروع الذكاء الاصطناعي وأكثرها تأثيرًا في العصر الرقمي، نظرًا لقدرته على بناء نماذج تحليلية تستند إلى الخوارزميات والبيانات الضخمة، بما يسمح للأنظمة بالتعلم الذاتي وتحسين أدائها بمرور الوقت دون تدخل بشري مباشر، وقد أثبتت التجارب التطبيقية أن خوارزميات التعلم الآلي تمتلك إمكانيات واسعة في مجالات التنبؤ، والتصنيف، والكشف عن الأنماط الخفية في البيانات، الأمر الذي جعلها محورًا رئيسًا في العديد من التطبيقات الصناعية والخدمية، لا سيما في المجالات التي تتطلب سرعة استجابة عالية ودقة في معالجة البيانات المعقدة (برارمة، ٢٠٢٤).

ويشهد العالم توسعًا كبيرًا في استخدام الأنظمة الرقمية المتصلة التي تقوم على التكامل بين الأجهزة الذكية والبنى التحتية المعلوماتية. وقد أسهم هذا التكامل في تطوير ما يُعرف بالأنظمة الذكية، مثل المدن الذكية، والمصانع المؤتمتة، وأنظمة النقل الذكية التي تُعد من أبرز مظاهر التحول الرقمي في العصر الحديث، فأنظمة النقل الذكية تمثل نقلة نوعية في إدارة الحركة المرورية، وتنظيم خدمات النقل العام والخاص، من خلال استثمار التقنيات الرقمية، وأجهزة الاستشعار، والاتصال اللحظي بالإنترنت لتحليل البيانات الميدانية واتخاذ القرارات الفورية. (Kalinin et al., 2021)

إن الترابط الواسع بين مكونات أنظمة النقل الذكية يجعلها أكثر حساسية تجاه أي اختراق أو هجوم إلكتروني، مما يستدعي تطوير آليات تقييم دقيقة للمخاطر قادرة على التنبؤ بالتهديدات وتحليلها بذكاء، وهنا يظهر الدور المحوري لتقنيات التعلم الآلي في دعم أنظمة الحماية والتقييم الأمني، باعتبارها من الأدوات القادرة على تحليل البيانات الديناميكية وتقديم مؤشرات مبكرة للمخاطر (Yao & García de Soto, 2024).

وقد شكّل موضوع تقييم مخاطر الأمن السيبراني محور اهتمام متزايد في الأدبيات الحديثة، نظرًا لتنامي التحديات التي تواجه البنى التحتية الذكية في ظل الاعتماد الواسع على الاتصال الرقمي، وتبرز أهمية هذا المجال في كونه لا يقتصر على الحماية التقنية فحسب، بل يمتد إلى إدارة المخاطر وتحليل نقاط الضعف وتقدير احتمالية التهديدات في بيئات عمل معقدة ومتشابكة. (Şahinoglu, 2024)

وفي ضوء هذا التكامل بين التكنولوجيا الذكية والأمن المعلوماتي، تبرز الحاجة إلى دراسات أكثر عمقًا تتناول أثر تقنيات التعلّم الآلي في تقييم مخاطر الأمن السيبراني ضمن أنظمة النقل الذكية، لما يمثله هذا القطاع من أهمية استراتيجية في التنمية الاقتصادية والاجتماعية، فهذه الأنظمة لا تقتصر على تحسين حركة النقل فحسب، بل تُعد جزءًا جوهريًا من البنية التحتية الرقمية التي تقوم عليها المدن الحديثة. (Ganesan et al., 2022).

وتأتي هذه الدراسة في سياق علمي معاصر يسعى إلى الربط بين مسارين بحثيين أساسيين هما : التعلّم الآلي بوصفه أداة تحليل وتنبؤ ذكية، والأمن السيبراني بوصفه ضرورة لحماية الأنظمة الذكية من المخاطر التقنية.

مشكلة الدراسة :

يشهد العالم اليوم تصاعدًا غير مسبوق في حجم وتعقيد الهجمات السيبرانية، حيث يُتوقع أن يصل حجم سوق الأمن السيبراني في الشرق الأوسط إلى نحو 15.30 مليار دولار أمريكي بحلول عام ٢٠٢٤، مع معدل نمو سنوي مركب يُقدر بـ 9.3% حتى عام ٢٠٣٣. (Market Data Forecast, 2024). كما أشارت تقارير أمنية حديثة إلى أن متوسط تكلفة الهجمة السيبرانية على المؤسسات في الشرق الأوسط يبلغ حوالي ٨.٧٥ مليون دولار أمريكي، أي ما يقارب ضعف المتوسط العالمي (Positive Technologies, 2024)، ويعكس ذلك أن الأنظمة الرقمية الذكية، وخاصة في قطاع النقل الذكي، تواجه بيئة تهديدات متزايدة التعقيد تتطلب حلولًا تحليلية أكثر ذكاءً ودقة.

وعلى الرغم من التطور الملحوظ في استخدام تقنيات الذكاء الاصطناعي في مجالات متعددة، إلا أن توظيف التعلّم الآلي (Machine Learning) في تقييم مخاطر الأمن السيبراني لا يزال محدودًا في قطاعات النقل، وقد بينت دراسة تحليلية شاملة أن أنظمة النقل الذكي تمثل إحدى أكثر البنى التحتية عرضة للهجمات السيبرانية نتيجة اعتمادها على شبكات مترابطة ومعالجة فورية للبيانات في الوقت الحقيقي

(Khan et al., 2024)، كما أظهرت دراسات أخرى أن معظم تطبيقات الأمن السيبراني الحالية تركز على الكشف بعد وقوع الهجوم، بينما تفتقر إلى النماذج التنبؤية القائمة على التحليل الذكي لأنماط المخاطر (Alshammari & Alshehri, 2023).

في حين انتقدت الدراسات السابقة على أهمية التعلم الآلي في التنبؤ والتحليل الذكي للبيانات (Ateya, 2024; Ben Turki & Seham, 2021; Phiri et al., 2025)، فإنها اختلفت عن الدراسة الحالية من حيث مجال التطبيق، إذ ركزت على قطاعات الاقتصاد، والتمويل، والطاقة، والتعليم، والرعاية الصحية (Wang et al., 2021; Ganesan et al., 2022; Rafaianni et al., 2023)، دون أن تمتد إلى قطاع النقل الذكي الذي يُعد من أكثر القطاعات تأثرًا بالتحول الرقمي وتهديدات الأمن السيبراني المتقدمة.

و تتمثل مشكلة الدراسة الحالية في وجود قصور علمي وتطبيقي في فهم وتقييم أثر تقنيات التعلم الآلي بأبعادها (التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي) على تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية، ويبرز هذا القصور في محدودية النماذج التي تدمج بين خوارزميات التعلم الآلي وآليات التقييم الأمني، مما يؤدي إلى ضعف قدرة المؤسسات المعنية بالنقل الذكي على التنبؤ المبكر بالهجمات السيبرانية والاستجابة الفعّالة لها.

وبناءً على سبق يمكن صياغة مشكلة الدراسة في التساؤل الرئيس التالي:

إلى أي مدى تُسهم تقنيات التعلم الآلي بأبعادها (التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي) في تحسين تقييم مخاطر الأمن السيبراني بأبعاده (الكشف، التقييم، الاستجابة، والتعافي) ضمن أنظمة النقل الذكية؟، وتتفرع منها عدة أسئلة فرعية :

١. ما مستوى تطبيق تقنيات التعلم الآلي بأبعادها المختلفة في بيئات النقل الذكية؟

٢. ما واقع تقييم وإدارة مخاطر الأمن السيبراني في أنظمة النقل الذكية من حيث (الكشف، التقييم، الاستجابة، والتعافي)؟

٣. ما طبيعة العلاقة بين التحليل التنبؤي وتقنيات التنبؤ بالتهديدات السيبرانية في أنظمة النقل الذكية؟

٤. إلى أي مدى يسهم الكشف الذكي عن الهجمات في رفع دقة وسرعة اكتشاف التهديدات السيبرانية في أنظمة النقل الذكية؟

٥. ما دور التصنيف التلقائي للمخاطر في تحسين كفاءة تقييم مستويات الخطورة وتحديد أولويات المعالجة الأمنية؟

٦. كيف يؤثر التحسين الذاتي في تعزيز قدرة أنظمة النقل الذكية على التكيف مع الهجمات وتقليل زمن التعافي؟

٧. ما الأبعاد الأكثر تأثيراً من بين تقنيات التعلم الآلي في تحسين تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية؟

٨. كيف يمكن توظيف نتائج الدراسة في بناء نموذج تكاملي تطبيقي لتقييم وإدارة مخاطر الأمن السيبراني اعتماداً على تقنيات التعلم الآلي؟

أهمية الدراسة

تسعى هذه الدراسة إلى استكشاف الأثر الفعلي لتقنيات التعلم الآلي في تقييم مخاطر الأمن السيبراني ضمن أنظمة النقل الذكية، من خلال بناء إطار علمي وتطبيقي يُسهم في تعزيز أمن هذه الأنظمة واستدامتها التشغيلية، وتتجلى أهمية الدراسة في بُعدين رئيسيين: البعد العلمي الذي يتمثل في إثراء المعرفة النظرية والتجريبية حول العلاقة بين التعلم الآلي والأمن السيبراني، والبعد العملي الذي يرتبط بإمكانية توظيف نتائج الدراسة في تطوير استراتيجيات ذكية لحماية البنى التحتية للنقل.

وتتمثل أهمية الدراسة فيما يلي:

أولاً: الأهمية العلمية

تتبع الأهمية العلمية لهذه الدراسة من حادثة موضوعها وتكامل أبعاده بين ثلاثة مجالات معرفية متقدمة، هي:

١. تسد فجوة معرفية واضحة في الأدبيات المعاصرة، إذ ندرت الدراسات التي تناولت التفاعل المباشر بين تقنيات التعلم الآلي وتقييم المخاطر السيبرانية في بيئات النقل الذكية، مما يمنح البحث قيمة إضافية في إثراء الحقل العلمي بالتطبيقات الحديثة.

٢. تُسهم في تطوير إطار علمي تكاملي يجمع بين علم البيانات والذكاء الاصطناعي والأمن السيبراني في سياق أنظمة النقل، بما يفتح آفاقًا بحثية جديدة لمقاربات متعددة التخصصات (Interdisciplinary Research).

٣. تعزز المنظور النظري للأمن السيبراني الحديث عبر توظيف خوارزميات التعلم الآلي كأدوات تحليلية للتنبؤ، والاكتشاف، والتصنيف، مما يوسع من حدود المفهوم التقليدي لإدارة المخاطر إلى نموذج استباقي ذكي.

٤. تضيف بعدًا منهجيًا متطورًا من خلال استخدام التحليل الإحصائي المتقدم واختبار العلاقات التأثيرية بين الأبعاد المتعددة لتقنيات التعلم الآلي ومكونات تقييم المخاطر السيبرانية، مما يعزز من دقة الاستنتاجات العلمية.

٥. تمدّ المجتمع الأكاديمي العربي بإسهام بحثي أصيل باللغة العربية في مجال نادر التناول، يواكب التطورات العالمية في مجال الذكاء الاصطناعي وتطبيقاته الأمنية في البنى التحتية الذكية.

٦. تُسهم في إثراء النماذج المفاهيمية الخاصة بتقييم الأمن السيبراني عبر إدخال بُعد التعلم الذاتي والتحليل التنبؤي ضمن أطر التقييم، وهو ما لم يتم تناوله بعمق في الأبحاث السابقة المتعلقة بالنقل الذكي.

ثانيًا: الأهمية العملية

تتجلى الأهمية العملية لهذه الدراسة في ما تقدمه من تطبيقات واقعية واستراتيجيات تشغيلية يمكن أن تُسهم في تعزيز الأمن السيبراني لأنظمة النقل الذكية، والتي تُعد من أكثر البنى التحتية عرضة للتهديدات والهجمات الرقمية نتيجة ارتباطها المباشر بالأنظمة الحسية والاتصالية والبيانات الضخمة.

١. تمثل الدراسة مرجعًا عمليًا لصُنّاع القرار والمهندسين في قطاع النقل الذكي، من خلال تقديم نموذج تطبيقي يمكن توظيفه في تحليل وتقدير التهديدات السيبرانية بدقة عالية.

٢. تُسهم في رفع كفاءة البنى التحتية الرقمية للنقل من خلال تمكينها من اكتشاف الهجمات مبكرًا والتعامل معها ذاتيًا، ما يعزز موثوقية الأنظمة واستمرارية الخدمات الحيوية.
٣. تدعم جهود التحول الرقمي الآمن في القطاعات الحكومية والخاصة عبر دمج تقنيات الذكاء الاصطناعي في سياسات الأمن السيبراني، بما يحقق التوازن بين التطور التقني والحماية الأمنية.
٤. تساعد المؤسسات على تقليل الخسائر التشغيلية والتقنية الناتجة عن الهجمات الإلكترونية، من خلال بناء أنظمة قائمة على التحليل الذكي للمخاطر والاستجابة السريعة للتهديدات.
٥. تُسهم في صياغة توصيات استراتيجية يمكن أن تُستثمر في تصميم أطر وطنية للأمن السيبراني في النقل الذكي، تدعم استدامة الأداء وتكامل البنية التحتية الذكية.
٦. تفتح آفاقًا للتعاون البحثي التطبيقي بين الجامعات ومراكز الأبحاث وشركات التكنولوجيا في تطوير حلول واقعية قائمة على خوارزميات التعلم الآلي للأمن السيبراني.
٧. تُمكن الجهات التنظيمية والتشريعية من الاستفادة من نتائج الدراسة في بناء معايير وطنية وإرشادات فنية لتقييم وإدارة المخاطر السيبرانية في أنظمة النقل الذكية.

أهداف الدراسة

تهدف هذه الدراسة إلى استقصاء أثر تقنيات التعلم الآلي بأبعادها (التحليل التنبؤي، والكشف الذكي عن الهجمات، والتصنيف التلقائي للمخاطر، والتحسين الذاتي) في تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية، وذلك من خلال تطوير إطار تكاملي يوظف قدرات الذكاء الاصطناعي في تحليل أنماط التهديدات السيبرانية، وتقدير مستويات المخاطر المحتملة، وتعزيز كفاءة آليات الاستجابة والتعافي ضمن بيئات النقل الذكي.

وتسعى الدراسة إلى توسيع الفهم النظري والتطبيقي لكيفية توظيف خوارزميات التعلم الآلي كأداة استراتيجية في تعزيز الأمن السيبراني للبنى التحتية الحيوية للنقل الذكي.

وتتفرع منه عدة أهداف فرعية :

١. تحديد مستوى تبني واستخدام تقنيات التعلم الآلي بأبعادها (التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي) في مكونات أنظمة النقل الذكية.
٢. تحليل آليات تقييم مخاطر الأمن السيبراني بأبعادها (الكشف، التقييم، الاستجابة، والتعافي) في بيئات النقل الذكي، واستكشاف التحديات المرتبطة بتطبيقها في السياقات الرقمية المعقدة.
٣. اختبار العلاقة الجوهرية بين تقنيات التعلم الآلي وتقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية، وقياس مستوى تأثير كل بُعد من أبعاد التعلم الآلي في تحسين كفاءة التقييم.
٤. استقصاء إسهام تقنيات التعلم الآلي في بناء أنظمة استباقية قادرة على التنبؤ بالتهديدات السيبرانية قبل وقوعها، وتقليل زمن الاستجابة وتعزيز فعالية الدفاعات الرقمية.
٥. بلورة نموذج مفاهيمي وتطبيقي مقترح لتوظيف خوارزميات التعلم الآلي في إدارة وتقييم مخاطر الأمن السيبراني بأنظمة النقل الذكية، بما يسهم في رفع كفاءتها التشغيلية وضمان استدامتها.
٦. صياغة مجموعة من التوصيات العلمية والممارسات التطبيقية الداعمة لتكامل تقنيات التعلم الآلي ضمن استراتيجيات الأمن السيبراني في قطاع النقل الذكي على المستويين المؤسسي والوطني.

فرضيات الدراسة

بناءً على ما تم عرضه من أهداف الدراسة ومشكلتها وأهميتها يمكن تحديد فرضيات الدراسة من خلال فرضية رئيسية تتمثل في:

الفرضية الرئيسية الأولى (H1): يوجد تأثير ذو دلالة إحصائية عند مستوى $(\alpha \leq 0.05)$ لتقنيات التعلم الآلي بأبعادها (التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي) على تقييم مخاطر الأمن السيبراني بأبعاده (الكشف، التقييم، الاستجابة، والتعافي) في أنظمة النقل الذكية.

وتتفرع منه عدة فرضيات فرعية :

H1.1: يوجد تأثير ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لبُعد التحليل التنبؤي على تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية..

H1.2: يوجد تأثير ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لبُعد الكشف الذكي عن الهجمات على تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية.

H1.3: يوجد تأثير ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لبُعد التصنيف التلقائي للمخاطر على تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية.

H1.4: يوجد تأثير ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لبُعد التحسين الذاتي على تقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية..

نموذج الدراسة:

يهدف هذا النموذج إلى التعرف على أثر تقنيات التعلم الآلي بأبعادها في تقييم مخاطر الأمن السيبراني بأبعادها، وذلك في سياق أنظمة النقل الذكية، سعيًا لبناء إطار علمي يوضح طبيعة التأثير المباشر للتقنيات الذكية في تعزيز أمن واستدامة البنى التحتية للنقل. ويتضمن النموذج المتغيرات التالية:

أولاً: مدخلات البيانات

تبدأ العملية بجمع البيانات التي تنتجها أنظمة النقل الذكية في السياق العملي، وتشمل بيانات أجهزة الاستشعار، وسجلات الشبكات، وبيانات الاتصال بين المركبات والبنية التحتية، إضافة إلى بيانات حركة المرور في الزمن الحقيقي وبيانات الهجمات السابقة. وتمثل هذه البيانات الأساس الذي تعتمد عليه عمليات التحليل والكشف والتصنيف.

ثانياً: طبقات المعالجة باستخدام تقنيات التعلم الآلي

يتم إدخال البيانات إلى سلسلة من مراحل المعالجة التي تمثل أبعاد التعلم الآلي الأربعة في الدراسة:

المتغير المستقل:

تقنيات التعلم الآلي بأبعادها: (التحليل التنبؤي - الكشف الذكي عن الهجمات - التصنيف التلقائي للمخاطر - التحسين الذاتي) بالاعتماد على دراسات (Phiri et al., 2025) ؛ (Ateya, 2024) ؛ (Bui et al., 2023)؛ (Kayraklioglu et al., 2021)

المتغير التابع:

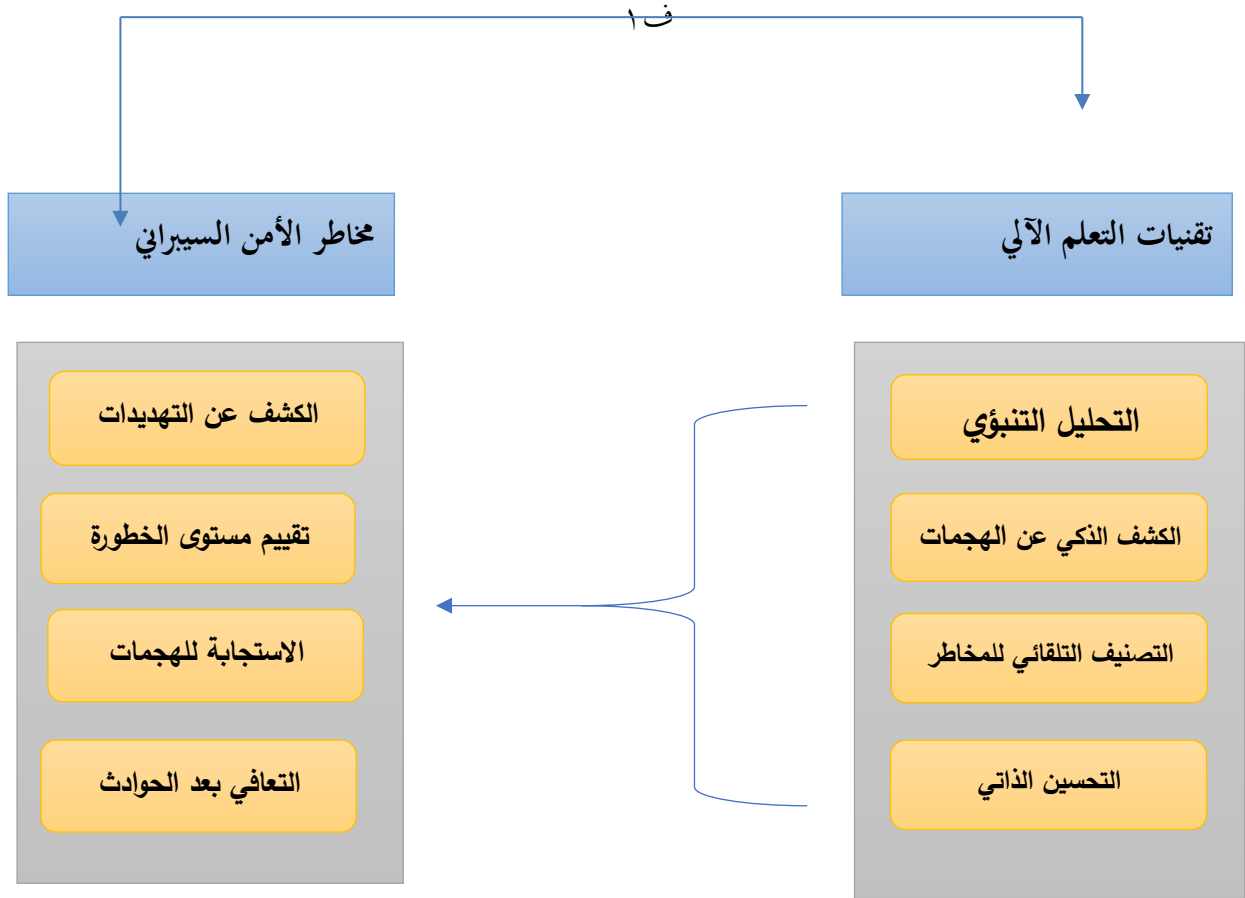
تقييم مخاطر الأمن السيبراني بأبعاده: (الكشف عن التهديدات - تقييم مستوى الخطورة - الاستجابة للهجمات - التعافي بعد الحوادث) بالاعتماد على دراسات (Şahinoglu, 2024) ؛ (Kalinin et al., 2021)؛ (Bitton et al., 2021)

المخرجات الأمنية

تنتهي عملية المعالجة بإنتاج مخرجات تساعد في تقييم المخاطر واتخاذ القرار، وتشمل:

- درجة مخاطر ديناميكية يتم تحديثها بحسب تغيّرات البيانات الفعلية.
- توصيات فورية للتخفيف من الهجمات مثل عزل المسار المعرض للخطر، أو تعزيز إجراءات الأمن في نقطة معينة داخل النظام.

الشكل رقم (١) متغيرات الدراسة



المصدر : من إعداد الباحث بالاعتماد على الدراسات السابقة

مصطلحات الدراسة وتعريفاتها الإجرائية:

أولاً: التعلم الآلي (Machine Learning)

اصطلاحاً: يُعرّف التعلم الآلي بأنه أحد فروع الذكاء الاصطناعي الذي يركّز على تطوير خوارزميات قادرة على معالجة البيانات الضخمة والتعلّم منها بطريقة ذاتية، بما يتيح للأنظمة اكتشاف الأنماط والعلاقات الخفية دون تدخل بشري مباشر، ويُستخدم لتوليد تنبؤات دقيقة واتخاذ قرارات مدعومة بالبيانات في البيئات المعقدة والمتغيرة. (Kayraklioglu et al., 2021)

إجرائيًا: يُقصد بالتعلم الآلي في هذه الدراسة مجموعة من التقنيات الذكية التي تشمل التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي، والتي تُساهم في بناء نموذج متكامل لتقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية.

أولاً: التحليل التنبؤي (Predictive Analytics)

اصطلاحًا: يُعرّف التحليل التنبؤي بأنه عملية تحليل متقدمة تعتمد على استخدام خوارزميات التعلم الآلي والنماذج الإحصائية لاكتشاف الأنماط في البيانات التاريخية والتنبؤ بالاتجاهات المستقبلية أو الأحداث المحتملة، مما يساعد المؤسسات على اتخاذ قرارات استباقية مبنية على الأدلة. (Ateya, 2024)

إجرائيًا: يُقصد بالتحليل التنبؤي في هذه الدراسة قدرة أنظمة النقل الذكية على استخدام خوارزميات التعلم الآلي لتحليل البيانات التشغيلية السابقة والتنبؤ بالتهديدات السيبرانية المستقبلية، بما يساهم في تعزيز الوقاية واتخاذ إجراءات أمنية استباقية.

ثانيًا: الكشف الذكي عن الهجمات (Intelligent Attack Detection)

اصطلاحًا: يُعرّف الكشف الذكي عن الهجمات بأنه تطبيق لخوارزميات التعلم الآلي في تحليل حركة البيانات الرقمية ورصد السلوكيات غير الطبيعية بهدف الكشف التلقائي عن التهديدات السيبرانية في الوقت الفعلي، مع تمييز الأنشطة الخبيثة عن العمليات المشروعة في الشبكات المعقدة. (Bui et al., 2023)

إجرائيًا: يُقصد بالكشف الذكي عن الهجمات في هذه الدراسة القدرة التلقائية للنظام على اكتشاف الأنماط الشاذة أو الأنشطة المشبوهة في شبكات النقل الذكية، وذلك من خلال تحليل تدفقات البيانات واستخدام النماذج الذكية للتعرف على الهجمات قبل وقوعها.

ثالثًا: التصنيف التلقائي للمخاطر (Automated Risk Classification)

اصطلاحًا: يُعرّف التصنيف التلقائي للمخاطر بأنه إحدى تطبيقات التعلم الآلي التي تهدف إلى تصنيف أنواع التهديدات أو الثغرات الأمنية ضمن فئات محددة وفقًا لدرجات الخطورة أو الاحتمالية، وذلك بالاعتماد على تحليل خصائص البيانات الأمنية. (Franco et al., 2022)

إجرائيًا: يُقصد بالتصنيف التلقائي للمخاطر في هذه الدراسة استخدام خوارزميات التعلم الآلي لتصنيف التهديدات السيبرانية في أنظمة النقل الذكية إلى فئات مثل: منخفضة، متوسطة، وعالية الخطورة، بما يتيح تحسين أولويات الاستجابة واتخاذ القرارات الأمنية السريعة.

رابعًا: التحسين الذاتي (Self-Optimization)

اصطلاحًا: يُعرّف التحسين الذاتي بأنه قدرة النظام القائم على التعلم الآلي على تحسين أدائه تلقائيًا بمرور الوقت من خلال تحليل نتائج القرارات السابقة، وتعديل الأوزان والمعايير الداخلية للنموذج بهدف الوصول إلى أفضل أداء ممكن. (Phiri et al., 2025)

إجرائيًا: يُقصد بالتحسين الذاتي في هذه الدراسة قدرة نظام النقل الذكي على تعلم كيفية تحسين استجابته للمخاطر السيبرانية بصورة مستمرة، عبر تعديل معايير التلقائية استنادًا إلى الخبرات السابقة والبيانات المستحدثة، مما يرفع من كفاءة حماية البنية التحتية للنقل.

ثانيًا: الأمن السيبراني (Cybersecurity)

اصطلاحًا: يُعرّف الأمن السيبراني بأنه مجموعة من الممارسات والتقنيات والسياسات المصممة لحماية الأنظمة الرقمية والشبكات والبيانات من التهديدات والهجمات الإلكترونية، مع ضمان توافر المعلومات وسريتها وسلامتها التشغيلية ضمن بيئات العمل التقنية المعقدة. (Şahinoglu, 2024)

إجرائيًا: يُقصد بالأمن السيبراني في هذه الدراسة منظومة الحماية الرقمية في أنظمة النقل الذكية، التي تشمل حماية قواعد البيانات وشبكات الاتصالات والتحكم المروري من الاختراق أو التعطيل، بهدف تعزيز القدرة على تقييم وتوقع المخاطر السيبرانية وتحسين كفاءة الاستجابة لها.

ثالثًا: تقييم مخاطر الأمن السيبراني (Cybersecurity Risk Assessment)

اصطلاحًا: يُعرّف تقييم مخاطر الأمن السيبراني بأنه عملية تحليلية منهجية تهدف إلى تحديد التهديدات المحتملة للأصول الرقمية، وتقدير احتمالية وقوعها وتأثيرها، من أجل تحديد أولويات المعالجة ووضع استراتيجيات فعّالة للحد من آثارها. (Ganesan et al., 2022)

إجرائيًا: يُقصد بتقييم مخاطر الأمن السيبراني في هذه الدراسة عملية تحليل وتقدير مستوى التهديدات السيبرانية في أنظمة النقل الذكية من خلال استخدام تقنيات التعلم الآلي في تحليل البيانات التشغيلية والكشف التنبؤي عن الهجمات وتصنيفها حسب درجة الخطورة.

رابعًا: أنظمة النقل الذكية (Intelligent Transportation Systems)

اصطلاحًا: تُعرّف أنظمة النقل الذكية بأنها منظومات متكاملة توظف تقنيات الاتصالات والمعلومات والاستشعار الذكي لتحسين كفاءة وأمان وموثوقية حركة النقل عبر تحليل البيانات الميدانية واتخاذ القرارات التشغيلية بشكل آلي. (Kalinin et al., 2021)

إجرائيًا: يُقصد بأنظمة النقل الذكية في هذه الدراسة البنية الرقمية التي تشمل المركبات الذكية، شبكات الطرق المزودة بأجهزة استشعار، وأنظمة المراقبة والتحكم الآلي، والتي تُستخدم كبيئة اختبار لتطبيق تقنيات التعلم الآلي في تحليل وتقييم المخاطر السيبرانية.

منهج الدراسة :

تعتمد هذه الدراسة منهجية متعددة المراحل، تجمع بين الأساليب التجريبية الحاسوبية والأساليب الكمية الوصفية، وذلك بما يتناسب مع طبيعة البحث التي تتناول تطبيقات التعلم الآلي في تقييم مخاطر الأمن السيبراني داخل أنظمة النقل الذكية، ويأتي تبني هذا النهج المتدرج في ضوء الحاجة إلى تجاوز الاعتماد التقليدي على الأدوات الإدراكية (مثل الاستبيانات) نحو منهجية أكثر صرامة تشمل النمذجة، والمحاكاة، والتحقق التجريبي، بما يحقق متطلبات الدراسات العليا في المجالات التقنية.

وسيتم توظيف مبادئ البحث في علوم التصميم (Design Science Research) لتطوير إطار عمل قائم على التعلم الآلي يمكن تطبيقه فعليًا في بيئات النقل الذكية، وتشمل هذه المرحلة تحديد الخوارزميات المناسبة لكل بُعد من أبعاد المتغير المستقل؛ إذ سيتم تطوير نموذج أولي للتحليل التنبؤي باستخدام تقنيات التنبؤ بالسلاسل الزمنية، مثل ARIMA أو نماذج Prophet. كما سيتم تطوير نماذج للكشف الذكي عن الهجمات باستخدام شبكات LSTM و CNN بوصفها خوارزميات فعّالة في تحليل البيانات الزمنية ورصد الأنماط الشاذة، وسيتم استخدام خوارزميات التجميع (K-means, DBSCAN) أو خوارزميات التصنيف الإشرافي مثل Random Forest و XGBoost لتطوير نموذج مبدئي للتصنيف

التلقائي للمخاطر. أما بُعد التحسين الذاتي فسيمثل بتطبيق خوارزميات التعلم المعزز (Reinforcement Learning) التي تسمح للنظام بتحسين قراراته استنادًا إلى التفاعل المستمر مع البيانات.

وفي المرحلة الثانية، سيتم إجراء تحقق تجريبي كمي عبر استخدام بيانات معيارية أو محاكاة مخصصة لبيئات النقل الذكية. وسيتم الاستناد إلى قواعد بيانات عالمية لأنظمة المركبات المتصلة أو الهجمات على المركبات، مثل *Car Hacking Dataset* أو مجموعات بيانات *CAN Bus Intrusion*. وفي حال عدم توفر بيانات مناسبة، سيتم تنفيذ عمليات محاكاة باستخدام أدوات متقدمة مثل برنامج SUMO لمحاكاة تدفق حركة المرور، أو بيئات *NS-3* لمحاكاة الشبكات، بهدف اختبار النموذج تحت سيناريوهات هجومية متعددة، وسيتم تقييم أداء النماذج باستخدام مقاييس علمية مثل الدقة، الاستدعاء، الدقة النوعية (Precision)، معدل الإيجابيات الخاطئة (False Positive Rate)، ومعامل F1، بما يوفر مؤشرات كمية موضوعية لقياس فعالية الإطار المقترح في مواجهة التهديدات السيبرانية.

وسيتم إجراء تحقق نوعي قائم على آراء الخبراء من خلال استبيان موجّه إلى العاملين في مجالات الأمن السيبراني، وتطوير الأنظمة الذكية، وإدارات النقل في المملكة العربية السعودية. ويهدف هذا المسار النوعي إلى جمع آراء الخبراء حول قابلية تطبيق الإطار المقترح في الواقع العملي، وتقييم مدى فعاليته، وتحديد التحديات التي قد تواجه تطبيقه في السياق السعودي، بما يضيف بُعدًا سياقيًا مهمًا لا يمكن الحصول عليه من البيانات المحاكاة أو التجريبية وحدها.

أداة الدراسة

ستعتمد هذه الدراسة على أداتين مكملتين لجمع البيانات، وذلك بما يتناسب مع طبيعة البحث التي تجمع بين الجانب التطبيقي القائم على نماذج التعلم الآلي والجانب الوصفي القائم على تحليل آراء الخبراء. ويأتي هذا التوزيع استجابةً لمتطلبات الدراسات التقنية التي تشترط وجود دليل تجريبي يعتمد على بيانات فعلية أو محاكاة دقيقة، إلى جانب بيانات ميدانية تدعم تفسير النتائج وتعزيز صلاحية الإطار المقترح.

وسيتمثل الدليل التجريبي الرئيس في هذه الدراسة في البيانات التشغيلية التي سيُدرَّب عليها نموذج التعلم الآلي المقترح؛ حيث سيتم استخدام مجموعة بيانات معيارية خاصة بأنظمة النقل الذكية أو بيانات هجمات المركبات المتصلة (مثل *Car-Hacking Dataset* أو *CAN Intrusion Dataset*) في حال توفرها. أما في حالة عدم توفر بيانات فعلية ملائمة للسياق السعودي، فسيتم توليد بيانات تركيبية (Synthetic)

(Data) باستخدام أدوات المحاكاة المتقدمة مثل محاكي حركة المرور SUMO أو محاكاة الشبكات NS-3 لإنشاء سيناريوهات هجومية وتمثيل بيانات الاستشعار، وحركة المرور، والتواصل بين المركبات. ويمثل هذا النوع من البيانات الأساس العلمي لتقييم أداء التقنيات المقترحة، واختبار دقتها في الكشف والتنبؤ والتصنيف والتحسين الذاتي داخل بيئة محاكاة تضاهي واقع النقل الذكي.

أما الأداة الثانية فهي الاستبانة، وستستخدم بوصفها أداة تحقق تكميلية لجمع آراء المتخصصين حول قابلية تطبيق الإطار المقترح وملاءمته للسياق السعودي. ويأتي دور الاستبانة مكملًا للبيانات التجريبية، إذ إنها تسهم في تفسير النتائج التقنية من منظور الخبراء، وتساعد في تحديد التحديات المؤسسية، والتشغيلية، والتقنية التي قد تواجه تطبيق نماذج التعلم الآلي داخل الأنظمة الذكية للنقل.

وستتكون الاستبانة من محورين رئيسيين يمثلان أبعاد المتغيرات قيد الدراسة، الأول لقياس مستوى تبني تقنيات التعلم الآلي في بيئات النقل الذكية، والثاني لقياس فعالية آليات تقييم المخاطر السيبرانية. كما سيُضاف محور للبيانات التعريفية لتمييز خصائص العينة وتحليل الفروق بين فئات المستجيبين. وستُبنى الاستبانة وفق مقياس ليكرت الخماسي، وستُعرض على نخبة من المحكمين للتحقق من صدق المحتوى. وبعد جمع البيانات، سيُختبر الثبات باستخدام معامل كرونباخ ألفا، ومن ثم تُحلل الاستجابات باستخدام الأساليب الإحصائية المناسبة لاختبار الفرضيات.

وبذلك تكون الدراسة قد جمعت بين بيانات تجريبية موضوعية (ناتجة عن النمذجة والمحاكاة) وبيانات إدراكية تفسيرية (ناتجة عن آراء الخبراء)، مما يعزز قوة الدليل العلمي، ويضمن ملاءمة الإطار المقترح لبيئات النقل الذكية في الواقع الخليجي والسعودي على وجه الخصوص.

مجتمع الدراسة:

سيتمّون مجتمع الدراسة من جميع الأفراد العاملين والمتخصصين في مجالات الأمن السيبراني، وتقنيات الذكاء الاصطناعي، وإدارة وتشغيل أنظمة النقل الذكية في المؤسسات الحكومية والخاصة ذات العلاقة بالبنى التحتية الرقمية للنقل في المملكة العربية السعودية، ويشمل ذلك على وجه الخصوص الهيئة العامة للنقل، ووزارة النقل والخدمات اللوجستية، والهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، والهيئة الوطنية للأمن السيبراني، إضافة إلى الشركات التقنية ومراكز الأبحاث المتخصصة في حلول النقل الذكي والأمن السيبراني.

ويمثل هذا المجتمع بيئة بحثية غنية ومتنوعة نظرًا لتداخل تخصصاته بين التقنية والأمن والإدارة، مما يتيح جمع بيانات دقيقة من ذوي الخبرة المباشرة في تشغيل الأنظمة الذكية وحمايتها من المخاطر السيبرانية، ومن المتوقع أن يضم مجتمع الدراسة ما يقارب (٦٠٠-٨٠٠) فرد من العاملين في الإدارات الفنية، ومراكز التحكم المروري الذكي، ووحدات الأمن السيبراني، ومختبرات البيانات في المؤسسات الحكومية وشركات التقنية الوطنية.

عينة الدراسة:

نظرًا لحجم مجتمع الدراسة المقدر بما يتراوح بين (600 - 800) فرد من المتخصصين في مجالات الأمن السيبراني، وتقنيات الذكاء الاصطناعي، والنقل الذكي، فستُختار عينة ممثلة من هذا المجتمع بطريقة العينة الطبقية العشوائية (Stratified Random Sampling)، وذلك لضمان تمثيل الفئات المختلفة من حيث جهة العمل، وطبيعة المهام، والمستوى الوظيفي، والتخصص الفني.

وبالاستناد إلى جدول مورجان وكريجسي (Krejcie & Morgan, 1970) لتحديد حجم العينات في البحوث الكمية، فإن الحجم المناسب لعينة من مجتمع يتراوح بين (٦٠٠ - ٨٠٠) فرد يُقدَّر بنحو (250 - 265) مفردة على الأقل لتحقيق مستوى ثقة إحصائية قدره (٩٥٪) وهامش خطأ لا يتجاوز (±5%).

وستستهدف الدراسة توزيع عدد (٣٠٠) استبانة لضمان الحصول على (250) استبانة صالحة للتحليل الإحصائي بعد استبعاد النماذج غير المكتملة أو غير الصالحة، وبما يعزز موثوقية النتائج وقابليتها للتعميم على مجتمع الدراسة الكلي، وسيتم توزيع الاستبانات إلكترونياً من خلال البريد المؤسسي والمنصات الرسمية للهيئة الوطنية للأمن السيبراني، والهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، والهيئة العامة للنقل، إضافة إلى عدد من شركات التقنية والمراكز البحثية المعنية بتطوير وتشغيل أنظمة النقل الذكية في المملكة.

مصادر البيانات في الدراسة

أولاً: المصادر الثانوية

ستعتمد هذه الدراسة على مصادر بيانات أولية وثانوية لتحقيق أهدافها والإجابة عن تساؤلاتها، بما يضمن شمولية المعلومات ودقتها وموثوقيتها.

أولاً: المصادر الأولية (Primary Data)

سوف تتمثل في البيانات الميدانية التي سيتم جمعها مباشرة من أفراد عينة الدراسة باستخدام الاستبانة التي صُممت خصيصاً لأغراض هذا البحث، وستغطي هذه البيانات آراء وتصورات الخبراء والمختصين في مجالات الأمن السيبراني، وتقنيات الذكاء الاصطناعي، والنقل الذكي، حول مدى تأثير تقنيات التعلم الآلي (التحليل التنبؤي، الكشف الذكي، التصنيف التلقائي، والتحسين الذاتي) في تحسين عمليات تقييم مخاطر الأمن السيبراني داخل أنظمة النقل الذكية، وسيتم جمع هذه البيانات إلكترونياً عبر استبانات رقمية تُوزع على المؤسسات ذات الصلة، مثل الهيئة الوطنية للأمن السيبراني، والهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، ووزارة النقل والخدمات اللوجستية، والهيئة العامة للنقل، إضافة إلى شركات تقنية رائدة مثل علم، وأرامكو الرقمية، وهوآوي السعودية، لضمان تمثيل دقيق للبيئة البحثية الواقعية.

ثانياً: المصادر الثانوية (Secondary Data)

ستعتمد الدراسة على تحليل الأدبيات النظرية والدراسات السابقة ذات الصلة بمجالات التعلم الآلي، والأمن السيبراني، وأنظمة النقل الذكية، سواء المنشورة في المجالات العلمية المحكمة، أو قواعد البيانات العالمية، إلى جانب التقارير الرسمية الوطنية الصادرة عن الهيئة الوطنية للأمن السيبراني، وسدايا، والبنك الدولي، ومنظمة النقل الذكي العالمية (ITS). وسيتم توظيف هذه المصادر في بناء الإطار النظري للدراسة، وتحديد الفجوة البحثية، وتطوير النموذج المفاهيمي، وصياغة الأداة الميدانية بما يتوافق مع الأسس العلمية الراسخة.

المعالجات الإحصائية المقترحة:

الأساليب الإحصائية

سُجِّرى المعالجات الإحصائية المقترحة باستخدام برنامج (SPSS) الإصدار الأحدث، وذلك بهدف تحليل البيانات الميدانية المستخلصة من الاستبانة والتحقق من صحة الفرضيات.

وسوف تُستخدم مجموعة من الأساليب الإحصائية الوصفية والاستدلالية وفق الخطوات التالية:

التحقق من صدق وثبات أداة الدراسة:

- سيتم حساب معامل الثبات كرونباخ ألفا (Cronbach's Alpha) لكل محور من محاور الاستبانة ولأداة ككل، للتأكد من درجة اتساقها الداخلي.
- كما سيتم التحقق من صدق المحكمين (Content Validity) وصدق الاتساق الداخلي من خلال معاملات الارتباط بين الفقرات ومحاورها.

التحليلات الإحصائية الوصفية:

- استخدام التكرارات، النسب المئوية، المتوسطات الحسابية، والانحرافات المعيارية لوصف خصائص عينة الدراسة وقياس مستوى استجاباتهم تجاه بنود كل محور.
- تحليل الاتجاه العام لاستجابات المبحوثين نحو أبعاد المتغيرات الرئيسية.
- التحليلات الإحصائية الاستدلالية (Inferential Statistics):
- اختبار معامل الارتباط بيرسون (Pearson Correlation) لقياس قوة واتجاه العلاقة بين أبعاد تقنيات التعلم الآلي ومكونات تقييم مخاطر الأمن السيبراني.
- تحليل الانحدار المتعدد (Multiple Regression Analysis) لاختبار الفرضيات الرئيسية والفرعية وتحديد حجم وتأثير كل بعد من أبعاد التعلم الآلي على تقييم المخاطر السيبرانية.

حدود الدراسة

- **الحدود الموضوعية:** تقتصر الدراسة على تحليل أثر تقنيات التعلم الآلي بأبعادها الأربعة (التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي) على تقييم مخاطر الأمن السيبراني بأبعاده الأربعة (الكشف، التقييم، الاستجابة، والتعافي) في أنظمة النقل الذكية.
- **الحدود الزمانية:** تُجرى هذه الدراسة خلال عام ٢٠٢٥.
- **الحدود المكانية:** تقتصر هذه الدراسة على البيئة السعودية بوصفها نموذجًا متطورًا في تبني تقنيات النقل الذكي والأمن السيبراني، وبخاصة في مدن مثل الرياض، وجدة، والدمام.

- **الحدود البشرية :** تشمل الحدود البشرية العاملين والمتخصصين في مجالات الأمن السيبراني، وتقنيات التعلم الآلي، وإدارة وتشغيل أنظمة النقل الذكية في المؤسسات الحكومية والخاصة داخل المملكة.

الفصل الثاني : الاطار النظري والدراسات السابقة

المبحث الأول : تقنيات التعلم الآلي في البيئات الرقمية الحيوية

تمهيد

شهد العقد الأخير تحولاً جوهرياً في الفكر التقني العالمي تجاه ما باتت تعرفه الأدبيات المتخصصة بـ"الأمثلة المعرفية" التي تنهض عليها خوارزميات التعلم الآلي، وهي التحول الذي أعاد رسم العلاقة بين المنظومات الرقمية والبيانات بوصفها مصدراً للقرار لا مجرد سجلٍ للأحداث.

ويتناول هذا المبحث الأبعاد المفاهيمية والنظرية والتطبيقية لتقنيات التعلم الآلي، بدءاً من نشأتها ضمن منظومة الذكاء الاصطناعي، مروراً بتعدد تعريفاتها وخصائصها وأنواعها، وانتهاءً بأبعادها الأربعة التي تتبناها الدراسة الحالية بوصفها متغيراً مستقلاً، إلى جانب استعراض التحديات والاتجاهات المعاصرة التي تؤطر مسار تطورها.

أولاً: نشأة التعلم الآلي وتطوره ضمن منظومة الذكاء الاصطناعي

يُعدّ التعلم الآلي (Machine Learning) أحد أبرز الفروع المنبثقة عن حقل الذكاء الاصطناعي، وقد نشأ في خمسينيات القرن العشرين بوصفه استجابة علمية للحاجة المتنامية إلى بناء أنظمة حاسوبية قادرة على محاكاة بعض القدرات الإدراكية البشرية، ولا سيما القدرة على التعلم من الخبرة وتحسين الأداء بمرور الوقت دون الحاجة إلى برمجة صريحة لكل سلوك، ولم يكن ظهور هذا الحقل حدثاً معزولاً، بل جاء استجابة لتطورات متلاحقة في علم الإحصاء ونظرية الاحتمالات والمنطق الرياضي، مما أتاح للباحثين توظيف أدوات تحليلية متقدمة في تصميم خوارزميات تتجاوز المعالجة الحتمية التقليدية إلى المعالجة الاحتمالية والتكيفية.

ويُشير العدوان (٢٠٢٢) إلى أن التطور التاريخي للتعلم الآلي مرّ بمراحل متعاقبة، حيث ارتبط في بداياته بالأنظمة الخبيرة ذات القواعد المغلقة، ثم انتقل تدريجياً نحو نماذج إحصائية أكثر مرونة، قبل أن يدخل في طوره الراهن المرتبط بالشبكات العصبية العميقة والقدرات الحوسبية الفائقة، وقد أسهم هذا التطور في إعادة تعريف العلاقة بين الإنسان والآلة، إذ لم تعد الآلة مجرد منفذ للأوامر، بل أصبحت كياناً قادراً على استخلاص الأنماط والتعلم من البيانات والتنبؤ بنتائج لم يسبق له مشاهدتها.

ويرى (Ateya (2024 أن التعلم الآلي يمثل نقلة نوعية في فلسفة معالجة المعلومات، إذ يقوم على افتراض جوهري مفاده أن البيانات تتطوي على بنى كامنة قابلة للاكتشاف عبر النمذجة الرياضية، وأن قدرة النظام على اكتشاف هذه البنى تتحسن طردياً مع تزايد حجم البيانات وتنوعها.

ويؤكد (Kayraklioglu et al. (2021 أن هذه الركائز الثلاث شكّلت بيئة خصبة أتاحت للتعلم الآلي تجاوز حدوده المخبرية ليصبح أداة تطبيقية في مجالات متعددة تشمل الأمن السيبراني والرعاية الصحية والصناعة والتمويل والنقل الذكي.

و يمكن القول إن النشأة المتدرجة للتعلم الآلي قد أفرزت تراكمًا معرفيًا واسعاً جعل منه حقلاً متعدد التخصصات، يتقاطع مع الإحصاء والرياضيات وعلوم الحاسب وعلم الأعصاب الحاسوبي، مما منحه ثراءً نظرياً وعمقاً تطبيقياً جعله قادراً على الاستجابة لمتطلبات البيئات الرقمية الحيوية المعقدة، ومنها أنظمة النقل الذكية التي تُمثّل محور الدراسة الحالية.

ثانياً: المفهوم التعلم الآلي

تعددت التعريفات التي قدّمها الباحثون لمفهوم التعلم الآلي تبعاً لاختلاف المداخل النظرية والتطبيقية التي انطلقوا منها، غير أن هذه التعريفات تتقاطع في جوهرها حول فكرة محورية مفادها أن التعلم الآلي يقوم على تمكين الأنظمة الحاسوبية من اكتساب المعرفة من البيانات دون برمجة مباشرة، ويُعرّف بن التركي وموسى وخالدي (٢٠٢١) التعلم الآلي بأنه فرع من الذكاء الاصطناعي يُعنى بتصميم خوارزميات قادرة على التعلم من البيانات وتحسين أدائها ذاتياً بمرور الوقت، بحيث تتمكن من اتخاذ قرارات أو إجراء تنبؤات بناءً على الأنماط التي اكتشفتها في مرحلة التدريب.

و يقدّم (Phiri et al. (2025 تعريفاً يصف التعلم الآلي بأنه منظومة من النماذج الرياضية والإحصائية التي تُمكن الحواسيب من معالجة كميات ضخمة من البيانات غير المهيكلة، وتحويلها إلى رؤى قابلة للاستثمار في دعم اتخاذ القرار في البيئات المتغيرة، ويتقاطع مع عبد ربه (٢٠٢٤) من أن التعلم الآلي يمثل جسراً معرفياً يربط بين البيانات الخام والقرار الذكي، حيث تتولى الخوارزميات استخلاص العلاقات الكامنة وتحويلها إلى نماذج تنبؤية قابلة للتطبيق في سياقات حقيقية تتسم بعدم اليقين.

ويُعرّف Bitton et al. (2023) التعلم الآلي بوصفه منظومة متكاملة من المكونات تشمل البيانات والخوارزمية والنموذج وآلية التقييم، تعمل في حلقة متصلة من التغذية الراجعة بحيث تُحسن المخرجات بصورة مستمرة.

ويُضيف Saba et al. (2024) بُعداً وظيفياً للتعريف، إذ يصف التعلم الآلي بأنه القدرة الحاسوبية على بناء تمثيلات تجريدية للظواهر الرقمية والمادية، تمكّن النظام من التعميم على حالات لم يسبق أن تعرّض لها أثناء التدريب، وهو ما يمنح هذا الحقل ميزة استثنائية في مواجهة بيئات شديدة الديناميكية كبيئات الأمن السيبراني والنقل الذكي.

ومن وجهة نظر الباحث يُعرّف بأنه "منظومة معرفية-تقنية متعددة الأبعاد، تقوم على توظيف خوارزميات إحصائية ورياضية قادرة على التعلم التكيفي من البيانات، وبناء نماذج تنبؤية وتصنيفية ذاتية التحسين، تمكّن الأنظمة الرقمية الحيوية ومنها أنظمة النقل الذكية من اكتشاف الأنماط المعقدة وتقدير المخاطر واتخاذ قرارات استباقية في بيئات تتسم بعدم اليقين والتطور المتسارع".

ثالثاً: الخصائص المميزة لخوارزميات التعلم الآلي

تتفرد خوارزميات التعلم الآلي بجملة من الخصائص النوعية التي تُميّزها عن الأنظمة الحاسوبية التقليدية القائمة على البرمجة الصريحة، وتُكسبها قدرة استثنائية على التعامل مع البيئات الرقمية المعقدة كبيئات الأمن السيبراني وأنظمة النقل الذكية، وقد تناول الباحثون هذه الخصائص من زوايا متعددة، فجاءت رؤاهم متكاملة في رسم ملامح هذه التقنية وتمييزها عن غيرها من الأدوات التحليلية.

فيشير عبد ربه (٢٠٢٤) إلى أن خوارزميات التعلم الآلي تتطوي على مجموعة من الخصائص الجوهرية التي تمنحها أفضلية تنافسية في معالجة الظواهر المعقدة، يمكن إجمالها على النحو التالي:

١. **القدرة التكيفية (Adaptability)** تتمتع هذه الخوارزميات بقدرة استثنائية على تعديل سلوكها استجابةً للتغيرات الحاصلة في البيانات المُدخلة، دون الحاجة إلى إعادة برمجة كاملة، الأمر الذي يجعلها أداة فاعلة في التعامل مع الظواهر شديدة الديناميكية كالتقلبات في الأسواق المالية وأنماط التهديدات السيبرانية المتطورة.

٢. **التعلم التراكمي من البيانات**: تقوم هذه الخوارزميات على مبدأ التحسين المستمر للأداء كلما تعرّضت لبيانات جديدة، بحيث تتطوّر معرفتها الكامنة بمرور الوقت، وهو ما يُحاكي إلى حدٍ بعيد آلية اكتساب الإنسان لخبراته المتراكمة.

٣. **التعامل مع البيانات الضخمة وغير المهيكلة**: تستطيع هذه الخوارزميات معالجة كميات هائلة من البيانات المتنوعة في طبيعتها ومصادرها، سواء أكانت نصية أم رقمية أم بصرية، وهو ما يمنحها أفضلية حاسمة في عصر تتراكم فيه البيانات بمعدلات غير مسبقة.

٤. **استخلاص الأنماط الكامنة**: تتميز هذه الخوارزميات بقدرتها على اكتشاف العلاقات غير الظاهرة بين المتغيرات، وتحويلها إلى نماذج تنبؤية قابلة للتطبيق في سياقات حقيقية تتسم بعدم اليقين.

كما يُشير (Saba et al(2024 إلى أن ما يُميّز خوارزميات التعلم الآلي من الناحية البنيوية والوظيفية يتمثّل في عدة خصائص متكاملة، أبرزها:

١. **القدرة على التعميم (Generalization)**: وتُشير إلى قدرة النموذج المُدرَّب على إنتاج تنبؤات صحيحة بشأن حالات لم يسبق له التعرّض لها أثناء مرحلة التدريب، وهي خاصية محورية لأنها تُحدّد الفارق الجوهرى بين النموذج الذي يحفظ البيانات والنموذج الذي يفهم بنيتها الكامنة.

٢. **الاستقلالية النسبية في اتخاذ القرار**: إذ يمكن لنماذج التعلم الآلي اتخاذ قرارات تشغيلية فورية دون تدخّل بشري مباشر، وهو ما يجعلها مناسبة للبيئات التي تتطلب استجابة آنية كأنظمة النقل الذكية التي تتعامل مع متغيرات متسارعة في كل لحظة.

٣. **قابلية التوسع (Scalability)**: حيث يمكن تطبيق النماذج المُطوّرة على نطاقات أكبر دون أن يتطلب ذلك تعديلات جوهرية على بنيتها الأساسية، مما يُتيح توظيفها في منظومات وطنية واسعة كأنظمة النقل الحضري والبنى التحتية الحيوية.

٤. **بناء التمثيلات التجريدية**: تمتلك هذه الخوارزميات القدرة على بناء تمثيلات رياضية تجريدية للظواهر الرقمية والمادية، مما يمكّنها من تحليل المشهد العام بدلاً من الاكتفاء بمعالجة البيانات الجزئية المعزولة.

ويُضيف نور الدين وبو صلاح (٢٠٢٥) بُعداً تكميلياً في توصيف خصائص خوارزميات التعلم الآلي، حيث يُشير إلى أن هذه الخوارزميات تنطوي على مجموعة من السمات التي تجعلها أداة استراتيجية في صناعة القرار التنظيمي، وتتمثل في:

١. **الدقة في النمذجة:** إذ تستطيع هذه الخوارزميات بناء نماذج عالية الدقة بفضل اعتمادها على أسس إحصائية ورياضية متينة، وهو ما يُقلل من نسبة الخطأ في التنبؤات والتصنيفات.

٢. **السرعة في المعالجة:** فهي قادرة على إنجاز عمليات تحليلية معقدة في زمن وجيز، وهو ما يُلبّي متطلبات البيانات التي تستلزم استجابة فورية كبيئات الكشف عن التهديدات السيبرانية.

٣. **التعدد الخوارزمي:** إذ تتوفر تشكيلة واسعة من الخوارزميات التي يمكن المفاضلة بينها وفقاً لطبيعة المشكلة المطروحة وبنية البيانات المتاحة، مما يمنح الباحث والمصمم مرونة عالية في الاختيار والتطبيق.

٤. **المرونة التطبيقية عبر القطاعات:** حيث لا ترتبط هذه الخوارزميات بقطاع بعينه، بل يمكن تكييفها لخدمة قطاعات متباينة كالقطاع الرياضي والتعليمي والصحي والأمني، مما يعكس طبيعتها العابرة للتخصصات.

رابعاً: أنواع التعلم الآلي

تتعدد تصنيفات خوارزميات التعلم الآلي تبعاً لطبيعة عملية التعلم وآليتها، وطبيعة البيانات المتاحة، والهدف من النمذجة. وقد استقرت الأدبيات المتخصصة على أربعة أنواع رئيسية تُمثل البنية التصنيفية المعتمدة لهذا الحقل، وهي: التعلم الموجّه (Supervised Learning)، والتعلم غير الموجّه (Unsupervised Learning)، والتعلم المعزز (Reinforcement Learning)، والتعلم العميق (Deep Learning). ولكل نوع من هذه الأنواع منطقه الخاص في معالجة البيانات وبناء النماذج، فضلاً عن مجالات توظيفه المثلى ومحدداته التطبيقية.

ويُفصّل برارمة (٢٠٢٤) الحديث عن الأنواع الأساسية للتعلم الآلي، موضحاً أن لكلٍ منها بنية معرفية مستقلة، وذلك على النحو التالي:

- **التعلم الموجّه (Supervised Learning):** يُعدّ النوع الأكثر شيوعاً في التطبيقات العملية، ويقوم على تدريب الخوارزمية على مجموعة من البيانات المُصنّفة مسبقاً، بحيث تتعلّم النموذج العلاقة بين المدخلات والمخرجات المعروفة، ثم تستثمر هذه العلاقة في التنبؤ بمخرجات حالات جديدة. ومن أبرز خوارزمياته: الانحدار الخطي، وأشجار القرار، وآلات المتجهات الداعمة (SVM).

- **التعلم غير الموجّه (Unsupervised Learning):** يقوم على معالجة بيانات غير مُصنّفة، حيث تتولّى الخوارزمية اكتشاف الأنماط والتجمعات الكامنة في البيانات دون توجيه مسبق، وهو ما يجعله أداة فاعلة في الكشف عن الأنماط الشاذة كالتي تُشير إلى محاولات اختراق سيبراني غير مألوفة.

- **التعلم المعزّز (Reinforcement Learning):** يستند إلى مبدأ التعلم بالتجربة والخطأ، حيث يتفاعل الوكيل الذكي (Agent) مع بيئته من خلال سلسلة من الإجراءات، ويتلقّى مكافآت أو عقوبات تبعاً لجودة قراراته، فيُعدّل سياسته تدريجياً نحو تعظيم المكافأة التراكمية.

أما (Ateya (2024 فيتناول النوع الرابع التعلم العميق (Deep Learning) بوصفه فرعاً متقدماً ينحدر من التعلم الآلي ويرتكز على الشبكات العصبية الاصطناعية متعددة الطبقات، ويُجمل أبرز ملامحه فيما يأتي:

- **البنية الطبقيّة المتعددة:** يقوم التعلم العميق على شبكات عصبية تتكوّن من طبقات متتالية، تتولّى كل طبقة استخلاص مستوى معيّن من التجريد، بحيث تنتقل البيانات من تمثيلات بسيطة في الطبقات الأولى إلى تمثيلات شديدة التجريد في الطبقات العليا.

- **القدرة على معالجة البيانات الخام:** يتميّز التعلم العميق عن النماذج التقليدية في قدرته على التعامل مع البيانات الخام دون الحاجة إلى مرحلة هندسة الخصائص (Feature Engineering) اليدوية، إذ تتولّى الشبكة استخراج الخصائص ذاتياً.

- **التفوّق في المهام المعقّدة:** يُبدي التعلم العميق تفوّقاً ملحوظاً في المسائل التي تتسم بتعقيد عالٍ كروية الحاسوب ومعالجة اللغات الطبيعية وتحليل سلاسل البيانات الزمنية، وهو ما جعله أداة محورية في تطبيقات الأمن السيبراني وأنظمة النقل الذكية.

- الحاجة إلى موارد حوسبية مرتفعة: يستلزم التعلم العميق بيئة حوسبية متطورة وكميات هائلة من البيانات التدريبية، وهو ما يُمثّل قيداً تطبيقياً ينبغي مراعاته عند اختيار هذا النوع.

ولاستيضاح الفروق الجوهرية بين هذه الأنواع، يمكن عرضها في الجدول التالي:

جدول رقم (١): مقارنة بين الأنواع الرئيسية لخوارزميات التعلم الآلي

وجه المقارنة	التعلم الموجّه	التعلم غير الموجّه	التعلم المعزّز	التعلم العميق
طبيعة البيانات	بيانات مُصنّفة مسبقاً	بيانات غير مُصنّفة	تفاعل ديناميكي مع البيئة	بيانات خام بأحجام ضخمة
الهدف الجوهري	التنبؤ والتصنيف	اكتشاف الأنماط والعناقيد	تعظيم المكافأة التراكمية	استخلاص تمثيلات متعددة المستويات
آلية التعلم	المقارنة بالمرجات المعروفة	التحليل الذاتي للبنية الكامنة	التجربة والخطأ والتغذية الراجعة	الشبكات العصبية متعددة الطبقات
الموارد المطلوبة	متوسطة	منخفضة إلى متوسطة	عالية	عالية جداً
التطبيق في الأمن السيبراني	تصنيف التهديدات المعروفة	الكشف عن السلوكيات الشاذة	تطوير سياسات استجابة تكييفية	التحليل التنبؤي العميق للهجمات

خامساً: أبعاد لتقنيات التعلم الآلي

تمّ تحديد أبعاد المتغير المستقل (تقنيات التعلم الآلي) في الدراسة الحالية بناءً على المراجعة المُعمّقة للأدبيات المتخصصة، ولا سيّما دراسة شيت وإبراهيم (٢٠٢٣) التي قدّمت إطاراً تطبيقياً لتوظيف التعلم الآلي في تقييم مخاطر الأمن السيبراني، ودراسة Franco et al (2022) التي طوّرت نموذجاً قائماً على التعلم الآلي للتنبؤ بالمخاطر السيبرانية في المؤسسات، ودراسة Saba et al(2024) التي طرحت إطاراً ذكياً ثنائي المرحلة لتعزيز الأمن السيبراني في تطبيقات إنترنت الأشياء، فضلاً عن دراسة

(Chowdhury (2025) التي تناولت توظيف نماذج التعلم العميق في التقييم الآني لمخاطر الأمن السيبراني في الأنظمة المؤسسية، وقد تقاطعت هذه الدراسات في إبراز أربعة أبعاد جوهرية يقوم عليها توظيف التعلم الآلي في تقييم المخاطر السيبرانية، تتمثل في: **التحليل التنبؤي، والكشف الذكي عن الهجمات، والتصنيف التلقائي للمخاطر، والتحسين الذاتي،** وهي الأبعاد التي تتبناها الدراسة الحالية بوصفها إطاراً قياسياً للمتغير المستقل.

١. البُعد الأول: التحليل التنبؤي (Predictive Analytics)

يُمثل التحليل التنبؤي حجر الزاوية في منظومة التعلم الآلي الموجهة للأمن السيبراني، إذ يُتيح الانتقال من نمط الاستجابة التفاعلية إلى نمط الدفاع الاستباقي القائم على استشراف التهديدات قبل وقوعها. **ويذهب عبد ربه (٢٠٢٤) إلى أن التحليل التنبؤي يقوم على منظومة متكاملة من الآليات الإحصائية والخوارزمية، يُجمل أبرز ركائزها فيما يأتي:**

- الاعتماد على البيانات التاريخية بوصفها مصدراً لاستنباط الأنماط التي قد تتكرر مستقبلاً، إذ يفترض التحليل التنبؤي أن الماضي يحمل إشارات قابلة للاستثمار في توقع المستقبل.
- توظيف النماذج الإحصائية المتقدمة كنماذج الانحدار والسلاسل الزمنية، التي تُمكن من قياس العلاقات بين المتغيرات وتحديد اتجاهاتها المستقبلية بدقة عالية.
- التعامل مع عدم اليقين عبر إنتاج تقديرات احتمالية بدلاً من قيم حتمية، مما يعكس الطبيعة الاحتمالية للظواهر المُتنبأ بها كالهجمات السيبرانية.
- التحسين المستمر للنماذج من خلال إعادة معايرتها دورياً في ضوء البيانات الجديدة، بحيث تتطور دقتها مع مرور الوقت.

ويُكمل Yao & García de Soto (2024) هذا الطرح برؤية متخصصة في سياقات البنى التحتية الحيوية، إذ يُشير إلى أن التحليل التنبؤي يستند إلى الاستشعار الاستباقي للتهديدات عبر رصد الإشارات الضعيفة التي تسبق الهجمات، والنمذجة الديناميكية للمخاطر التي تأخذ في الاعتبار التغيرات المستمرة في بيئة التهديد، ودمج البيانات متعددة المصادر بما يمنح النموذج رؤية شمولية، إلى جانب توفير أساس كمي لاتخاذ القرار يحول القرارات الأمنية من قرارات حدسية إلى قرارات مدعومة بأدلة موضوعية.

ومن المنظور التطبيقي، يكتسب هذا البُعد في بيئة النقل الذكي أهمية مضاعفة، إذ تُمثّل القدرة على التنبؤ بالتهديدات قبل وقوعها شرطاً جوهرياً لاستدامة المنظومة الأمنية في بيئة تتدفّق فيها البيانات بصورة لحظية من المركبات المتصلة والبنية التحتية الذكية.

٢. البُعد الثاني: الكشف الذكي عن الهجمات (Intelligent Attack Detection)

يُمثّل الكشف الذكي عن الهجمات البُعد التطبيقي الأكثر التصاقاً بمهمة الحماية السيبرانية، إذ يُعنى ببناء نماذج خوارزمية قادرة على التمييز بين السلوكيات الطبيعية والسلوكيات الخبيثة داخل المنظومات الرقمية في الزمن الحقيقي. ويرى شيت وإبراهيم (٢٠٢٣) أن الكشف الذكي عن الهجمات يقوم على مجموعة من الآليات الخوارزمية المتكاملة، تتمثّل في:

- التحليل السلوكي للحركة الشبكية عبر رصد أنماط حركة البيانات داخل الشبكة، واستخلاص بصمة سلوكية مرجعية للمستخدمين والأنظمة، تُستخدم لاحقاً في الكشف عن أي انحراف عنها.
- توظيف خوارزميات التصنيف المُدرّبة على قواعد بيانات الهجمات المعروفة، بحيث تتمكّن من التعرّف الفوري على أنماط الهجوم المتكرّرة كهجمات الحرمان من الخدمة (DDoS) واختراق التشفير وحقق الأكواد.
- الكشف عن الأنماط الشاذة (Anomaly Detection) التي لا تنتمي إلى أي نمط معروف مسبقاً، وهو ما يمنح النموذج قدرة على رصد الهجمات الجديدة (Zero-Day Attacks) التي لم يسبق توثيقها.
- التكامل مع منظومات الاستجابة الآلية بحيث لا يقتصر دور النموذج على الكشف، بل يمتد إلى تحريك إجراءات الاحتواء الفوري.

ويطرح Bui et al (2023) رؤية تخصصية حول الكشف الذكي عن الهجمات في حركة المرور المُشفّرة، مُبرزاً أن هذا البُعد يستثمر تقنيات استخلاص الخصائص (Feature Extraction) من البيانات الشبكية لتحويلها إلى مدخلات قابلة للتحليل بواسطة نماذج التعلم الآلي، حتى في الحالات التي يصعب فيها تفنّيش محتوى الحزم المُشفّرة .

٣. البُعد الثالث: التصنيف التلقائي للمخاطر (Automated Risk Classification)

يُمثّل التصنيف التلقائي للمخاطر البُعد الذي يُحوّل الكشف إلى فعل تشغيلي قابل للترتيب والإدارة، إذ لا يكفي رصد التهديد، بل لا بدّ من تقدير مستواه وتصنيفه ضمن مصفوفة أولويات تُمكن الجهات المعنية من توجيه مواردها بكفاءة. ويُفصّل (Rafaiani et al (2023) الحديث في هذا البُعد، مُشيرين إلى أن التصنيف التلقائي للمخاطر يقوم على مجموعة من النماذج الخوارزمية المتكاملة، يمكن إجمالها على النحو التالي:

- النمذجة متعدّدة المعايير التي تأخذ في الاعتبار أبعاداً متعددة لكل تهديد كاحتمالية وقوعه وحدّة أثره ونطاق انتشاره، وتُنتج تصنيفاً مركّباً يعكس وزن المخاطرة الفعلي.
- التصنيف الهرمي للمخاطر الذي يُرتّب التهديدات في فئات متدرّجة من الأقل خطورة إلى الأعلى، مما يُسهّل توجيه الاستجابة وفقاً لمستوى الأولوية.
- التكيف الديناميكي للتصنيفات بحيث لا تبقى ثابتة، بل تُعاد معايرتها استجابةً للتغيّرات في بيئة التهديد ومستجّات المشهد السيبراني.
- الربط بين التصنيف والاستجابة من خلال تصميم نماذج تُترجم التصنيف الخوارزمي إلى توصيات تشغيلية محدّدة قابلة للتنفيذ.

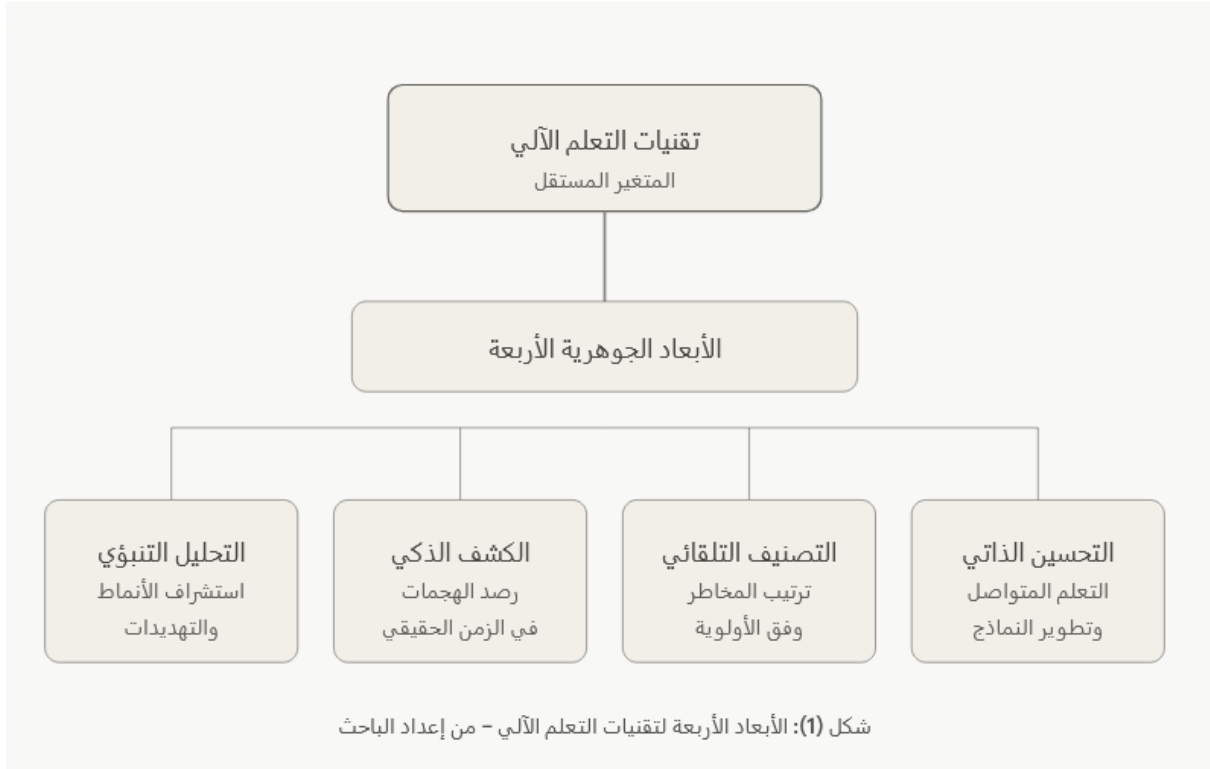
٤. البُعد الرابع: التحسين الذاتي (Self-Optimization)

يُمثّل التحسين الذاتي البُعد الأكثر تطوراً في منظومة التعلم الآلي، إذ يتجاوز فكرة التدريب لمرة واحدة إلى فكرة التعلم المتواصل والتحديث المستمر للنماذج استجابةً للبيانات الجديدة والتهديدات المتطوّرة. ويُؤكد (Chowdhury (2025 أن التحسين الذاتي يُمثّل السمة التي تمنح نماذج التعلم الآلي طابعها التكيفي في بيئات تتسم بالتغير المتسارع، وهو يقوم على عدة ركائز:

- آليات التغذية الراجعة المغلقة (Closed-Loop Feedback) التي تُتيح للنموذج تقييم أدائه ذاتياً، وتعديل معلماته في ضوء نتائج هذا التقييم دون تدخّل بشري مستمر.
- التعلم المعزّز الذي يُمكن النموذج من تطوير سياساته بناءً على تجارب التفاعل مع البيئة، بحيث يُحسّن سلوكه تدريجياً نحو القرارات الأكثر فاعلية.

- معالجة الانحراف المفاهيمي (Concept Drift) الذي يطرأ حين تتغير بنية البيانات أو طبيعة الظواهر المرصودة، إذ تتولى آليات التحسين الذاتي إعادة معايرة النموذج للحفاظ على دقته.
- تحسين معلمات النموذج تلقائياً (Hyperparameter Tuning) عبر خوارزميات بحث ذكية تستكشف الفضاء الواسع للمعلمات وتختار التوليفة المثلى وفق معايير الأداء.

ويضيف (Saba et al (2024) بُعداً تكميلياً يُبرز فيه أن التحسين الذاتي في سياق الأمن السيبراني لأنظمة إنترنت الأشياء يستند إلى بنية ثنائية المرحلة تتألف من مرحلة تعلم أولي تُبنى فيها النماذج، ومرحلة تطوير مستمر تُحدّث فيها هذه النماذج بصورة دورية، كما يؤكدان أن التحسين الذاتي يُحقّق التوازن بين الاستقرار والمرونة؛ فهو يحافظ على القدرات المكتسبة سابقاً، ويُتيح في الوقت ذاته اكتساب قدرات جديدة دون فقدان الأولي، وهو ما يُعرف بمشكلة "النسيان الكارثي" التي تتصدى لها آليات التحسين الذاتي المتقدمة، ويُضفي هذا البُعد على منظومة التعلم الآلي طابعاً حيوياً يجعلها تتطوّر بمرور الوقت بدلاً من التجمّد عند نقطة زمنية معيّنة، وهو ما يتلاءم مع الطبيعة المتغيرة لبيئة التهديد السيبراني، ومع متطلبات الاستدامة التشغيلية لأنظمة النقل الذكية.



سادساً: مجالات توظيف التعلم الآلي في القطاعات الحيوية

شهدت العقود الأخيرة توسعاً ملحوظاً في مجالات توظيف خوارزميات التعلم الآلي، إذ تجاوزت هذه التقنيات حدودها المخبرية لتصبح مكوناً جوهرياً في البنى التشغيلية لقطاعات اقتصادية وخدمية متعددة. ولم يأت هذا التوسع وليد المصادفة، بل جاء استجابة طبيعية للحاجة المتنامية إلى أدوات تحليلية قادرة على التعامل مع التعقيد المتزايد للبيانات، وعلى توليد رؤى قابلة للاستثمار في صناعة القرار في بيئات تتسم بعدم اليقين والتغير المتسارع، وقد تنوّعت مجالات هذا التوظيف بحسب طبيعة كل قطاع ومتطلباته المعرفية والتشغيلية، وهو ما يُمكن استجلاؤه من خلال استعراض أبرز التطبيقات في القطاعات الحيوية.

يستهلّ بن التركي وآخرون (٢٠٢١) نقاشهم لهذه المجالات بالتأكيد على القطاع اللوجستي وسلاسل التوريد بوصفه أحد أكثر القطاعات استثماراً لقدرات التعلم الآلي، حيث تتجلى تطبيقاته في:

- التنبؤ بالطلب وإدارة المخزون، إذ تُتيح خوارزميات التعلم الآلي بناء نماذج دقيقة لتوقع حجم الطلب على المنتجات، مما يُسهم في تخفيض التكاليف التشغيلية ورفع كفاءة إدارة المخزون.
- تحسين مسارات النقل والتوزيع من خلال نماذج تأخذ في الاعتبار عوامل متعددة كحالة الطرق وظروف الطقس وأنماط الازدحام، وتُقدّم توصيات لحظية لاختيار المسار الأمثل.

- رصد المخاطر التشغيلية في سلاسل التوريد عبر تحليل البيانات التاريخية وبيانات الموردين، بما يُتيح الكشف المبكر عن نقاط الضعف المحتملة.

- التكامل مع منظومة إنترنت الأشياء التي تُغذي خوارزميات التعلم الآلي ببيانات الاستشعار في الزمن الحقيقي، مما يدعم اتخاذ قرارات تشغيلية فورية.

وتُبرز Ateya (2024) رؤية متخصصة في توظيف خوارزميات التعلم الآلي لتعزيز القدرة التنبؤية للمعلومات المحاسبية، مُشيرةً إلى أن هذا التوظيف يتجلى في تحليل الأداء المالي للمؤسسات عبر نماذج تستثمر البيانات التاريخية للشركات المُدرجة في توقع مؤشرات الأداء المستقبلية، وفي تقييم المخاطر الائتمانية للعملاء بصورة أكثر دقة من النماذج التقليدية، فضلاً عن اكتشاف الاحتيال المالي من خلال الكشف عن الأنماط الشاذة في المعاملات.

كما يُكمل هذا الطرح ما يطرحه Phiri et al (2025) من تطبيقات في التقييم العقاري في الأسواق المتقلبة، حيث تُمكن نماذج التعلم الآلي من معالجة تعقيد العوامل المؤثرة في القيمة السوقية للعقارات، وتقديم تقديرات أكثر استجابة لتقلبات السوق.

و تُسلط برارمة (٢٠٢٤) الضوء على مجال إدارة المخاطر المؤسسية، مُبرزةً أن خوارزميات التعلم الآلي أعادت تشكيل الممارسات التقليدية لإدارة المخاطر في المؤسسات الاقتصادية عبر عدة مداخل تكاملية، يمكن تلخيصها فيما يلي:

- التحوّل من النموذج التفاعلي إلى النموذج الاستباقي، حيث لم تعد إدارة المخاطر محصورة في الاستجابة للأحداث بعد وقوعها، بل أصبحت قادرة على استشراف المخاطر قبل بروزها.

- معالجة المخاطر متعدّدة الأبعاد التي تتشابك فيها عوامل مالية وتشغيلية واستراتيجية، وهو ما يصعب على الأدوات التقليدية الإحاطة به.

- تخصيص الموارد بكفاءة عبر توجيهها نحو المناطق الأعلى احتمالاً لوقوع المخاطر، بدلاً من توزيعها بصورة متجانسة.

- دعم الحوكمة الرشيدة من خلال توفير أساس كمي شفاف لاتخاذ القرارات المتعلقة بإدارة المخاطر.

ولا يقتصر التوظيف على ما تقدّم، إذ يُضيف نور الدين وبو صلاح (٢٠٢٥) بُعداً نوعياً يتعلق بالقطاعات الخدمية وغير الربحية، مؤكّدين أن خوارزميات التعلم الآلي وجدت موطئ قدم لها في القطاع الرياضي ومنظمات المجتمع المدني عبر تعزيز عمليات التخطيط الاستراتيجي للجمعيات والنوادي الرياضية، وتحليل أداء الفرق والأفراد استناداً إلى بيانات تفصيلية حول مؤشرات الأداء، وتحسين عمليات التسويق الرياضي عبر فهم أعمق لأنماط الجمهور وتفضيلاته.

ويعكس هذا التوظيف الطبيعة العابرة للقطاعات لخوارزميات التعلم الآلي، إذ لم تعد محصورة في القطاعات التقنية أو المالية، بل امتدّت إلى قطاعات كانت تُعدّ تقليدياً بعيدة عن أدوات التحليل الحاسوبي المتقدمة. ومن خلال ما سبق، يتّضح أن خوارزميات التعلم الآلي قد رسّخت حضورها في طيف واسع من القطاعات الحيوية، تمتدّ من اللوجستيات والمال والإدارة إلى الرياضة والأمن السيبراني والنقل الذكي، ويُمثّل هذا التنوّع التطبيقي شاهداً على القدرة الكامنة لهذه التقنية في إعادة تشكيل الممارسات التقليدية في القطاعات المختلفة، كما يُؤسّس منطقياً لاختيار قطاع النقل الذكي ميداناً للدراسة الحالية، باعتباره أحد أكثر القطاعات تعقيداً وحساسيةً، وأشدّها حاجةً إلى أدوات تحليلية متقدمة قادرة على مواكبة تنامي التهديدات السيبرانية وتعدّد البنية الرقمية المتصلة.

سابعاً: المتطلبات التقنية والتنظيمية لتبني تقنيات التعلم الآلي

لا يُمكن أن يتحقق التوظيف الفعال لخوارزميات التعلم الآلي في البيئات الرقمية الحيوية إلا في ظل توافر منظومة متكاملة من المتطلبات التقنية والتنظيمية التي تُهيئ الأرضية اللازمة لاستثمار قدرات هذه التقنيات على النحو الأمثل. وتتوزع هذه المتطلبات على مستويين متلازمين؛ مستوى تقني يتصل بالبنية التحتية الرقمية وجودة البيانات وكفاءة الخوارزميات، ومستوى تنظيمي يتعلق بالحوكمة والسياسات والكوادر البشرية. وقد تباينت رؤى الباحثين في ترتيب أولوية هذه المتطلبات، غير أنهم اتفقوا على أن غياب أيٍّ منها يُمثّل عائقاً حقيقياً أمام تحقيق العائد المنشود من تبني هذه التقنية.

تطرح برارمة (٢٠٢٤) منظوراً تحليلياً يُبرز فيه جملة من الركائز التي تُمثّل الحد الأدنى لتبني خوارزميات التعلم الآلي في المؤسسات الاقتصادية، تتمثّل في:

- توافر بنية تحتية حوسبية قادرة على معالجة كميات ضخمة من البيانات بسرعة عالية، بما يشمل وحدات معالجة الرسومات (GPUs) والخوادم المتخصصة وخدمات الحوسبة السحابية.

- بناء قواعد بيانات منظمة وعالية الجودة تُغذي نماذج التعلم الآلي ببيانات تدريبية موثوقة، إذ تتوقف دقة المخرجات على جودة المدخلات بصورة جوهرية.
- تطوير منصات تحليلية متكاملة تربط بين المصادر المتعددة للبيانات وأدوات النمذجة والتصور، بحيث تتدفق البيانات بصورة سلسلة عبر مراحل المعالجة.
- ضمان أمن البيانات وحوكمتها من خلال آليات تشفير ومراقبة وصول، خاصة في القطاعات الحيوية التي تتعامل مع بيانات حساسة.
- وتُفصل العدوان (٢٠٢٢) جملة من الشروط المؤسسية التي تُحدّد فرص نجاح التبني، يمكن إجمالها في:
 - توفير إطار حوكمي واضح يُحدّد المسؤوليات والصلاحيات في إدارة منظومة التعلم الآلي، ويرسم حدود اتخاذ القرار البشري والآلي.
 - بناء قدرات بشرية متخصصة في علم البيانات وهندسة التعلم الآلي والأمن السيبراني، إذ تظل الخوارزميات عاجزة دون كوادر مؤهلة قادرة على تطويرها وإدارتها.
 - تطوير سياسات أخلاقية تضبط استخدام الخوارزميات وتضمن الشفافية والعدالة وحماية الخصوصية.
 - تهيئة الثقافة التنظيمية لاستيعاب التحول الرقمي، بحيث لا تُقاوم التقنية بوصفها تهديداً للوظائف التقليدية، بل تُستثمر بوصفها أداة لتمكين الكوادر البشرية.
- ويؤكد Chowdhury (2025) من ضرورة توافر إطار تنظيمي رقابي يتولّى الإشراف على تطبيقات التعلم الآلي في الأنظمة المؤسسية الحساسة، خاصة تلك المرتبطة بالأمن السيبراني، إذ إن طبيعة هذه التطبيقات تستلزم توازناً دقيقاً بين السرعة التشغيلية والدقة وقابلية التفسير، وهو توازن لا يتحقق إلا في ظل إطار رقابي محكم يُحدّد المعايير المقبولة للأداء والاعتمادية، كما يُشير إلى أن هذا الإطار ينبغي أن يستوعب متطلبات الامتثال للتشريعات المحلية والدولية المتعلقة بحماية البيانات وحقوق الأفراد، وأن يُتيح في الوقت ذاته مرونة كافية لمواكبة التطور المتسارع في هذه التقنية.

ثامناً: التحديات والقيود التي تواجه تطبيق التعلم الآلي

تواجه تطبيقات التعلم الآلي في البيئات الرقمية الحيوية مجموعة من التحديات والقيود التي تحدّ من فاعلية توظيفها وتؤثر على مخرجاتها. وتنقسم هذه التحديات إلى ثلاث فئات رئيسية: تحديات تقنية مرتبطة ببنية الخوارزميات وطبيعة البيانات، وتحديات معرفية تتصل بقابلية التفسير والثقة في المخرجات، وتحديات تنظيمية وأخلاقية ترتبط بالحوكمة والمساءلة.

أولاً: التحديات التقنية المرتبطة بالنماذج والبيانات

تتصدّر التحديات التقنية قائمة العقبات التي تواجه تطبيق التعلم الآلي. ويرصد (Ijiga et al 2024) في هذا السياق ظاهرة التعلم الآلي العدائي (Adversarial Machine Learning)، التي تتمثل في قابلية النماذج للخداع عبر تعديلات دقيقة على البيانات المدخلة قد لا تُلحظ بصرياً، لكنها تؤدي إلى انحراف جوهري في المخرجات، ويضيف الباحثون أن هذه الظاهرة تشمل عدة أشكال، منها: تسميم بيانات التدريب عبر حقن عينات خبيثة تُفسد قدرة النموذج التنبؤية، واستخراج النماذج عبر استجوابها بأسئلة محسوبة لإعادة بنائها، وهجمات التهرّب التي تتجاوز أنظمة الكشف عبر تصميم تهديدات لا تتطابق مع الأنماط المُدرّب عليها.

ويتقاطع هذا الطرح مع ما يرصده (Bitton et al 2023) من تحديات تطرأ على نماذج التعلم الآلي بعد نشرها في البيئة التشغيلية، وفي مقدمتها ظاهرة الانحراف المفاهيمي (Concept Drift) التي تنشأ من تغيّر طبيعة البيانات بمرور الوقت، فيتدنّى أداء النموذج تدريجياً، ويُشير الباحثون أيضاً إلى صعوبة المعايرة الدورية للنماذج المنشورة في بيئات الإنتاج، نظراً لما تستلزمه من توقف مؤقت قد يُؤثر على استمرارية الخدمة في القطاعات التي تتطلب تشغيلاً متواصلاً كأنظمة النقل الذكية.

ثانياً: التحديات المعرفية المتصلة بقابلية التفسير والثقة

تُمثّل قابلية التفسير (Interpretability) أحد أبرز التحديات المعرفية في تطبيقات التعلم الآلي، وتُعرف هذه الإشكالية بظاهرة "الصندوق الأسود" (Black Box) وتُشير العدوان (٢٠٢٢) إلى أن هذه الظاهرة تُصعّب على المسؤولين فهم آلية وصول النموذج إلى قراراته، مما يُولّد فجوة بين دقّة النموذج وقابلية الاعتماد عليه في القرارات الحساسة. ويرتبط بهذا التحدي إشكالية الانحياز الخوارزمي (Algorithmic Bias) الذي ينشأ حين تعكس بيانات التدريب تحيّزات تاريخية، فنُعيد الخوارزمية إنتاجها في قراراتها.

ويُضيف (Saba et al (2024) بُعداً مكملاً يتعلق بمحدودية البيانات التدريبية الموثوقة في القطاعات الأمنية، إذ تصعب مشاركة بيانات الحوادث السيبرانية الفعلية بين المؤسسات لاعتبارات أمنية وقانونية، مما يُقلص حجم البيانات المتاحة لتدريب النماذج. ويترتب على ذلك أن النماذج المُدرّبة على بيانات محدودة قد تعجز عن التعميم على التهديدات الجديدة، وهو ما يُمثّل قيداً جوهرياً في بيئة التهديد السيبراني المتطوّر.

ثالثاً: التحديات التنظيمية والأخلاقية

تتجاوز التحديات حدودها التقنية لتطال الأبعاد التنظيمية والأخلاقية. ويتناول (Chowdhury (2025 هذا الجانب بالإشارة إلى التوتر القائم بين سرعة تطور تقنيات التعلم الآلي وبطء استجابة الأطر التشريعية، مما يُوجد فراغاً تنظيمياً يُصعّب على المؤسسات تحديد حدود المسؤولية القانونية عند وقوع أخطاء خوارزمية. ويرتبط بذلك تحدي المساءلة (Accountability)، إذ يصعب تحديد الجهة المسؤولة عن قرار خوارزمي أدّى إلى ضرر؛ هل هي الجهة المُصمّمة للنموذج، أم المُشغِّل له، أم المسؤولة عن البيانات التدريبية؟ كما يُضاف إلى ذلك التحدي المتعلق بالتكلفة المرتفعة لتطوير وصيانة منظومات التعلم الآلي، الذي تُبرزه برارمة (٢٠٢٤) ضمن العقبات التي تحول دون التبني الواسع لهذه التقنية، خاصة في المؤسسات التي تقتقر إلى الموارد المالية والكوادر المتخصصة الكافية. ويتعمّق هذا التحدي في القطاعات الحيوية كالنقل الذكي، حيث تستلزم البنية المعقدة استثمارات ضخمة في البنية التحتية والكوادر البشرية.

جدول رقم (٢): ملخص التحديات الرئيسية لتطبيق التعلم الآلي

فئة التحدي	أبرز مظاهره	انعكاسه على أنظمة النقل الذكي
تقنية	الهجمات العدائية، تسميم البيانات، الانحراف المفاهيمي	تهديد موثوقية الكشف عن الهجمات في الزمن الحقيقي
معرفية	الصندوق الأسود، الانحياز الخوارزمي، محدودية البيانات	إضعاف الثقة في القرارات الأمنية الآلية
تنظيمية وأخلاقية	الفراغ التشريعي، إشكالية المساءلة، التكلفة المرتفعة	عرقلة التبني المؤسسي والوطني الواسع

المبحث الثاني : تقييم مخاطر الأمن السيبراني كمدخل استراتيجي لحماية أنظمة النقل الذكية

تمهيد

يتناول هذا المبحث المتغير التابع في الدراسة (تقييم مخاطر الأمن السيبراني) ضمن السياق التطبيقي الذي تتبناه الدراسة (أنظمة النقل الذكية)، ويعرض المبحث الإطار المفاهيمي للأمن السيبراني وطبيعة المخاطر المرتبطة به، ويتناول مكونات أنظمة النقل الذكية ونقاط الضعف فيها، ويُسلط الضوء على واقع هذا القطاع في المملكة العربية السعودية في إطار رؤية ٢٠٣٠، قبل أن يُفصل الأبعاد الأربعة لتقييم المخاطر السيبرانية المعتمدة في الدراسة وهي: الكشف، والتقييم، والاستجابة، والتعافي.

أولاً: المفهوم المعاصر للأمن السيبراني وتطوره

تعددت التعريفات التي قدّمها الباحثون لمفهوم الأمن السيبراني، وتباينت زوايا تناولهم تبعاً للسياق التطبيقي الذي انطلقوا منه، غير أن هذه التعريفات تتقاطع في إبراز جوهر مشترك يتمثل في حماية الأصول الرقمية والمعلوماتية من التهديدات والاختراقات، ويُعرّف (Dawodu et al. (2023) الأمن السيبراني بأنه منظومة متكاملة من الممارسات والتقنيات والسياسات الموجهة لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تستهدف الوصول غير المشروع إلى المعلومات الحساسة، أو تعديلها، أو تدميرها، أو ابتزاز الأموال من المستخدمين، أو تعطيل العمليات التشغيلية المعتادة.

ويطرح (Ganesan et al. (2022) تعريفاً يصف الأمن السيبراني بأنه الحالة التي تكون فيها الأصول المعلوماتية محمية من التهديدات السيبرانية عبر تطبيق ضوابط متعددة المستويات تشمل البعد التقني والبعد التنظيمي والبعد البشري، بحيث تتكامل هذه الأبعاد في تكوين منظومة دفاعية شاملة.

وتذهب العدوان (٢٠٢٢) إلى أن الأمن السيبراني يُمثّل حقلاً معرفياً متعدد التخصصات، يجمع بين علم الحاسب والإدارة والقانون والسلوك التنظيمي، ويسعى إلى ضمان السرية والسلامة والتوافر للأصول المعلوماتية بوصفها الركائز الجوهرية التي تقوم عليها فلسفة الأمن السيبراني.

ويُكمل (Wang et al. (2021) هذه التعريفات بطرح يركّز على البعد الديناميكي للمفهوم، إذ يُشير إلى أن الأمن السيبراني لم يعد يُمكن تعريفه بوصفه حالة ثابتة يمكن الوصول إليها، بل هو عملية مستمرة من التكيف والاستجابة للتهديدات المتطورة.

ومن وجهة نظر الباحث، يمكن تقديم تعريف تكاملي للأمن السيبراني يستوعب الأبعاد الثلاثة، فيُعرّف بأنه: "منظومة متكاملة من السياسات والتقنيات والممارسات الإدارية والبشرية، تعمل في تفاعل مستمر للحفاظ على سرية الأصول المعلوماتية وسلامتها وتوافرها، وتُمكن المنظمات والبنى التحتية الحيوية ومنها أنظمة النقل الذكية من التكيف مع التهديدات السيبرانية المتطورة، والاستجابة لها بصورة استباقية، والتعافي من آثارها بأقل قدر ممكن من الخسائر التشغيلية."

أما من حيث التطور التاريخي، فقد مرّ مفهوم الأمن السيبراني بمراحل متعاقبة عكست تطور التهديدات والاستجابات الدفاعية. ففي مراحله الأولى، اقتصر على حماية الأنظمة الحاسوبية الفردية من الفيروسات والبرمجيات الخبيثة، ثم توسّع مع انتشار الشبكات ليشمل حماية البنية الشبكية، قبل أن يتحوّل في طوره الراهن إلى منظومة شاملة تستوعب التهديدات الموجهة ضد البنى التحتية الحيوية كالنقل الذكي والمدن الذكية وأنظمة الطاقة.

وقد رافق هذا التطور بروز مفاهيم مساندة كالمرونة السيبرانية (Cyber Resilience) والاستخبارات السيبرانية (Cyber Intelligence) والدفاع الاستباقي (Proactive Defense)، وهي مفاهيم تعكس النضج المعرفي لهذا الحقل وتجاوزه للأطر التقليدية المحدودة.

ثانياً: طبيعة المخاطر السيبرانية وتصنيفاتها

تتعدد المخاطر السيبرانية وتتنوع تصنيفاتها تبعاً لطبيعتها ومصادرها وآثارها، وتُمثّل هذه المخاطر مجموع التهديدات المحتملة التي قد تستهدف الأصول المعلوماتية والرقمية للمؤسسات، ويُحدّد Sahinoglu (2024) المخاطر السيبرانية بأنها احتمالية وقوع حدث سلبي يؤدي إلى الإضرار بالأصول المعلوماتية، مضروبة في حجم الأثر المترتب على وقوع هذا الحدث، وهي معادلة تُجسّد البُعد الاحتمالي للمخاطر وارتباطها بمتغيرين أساسيين هما الاحتمالية والأثر.

و يطرح (Stelkens-Kobsch et al. (2024 تصنيفاً ثلاثياً للمخاطر السيبرانية يأخذ في الاعتبار طبيعة كل خطر ومستوى تأثيره، يتمثّل في:

- **المخاطر التقنية:** وتشمل تلك المرتبطة بالبنية التقنية كثغرات البرمجيات، وضعف بروتوكولات التشفير، وأخطاء التكوين، وقدم الأنظمة، وقصور آليات المصادقة. وتتميّز هذه المخاطر بقابليتها للقياس النسبي وإمكانية معالجتها عبر حلول تقنية محدّدة.

- **المخاطر التشغيلية:** وتتعلق بسير العمليات اليومية وممارسات المستخدمين، كأخطاء العاملين، وضعف الالتزام بسياسات الأمن، وقصور إجراءات إدارة الحوادث، وثغرات سلاسل التوريد التقنية. وتتميز هذه المخاطر بصعوبة ضبطها كلياً نظراً لارتباطها بالعنصر البشري.

- **المخاطر الاستراتيجية:** وتمتد لتشمل التهديدات ذات الأثر طويل المدى على المنظمة، كالهجمات الموجهة من جهات متقدمة (APT) ، والتهديدات الجيوسياسية، والمخاطر المرتبطة بفقدان الثقة المؤسسية وتدهور السمعة. وتتميز هذه المخاطر بكونها متعددة الأبعاد وعابرة للتخصصات.

ويُكمل هذا الطرح ما تناوله Wang et al. (2021) من تصنيف للمخاطر السيبرانية وفق نموذج شجرة الهجوم والدفاع (Attack-Defense Tree) ، الذي يُقسّم المخاطر بحسب مصادرها إلى مخاطر داخلية تنشأ من داخل المنظمة (كأخطاء الموظفين أو هجمات المعلنين)، ومخاطر خارجية تنشأ من جهات خارج المنظمة (كالقرصنة والمنظمات الإجرامية الإلكترونية والدول المعادية). وتختلف آليات التعامل مع كل فئة باختلاف منشأها وطبيعتها.

ومن منظور (Kalinin et al. (2021) ، تتوزع المخاطر السيبرانية في البنى التحتية للمدن الذكية بحسب الأثر إلى أربع فئات: مخاطر تستهدف توافر الخدمات (Availability) عبر تعطيل الأنظمة وحرمان المستخدمين منها، ومخاطر تستهدف سرية البيانات (Confidentiality) عبر الوصول غير المشروع للمعلومات الحساسة، ومخاطر تستهدف سلامة البيانات (Integrity) عبر التلاعب بالمعلومات وتعديلها، ومخاطر تستهدف عدم الإنكار (Non-Repudiation) عبر التشكيك في صحة المعاملات الرقمية.

ولتيسير استيعاب هذه التصنيفات وعلاقاتها المتداخلة، يمكن عرضها على النحو التالي:

جدول رقم (٣): التصنيفات الرئيسية للمخاطر السيبرانية في البنى التحتية الحيوية

معايير التصنيف		أبرز ملامحها
طبيعة المخاطر	تقنية – تشغيلية – استراتيجية	تتدرج من الملموس التقني إلى الأثر بعيد المدى
المصدر	داخلية – خارجية	تختلف آليات الكشف والمواجهة باختلاف المنشأ

الأثر المستهدف	التوافر - السرية - السلامة - عدم الإنكار	تستهدف ركائز منظومة الحماية المعلوماتية
الفاعل	فردى - منظم - موجّه من جهات متقدمة	يتفاوت مستوى التعقيد والدوافع

ثالثاً: مصادر التهديدات السيبرانية في أنظمة النقل الذكية

تتنوع مصادر التهديدات السيبرانية التي تستهدف أنظمة النقل الذكية، ويعكس هذا التنوع الطبيعة المعقدة لهذه الأنظمة التي تجمع بين أكثر من عنصر بنيوي (المركبات، البنية التحتية، الشبكات، المنصات السحابية، المستخدمون). ويُحدّد Khan et al. (2024) المصادر الرئيسية للتهديدات السيبرانية في قطاع النقل بأنها تنقسم إلى ثلاث فئات :

الجهات الفاعلة الخارجية التي تشمل الجماعات الإجرامية الإلكترونية والقرصنة الموجهين من دول، والجهات الفاعلة الداخلية التي تشمل الموظفين والمتعاقدين الذين يمتلكون صلاحيات الوصول إلى الأنظمة.

التهديدات العرضية التي تنشأ من الأخطاء البشرية أو فشل الأنظمة.

ويُكمل هذا الطرح Sabaliauskaite et al. (2018) في دراستهم لأنظمة النقل الذكية التعاونية (Cooperative Intelligent Transport Systems)، حيث يُبرزون أن مصادر التهديدات في هذه الأنظمة تنقسم إلى مصادر تستهدف قنوات الاتصال بين المركبات والبنية التحتية (V2I) أو بين المركبات بعضها بعضاً (V2V) ، ومصادر تستهدف الوحدات المُدمجة داخل المركبات، ومصادر تستهدف المنصات المركزية التي تُدير المنظومة. ويُؤكد الباحثون أن كل مصدر من هذه المصادر يتطلب استراتيجية حماية متخصصة تأخذ في الاعتبار طبيعته الفنية وموقعه في الهيكل العام للمنظومة.

ومن زاوية مكمّلة، يطرح Vogt et al. (2021) رؤية تركز على المصادر الخارجية للتهديدات في أنظمة النقل الذكية، مُشيرين إلى أن هذه المصادر تتوزع على مستويات متعددة:

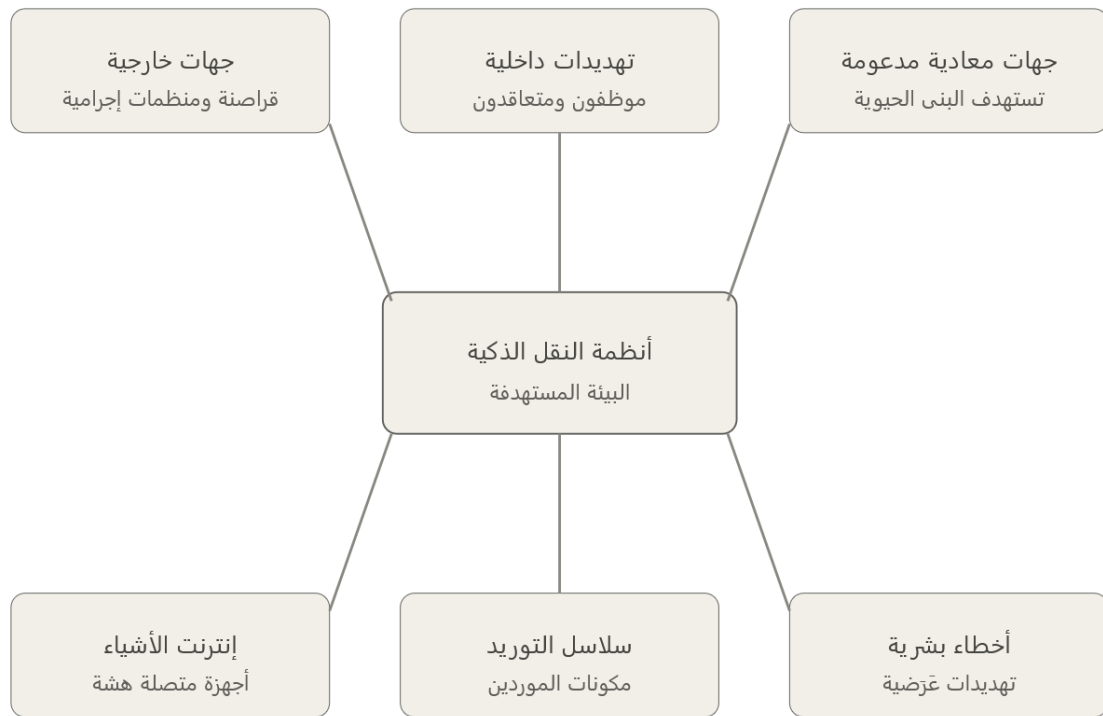
- قرصنة فرادى يسعون إلى إثبات قدراتهم التقنية أو إلى تحقيق منافع مالية محدودة.

- منظمات إجرامية إلكترونية تستهدف الأنظمة بقصد الابتزاز عبر برامج الفدية أو سرقة بيانات المستخدمين.

- جهات تجسس صناعي تسعى إلى الحصول على المعرفة التقنية والتجارية للشركات العاملة في القطاع.

- جهات معادية مدعومة من دول تستهدف البنى التحتية الحيوية بهدف تعطيلها في إطار صراعات سياسية أو اقتصادية.

ويُضيف (Galego & Pascoal (2021) بُعداً جوهرياً يتعلق بمصادر التهديدات في سياق المدن الذكية، حيث يُبرز أن إنترنت الأشياء يُمثل في حد ذاته مصدراً متنامياً للتهديدات نظراً لكثرة الأجهزة المتصلة وتنوع مورديها وضعف معايير الحماية في بعضها.



شكل (2): مصادر التهديدات السيبرانية في أنظمة النقل الذكية - من إعداد الباحث

رابعاً: النماذج الدولية للأمن السيبراني وحدود قابليتها للتطبيق في أنظمة النقل الذكية

تُشكّل الأطر المرجعية الدولية للأمن السيبراني المعمار المعرفي الذي انبنت عليه الممارسة العالمية في هذا الحقل خلال العقدين الأخيرين، إذ نشأت هذه الأطر بوصفها استجابة مؤسسية منظّمة لظاهرة تصاعد

التحديات السيبرانية وتنامي الحاجة إلى لغة مشتركة تُيسر التواصل بين المؤسسات ومقدمي الخدمات والجهات الرقابية. ويُشير (Dawodu et al. (2023 إلى أن هذه الأطر تتقاسم هدفاً استراتيجياً واحداً يتمثل في توفير مرجعية معيارية قابلة للقياس والمقارنة تُتيح تقييم النضج السيبراني للمؤسسات وفق معايير موحدة، غير أن هذه الأطر على أهميتها المرجعية طُورت في سياقات مؤسسية عامة، ولم تُصمَّم أصلاً لاستيعاب الخصوصيات البنيوية العميقة لأنظمة النقل الذكية التي تتسم بتشابك المنظومات السيبرانية-الفيزيائية (Cyber-Physical Systems) وتدفق البيانات في الزمن الحقيقي وتعدّد نقاط الاتصال بين المركبات والبنية التحتية والمستخدمين، فضلاً عن كونها لم تستوعب السياقات التنظيمية الوطنية المتعددة، ممّا يُبرز مواطن الحاجة إلى تطويرها وتوطينها.

ويتناول هذا القسم بالتحليل النقدي ثلاثة نماذج مرجعية دولية تُمثل العمود الفقري للممارسة السيبرانية المعاصرة، مع رصد نقاط قوتها وحدود قابليتها للتطبيق في منظومة النقل الذكي، بوصف ذلك مدخلاً منهجياً لتأصيل الحاجة إلى الإطار المقترح في الدراسة الحالية.

١. إطار NIST للأمن السيبراني (NIST Cybersecurity Framework)

١.١ النشأة والتطور

طوّر المعهد الوطني الأمريكي للمعايير والتقنية (National Institute of Standards and Technology) هذا الإطار في نسخته الأولى عام ٢٠١٤م، استجابةً للأمر التنفيذي رقم ١٣٦٣٦ الصادر عام ٢٠١٣م، الذي دعا إلى تطوير إطار طوعي لتعزيز الأمن السيبراني للبنى التحتية الحيوية. وقد صدرت نسخته الثانية (NIST CSF 2.0) في فبراير ٢٠٢٤م، متضمّنةً توسّعاً في نطاق التطبيق ليشمل المؤسسات الصغيرة والمتوسطة، مع إضافة وظيفة سادسة تتعلق بالحوكمة (Govern). ويُبرز (Stelkens-Kobsch et al. (2024 أن هذا التطور يعكس النضج المعرفي لهذا الإطار الذي انتقل من كونه أداة استرشادية للقطاع الأمريكي إلى مرجعية عالمية تعتمد عليها أكثر من ثلاثين دولة بصور متفاوتة.

١.٢ البنية الوظيفية

يقوم الإطار في نسخته المرجعية على خمس وظائف رئيسية متكاملة، يستعرضها Stelkens-Kobsch et al. (2024) على النحو التالي:

• **التعرف: (Identify)** ويشمل فهم البيئة المؤسسية، وتحديد الأصول والأنظمة والبيانات الحيوية، وحصر التبعيات والوظائف الحرجة، وتقييم المخاطر على المستوى المؤسسي.

• **الحماية: (Protect)** ويتضمن تطبيق الضوابط الوقائية لضمان استمرارية الخدمات الحرجة، بما في ذلك ضوابط التحكم في الوصول، والتوعية والتدريب، وأمن البيانات، وحماية التقنية.

• **الكشف: (Detect)** ويعنى بتطوير أنشطة الكشف المبكر عن الحوادث السيبرانية عبر المراقبة المستمرة وتحليل الأحداث.

• **الاستجابة: (Respond)** ويشمل إجراءات احتواء الحوادث وتحليلها والتخفيف من آثارها والتواصل بشأنها.

• **التعافي: (Recover)** ويتضمن خطط استعادة الخدمات والقدرات بعد وقوع الحوادث، مع دمج الدروس المستفادة في التحسين المستمر.

ويلاحظ أن هذه الوظائف الخمس تتقاطع بنوياً مع الأبعاد الأربعة لتقييم المخاطر المعتمدة في الدراسة الحالية (الكشف، والتقييم، والاستجابة، والتعافي)، مما يؤقر لهذا الإطار قيمة مرجعية في تأطير المتغير التابع للدراسة.

يبرز (Şahinoglu 2024) أن هذا الإطار يتميز بثلاث خصائص جوهرية تُفسر انتشاره الواسع: أولاً المرونة التكيفية التي تُتيح تطبيقه على مؤسسات متباينة الأحجام والقطاعات، وثانيها الشمولية المفاهيمية التي تستوعب أبعاد الأمن السيبراني كافة في هيكل موحد، وثالثها قابليته للتكامل مع النماذج المرجعية الأخرى بوصفه إطاراً شاملاً لا يتعارض مع المعايير التخصصية. ويُضيف Kalinin et al. (2021) بعداً تكملياً يتمثل في أن هذا الإطار يؤقر لغة مشتركة تُيسر التواصل بين الجهات التقنية والإدارية والرقابية، وهو ما يُقلل من فجوة الفهم التي كثيراً ما تُعرق تنفيذ استراتيجيات الأمن السيبراني في البنى التحتية الحيوية.

١.٣ المحدوديات في سياق النقل الذكي

على الرغم من هذه الخصائص، يرصد الباحثون جملة من المحدوديات التي تكتسب حدة خاصة في بيئة النقل الذكي:

يلاحظ (Leungbootnak & Heaslip (2025) في مراجعتهم التحليلية لأساليب تقييم المخاطر السيبرانية في شبكات الطرق وأنظمة النقل الذكية — أن هذا الإطار يُقدّم توصيفاً وظيفياً عاماً لا يتضمن آليات كمية للتنفيذ ولا خوارزميات محدّدة للكشف عن التهديدات، ممّا يجعله يعمل بمنطق "الصندوق النظري" الذي يستلزم منظومة تنفيذية موازية لتحويله إلى نظام عملي، ويتّسق هذا الطرح مع ما يُبرزه Chowdhury (2025) من أن الأطر المفاهيمية العامة تقتصر إلى **البُعد الاستدلالي الآلي** الذي يُتيح للنظام اتخاذ قرارات في الزمن الحقيقي.

و يرصد (Sabaliauskaite et al. (2018 أن هذا الإطار طُوّر أصلاً لبيئات تقنية المعلومات التقليدية، دون أن يستوعب الطبيعة السيبرانية-الفيزيائية لأنظمة النقل الذكية، إذ لا يُميّز في وظائفه الخمس بين التهديدات ذات الأثر الرقمي المحض والتهديدات التي تمتدّ آثارها إلى السلامة الفيزيائية للأشخاص والممتلكات، وهو تمييز جوهري في منظومة النقل التي قد يترتب على اختراقها فقدان أرواح لا مجرد فقدان بيانات.

ويُضاف إلى ذلك ما يرصده (Vogt et al. (2021 في دراستهم المخصّصة لإدارة مخاطر أمن المعلومات في أنظمة النقل الذكية، من أن الإطار في نسخته الحالية لا يستوعب **التعقيد الطبقي** لمنظومة النقل الذكي التي تتوزّع بين مستوى المركبات، ومستوى البنية التحتية، ومستوى قنوات الاتصال، ومستوى المنصات السحابية، إذ يُعامل هذه المستويات معاملة موحّدة رغم اختلاف طبيعة تهديداتها وآليات حمايتها.

ويرصد (Khan et al. (2024 في تحليلهم الشامل لتحديات الأمن السيبراني في صناعة النقل بُعداً تنظيمياً مكملًا، مفاده أن الإطار يُقدّم توصيات دون آليات إلزامية لضمان تطبيقها، ممّا يُضعف قابليته للتطبيق في القطاعات التي تتطلّب مستوى عالياً من الامتثال كقطاع النقل الحيوي.

٢. معيار ISO/IEC 27001 ومنظومة المعايير المرافقة

٢.١. النشأة والتطور

يُمثّل معيار ISO/IEC 27001 أحد أبرز المعايير الدولية لإدارة أمن المعلومات، وقد نشأ من تطور معيار BS 7799 البريطاني الذي طُوّر في تسعينيات القرن الماضي، قبل أن يُعتمد دولياً بمنظمة المعايير الدولية (ISO) والمفوضية الدولية للكهرباء (IEC) عام ٢٠٠٥م، ثم شهد تحديثات لاحقة، أحدثها في أكتوبر ٢٠٢٢م الذي أعاد هيكلة الضوابط في أربع فئات (تنظيمية، وبشرية، ومادية، وتكنولوجية).

٢.٢ البنية والمكونات

يرتكز المعيار على بناء نظام إدارة أمن المعلومات (Information Security Management System – ISMS) بوصفه منظومة متكاملة تشمل السياسات والإجراءات والضوابط والوثائق. وتُشير

Ganesan et al. (2022) إلى أنه يقوم على دورة منهجية معروفة بدورة PDCA (التخطيط، والتنفيذ، والمراجعة، والتحسين) تضمن التطوير المستمر لمنظومة الأمن السيبراني وفق نموذج ديناميكي يتسق مع تطور التهديدات.

وترتبط بهذا المعيار منظومة معايير مكملة تُشكّل عائلة ISO/IEC 27000 ، منها ISO/IEC 27005 : المخصص لإدارة مخاطر أمن المعلومات، و ISO/IEC 27032 المتعلق بإرشادات الأمن السيبراني، و ISO/IEC 27701 الخاص بإدارة معلومات الخصوصية. ويُبرز Dawodu et al. (2023) في دراستهم لتقييم المخاطر السيبرانية في القطاع البنكي أن هذه المنظومة الشاملة تُوفّر معياراً معيارياً متعدد الطبقات يُمكن المؤسسات من بناء منظومة حماية شاملة، شريطة توافر الموارد التنظيمية والبشرية اللازمة لتنفيذها.

ويُقدّم هذا المعيار بحسب Wang et al. (2021) ثلاث ميزات جوهرية: أولاً الاعتراف الدولي الذي يُوفّر للمؤسسات المُعتمدة ميزة تنافسية في التعاملات الدولية، وثانيها الطابع الحوكمي المنظم الذي يربط الأمن السيبراني بمنظومة الحوكمة المؤسسية، وثالثها القابلية للتدقيق التي تُتيح التحقق من الالتزام عبر جهات اعتماد مستقلة. وتُضيف Ganesan et al. (2022) بُعداً تنظيمياً مكملاً يتمثل في أن هذا المعيار يلزم المؤسسات بتوثيق تقييم المخاطر بصورة منهجية، ممّا يُوفّر أساساً موضوعياً لصنع القرار السيبراني.

٢.٤ المحدوديات في سياق النقل الذكي

يُؤخذ على هذا المعيار في سياق النقل الذكي ثلاث محدوديات جوهرية:

المحدودية الأولى: هيمنة البُعد الإداري-الحوكمي على حساب البُعد التقني-التشغيلي. فالمعيار يتعامل مع أمن المعلومات باعتباره منظومة سياسات وإجراءات وضوابط تنظيمية، دون أن يوفّر آليات فنية لمعالجة تهديدات ناقل CAN داخل المركبات، أو هجمات انتحال V2V بين المركبات، أو التلاعب ببيانات الاستشعار في الزمن الحقيقي، وهي الفئات التهديدية الغالبة على منظومة النقل الذكي كما يرصدها

Sabalaiuskaite et al. (2018) و He et al. (2020).

المحدودية الثانية: عدم استيعاب الطبيعة السيبرانية-الفيزيائية. يُشير (Vogt et al. 2021) إلى أن المعيار طُوّر أصلاً لبيئات معالجة المعلومات، ولا يستوعب البنية المزدوجة لأنظمة النقل الذكية التي تجمع بين المكونات الرقمية والمكونات الفيزيائية، مما يترك فجوة بين معايير الحماية الرقمية ومعايير السلامة الفيزيائية.

المحدودية الثالثة: البطء النسبي في مواكبة التطور التقني. يُلاحظ (Chowdhury 2025) أن دورات مراجعة المعيار تمتدّ لسنوات، بينما تتطوّر التهديدات السيبرانية وتقنيات الذكاء الاصطناعي في دورات شهرية، مما يُوجد فجوة زمنية بين ما ينصّ عليه المعيار وما تفرضه الواقعة التقنية. ويُعزّز هذا الملاحظة ما تُبرزه العدوان (٢٠٢٢) من أن الأطر التنظيمية التقليدية تُواجه صعوبة في مواكبة التسارع المعرفي في حقل الأمن السيبراني القائم على الذكاء الاصطناعي.

ويُضاف إلى ذلك أن معيار — ISO 27001 رغم إشارته إلى تقييم المخاطر — يُحيل هذه المهمة إلى معيار ISO 27005 دون أن يتضمن آليات قياس كمّي دقيقة، وهو ما يرصده (Şahinoglu 2024) بوصفه ثغرة منهجية تستلزم استكمالها بأدوات كمّية متقدمة كخوارزميات التعلم الآلي.

٣. نموذج MITRE ATT&CK والمصفوفات المتخصصة

٣.١. النشأة والتطور

طوّرت مؤسسة — MITRE وهي منظمة أمريكية غير ربحية تعمل بالشراكة مع الحكومة الفيدرالية — هذا النموذج في عام ٢٠١٣م، بوصفه قاعدة معرفية موثقة لتكتيكات وتقنيات وإجراءات المهاجمين السيبرانيين (Tactics, Techniques, and Procedures – TTPs) واسم النموذج اختصاراً لـ "Adversarial Tactics, Techniques, and Common Knowledge"، وقد شهد تطوراً مطّرداً منذ إنطلاقه ليشمل مصفوفات متخصصة لبيئات تقنية متعدّدة.

٣.٢. البنية والمصفوفات المتخصصة

يقوم النموذج على تنظيم سلوك المهاجمين في مصفوفات (Matrices) يُمثّل كل عمود منها تكتيكاً — (Tactic) أي هدفاً استراتيجياً للمهاجم كالوصول الأولي أو الحركة الجانبية أو الاستخراج — وتُمثّل الصفوف داخل كل عمود تقنيات (Techniques) محدّدة يستخدمها المهاجمون لتحقيق ذلك التكتيك. وقد تطوّرت المصفوفات لتشمل:

• MITRE ATT&CK for Enterprise للبيئات تقنية المعلومات المؤسسية.

• MITRE ATT&CK for Mobile للأنظمة المحمولة.

• MITRE ATT&CK for ICS للأنظمة التحكم الصناعي، وهي الأقرب إلى بيئة النقل الذكي.

• MITRE ATT&CK for Cloud للبيئات السحابية.

يتميز هذا النموذج بحسب (Ijiga et al. (2024) بكونه قائماً على رصد سلوك المهاجم الفعلي بدلاً من الاعتماد على الافتراضات النظرية، مما يكسبه واقعية عالية. ويُضيف (Nikoloudakis et al. (2021 أن هذا النموذج يُوفّر لغة موحّدة لوصف الهجمات تُيسّر تبادل المعلومات الاستخباراتية السيبرانية بين المؤسسات والدول، فضلاً عن أنه يُتيح للمؤسسات تقييم جاهزيتها الدفاعية عبر مقارنة قدراتها بالتقنيات الهجومية الموثّقة، فيما يُعرف بتمارين "الفريق الأحمر مقابل الفريق الأزرق (Red Team vs. Blue Team)".

٣.٤ المحدوديات في سياق النقل الذكي

يُلاحظ (Ijiga et al. (2024) أن النموذج رغم قوّته التصنيفية يظلّ وصفيّاً-تصنيفياً أساساً، إذ يُقدّم موسوعة للأنماط الهجومية دون أن يتضمّن آلية خوارزمية للاكتشاف أو التنبؤ، فيصلح أداة معرفية لا أداة تنفيذية.

ويرصد (Kumar et al. (2021 في إطارهم المخصّص للنقل البحري الذكي فجوةً بنوعية أعمق، مفادها أن نسخة MITRE ATT&CK for ICS رغم قربها من بيئات النقل — طُوّرت أصلاً للأنظمة التحكم الصناعي الثابتة (كأنظمة الطاقة والمياه)، ولا تستوعب الطبيعة المتنقّلة للأنظمة النقل الذكية التي تتحرّك فيها العُقد عبر نطاقات جغرافية وشبكية متعدّدة، ولا البروتوكولات المتخصصة للاتصال بين المركبات (V2V, V2I, V2X) القائمة على معايير IEEE 802.11p و ETSI ITS-G5. ويتّسق هذا الطرح مع ما يُبرزه (Khan et al. (2024) من أن الأدبيات لم تُطوّر مصفوفة MITRE ATT&CK متخصصة بأنظمة النقل الذكية، ممّا يترك المؤسسات المُشغّلة لهذه الأنظمة في وضع اضطراري لاستتساخ المصفوفات القائمة مع ما ينطوي عليه ذلك من قصور تغطية.

ويُضيف (Bitton et al. (2023) بُعداً تكملياً يتعلّق بأن النموذج لا يُغطّي التهديدات الموجهة ضد نماذج التعلم الآلي ذاتها، كتسميم بيانات التدريب واستخراج النماذج والهجمات العدائية (Adversarial Attacks)، وهي فئة تهديدية تكتسب حدّة متزايدة في المنظومات الذكية التي تعتمد على خوارزميات التعلم الآلي. وهذا القصور يجعل النموذج غير مؤهل لتغطية بيئة يُوظّف فيها التعلم الآلي بوصفه أداة للحماية، إذ إن الأداة ذاتها تُصبح جزءاً من سطح الهجوم.

خامساً: المنظومة التنظيمية السعودية للأمن السيبراني البنية التشريعية والمؤسسية لتوطين الأطر الدولية

لا يكتمل الإطار النظري للأمن السيبراني في السياق السعودي دون استيعاب المنظومة التنظيمية الوطنية التي تُشكّل الأرضية التشريعية والمؤسسية لأي إطار تقني يُطبّق في المملكة، إذ إن التوطين — كما اتّضح من المُحصّلة النقدية للنماذج الدولية — لا يتحقّق بالترجمة اللغوية أو بالتكييف السطحي، بل يستلزم اندماجاً بنيوياً في المنظومة التنظيمية القائمة. وقد شهدت المملكة العربية السعودية خلال العقد الأخير تطويراً منهجياً متسارعاً لهذه المنظومة، تجلّى في إنشاء ثلاث جهات مرجعية متكاملة يعمل كلّ منها في نطاق اختصاصه، وإصدار حزمة متكاملة من الأنظمة والضوابط تُشكّل في مجموعها الإطار الحاكم لممارسة الأمن السيبراني في البنى التحتية الحيوية، ومنها أنظمة النقل الذكية.

ويستعرض هذا القسم هذه المنظومة بأبعادها الثلاثة: البُعد الفني عبر الهيئة الوطنية للأمن السيبراني وضوابطها، والبُعد القانوني عبر نظام حماية البيانات الشخصية، والبُعد الأخلاقي التقني عبر الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) ومبادئها.

١. الهيئة الوطنية للأمن السيبراني والضوابط الفنية الإلزامية

١.١ النشأة والاختصاص

أنشئت الهيئة الوطنية للأمن السيبراني بموجب الأمر الملكي رقم (٦٨٠١) بتاريخ ١١/٢/١٤٣٩هـ الموافق ٣١/١٠/٢٠١٧م، بوصفها الجهة المرجعية الوطنية للأمن السيبراني في المملكة، وترتبط برئيس مجلس الوزراء مباشرة. وتختص الهيئة وفق نظامها بتعزيز الأمن السيبراني للدولة، وحماية مصالحها الحيوية، وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات والأنشطة الحكومية. وقد جاء إنشاء الهيئة استجابةً لتصاعد التهديدات السيبرانية الموجهة إلى المنطقة، ولا سيّما ما رصده تقرير

(Positive Technologies (2024) حول المشهد السيبراني في الشرق الأوسط الذي أشار إلى أن المملكة تُعدّ من أكثر دول المنطقة استهدافاً من الجهات الفاعلة السيبرانية.

١.٢ الضوابط الأساسية للأمن السيبراني (ECC-1:2018)

أصدرت الهيئة في عام ٢٠١٨م الضوابط الأساسية للأمن السيبراني (Essential Cybersecurity Controls – ECC-1:2018) التي تُمثّل الحد الأدنى الإلزامي لمتطلبات الأمن السيبراني في الجهات الوطنية، وهي ضوابط تُطبّق على الجهات الحكومية وأشباه الحكومية، والقطاع الخاص المُشغّل للبنية التحتية الحساسة، ومنها قطاع النقل. وتتوزّع هذه الضوابط على خمسة مكونات رئيسية تنبثق منها ٣٣ ضابطاً رئيسياً و ١١٤ ضابطاً فرعياً، وتشمل:

- **حوكمة الأمن السيبراني (Cybersecurity Governance)** التي تُعنى بتحديد المسؤوليات والسياسات وإدارة المخاطر السيبرانية على المستوى المؤسسي.
 - **تعزيز الأمن السيبراني (Cybersecurity Defense)** الذي يشمل الضوابط الفنية للحماية والكشف والاستجابة.
 - **صمود الأمن السيبراني (Cybersecurity Resilience)** الذي يُعنى بضمان استمرارية الأعمال والتعافي من الحوادث.
 - **الأمن السيبراني للأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)** الذي يُنظّم العلاقة مع الموردين والخدمات السحابية.
 - **الأمن السيبراني لأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity)** الذي يُعنى بحماية الأنظمة التشغيلية المرتبطة بالبنية التحتية الحيوية.
- ويكتسب المكوّن الأخير أهمية جوهرية في سياق الدراسة الحالية، إذ يتقاطع تقاطعاً بنيوياً مع منظومة النقل الذكي التي تُصنّف أنظمتها التشغيلية ضمن نطاق أنظمة التحكم الصناعي الموسّعة، وهو ما يُشير إليه Sabaliauskaite et al. (2018) في تحليلهم للأمن السيبراني في أنظمة النقل التعاونية بوصفها بيئة سيبرانية-فيزيائية تستلزم ضوابط مماثلة لضوابط أنظمة التحكم الصناعي.

١.٣ ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019)

أصدرت الهيئة في عام ٢٠١٩م ضوابط الأمن السيبراني للأنظمة الحساسة (Critical Systems Cybersecurity Controls) التي تُشكّل مستوى متقدماً من الضوابط الأساسية، وتُطبّق على الأنظمة المُصنّفة "حساسة" وفق معايير الهيئة، والتي يترتّب على اختراقها أثر جوهري على الأمن الوطني أو الاقتصاد أو الخدمات الأساسية. ويُصنّف كثير من أنظمة النقل الذكي — لا سيّما أنظمة التحكم المروري في المدن الكبرى وأنظمة إدارة الحركة الجوية والبحرية — ضمن هذه الفئة، ممّا يستلزم امتثال الإطار المقترح لهذا المستوى المُشدّد من الضوابط.

١.٤ الاستراتيجية الوطنية للأمن السيبراني

اعتمدت المملكة الاستراتيجية الوطنية للأمن السيبراني بوصفها الوثيقة المرجعية العليا التي تُحدّد التوجهات الاستراتيجية لتنمية القدرات السيبرانية الوطنية. وتقوم هذه الاستراتيجية على ست ركائز رئيسية: التنظيم والحوكمة، والدفاع، والردع، والبناء، والشراكات، والتعاون الدولي. ويُشير (Ali et al. (2025 في إطارهم الشامل لتقييم المخاطر السيبرانية لسمود البنية التحتية الوطنية الحيوية إلى أن الاستراتيجيات الوطنية للأمن السيبراني تُشكّل الأساس لتطوير أطر تقنية متكاملة، وأن استيعابها في التصميم التقني يُمثّل عاملاً حاسماً لنجاح التطبيق.

٢. نظام حماية البيانات الشخصية (Personal Data Protection Law – PDPL)

٢.١ النشأة والنطاق

صدر نظام حماية البيانات الشخصية بالمرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩هـ الموافق ٢٠٢١/٩/١٦م، وشهد تعديلات جوهريّة بموجب المرسوم الملكي رقم (م/١٤٨) بتاريخ ١٤٤٤/٩/٥هـ، قبل أن يدخل حيّز التنفيذ الكامل في ٢٠٢٣/٩/١٤م بعد فترة انتقالية استمرّت عاماً كاملاً. وتُشرف على تطبيق النظام الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) بوصفها الجهة المختصة بتلقّي البلاغات وإصدار اللوائح التنفيذية والتحقيق في المخالفات.

٢.٢ المبادئ الحاكمة ذات الصلة بالتعلم الآلي

يُنظّم النظام جمع البيانات الشخصية ومعالجتها وتخزينها ونقلها، ويتضمّن مبادئ حاكمة تُلقّي بظلالها المباشرة على تطبيقات التعلم الآلي في أنظمة النقل الذكية التي تُعالج بيانات حركة الأفراد ومواقعهم وأنماط تنقلهم، ومن أبرز هذه المبادئ:

- **مبدأ محدودية الغرض: (Purpose Limitation)** ويقتضي أن تُجمع البيانات لأغراض محدّدة ومشروعة معلنة مسبقاً، ولا يجوز معالجتها لأغراض تتنافى مع الغرض المُعلن. وينعكس هذا المبدأ على تصميم نماذج التعلم الآلي التي تتطلب بيانات كثيرة ومتنوعة، ممّا يستلزم توثيق الغرض من كل معالجة بيانات.
- **مبدأ تقليل البيانات: (Data Minimization)** ويقتضي جمع الحد الأدنى من البيانات اللازمة لتحقيق الغرض، وهو ما قد يتعارض مع الميل الطبيعي لخوارزميات التعلم العميق إلى استهلاك أكبر قدر ممكن من البيانات.
- **مبدأ الإفصاح عن اتخاذ القرارات الآلية:** ويستلزم إخطار أصحاب البيانات عند اتخاذ قرارات تُؤثر عليهم بناءً على معالجة آلية، وهو ما يُطبّق مباشرةً على قرارات الأمن السيبراني التي تتخذها خوارزميات التعلم الآلي.
- **الحق في التفسير:** ويعطي أصحاب البيانات الحق في الاطلاع على منطق المعالجة الآلية والنتائج المتوقعة منها، وهو ما يستلزم توظيف تقنيات الذكاء الاصطناعي القابل للتفسير (Explainable AI).

٢.٣ متطلبات الإبلاغ عن انتهاكات البيانات

يُلزم النظام الجهات المُتحمّكة في البيانات بالإبلاغ عن أي انتهاك للبيانات الشخصية إلى الهيئة المختصة خلال ٧٢ ساعة من علمها به، وإبلاغ أصحاب البيانات المتأثرين متى ما شكّل الانتهاك خطراً على بياناتهم. ويتقاطع هذا المتطلب مباشرةً مع بُعد التعافي في الإطار المقترح، إذ يستلزم تصميم المنظومة بحيث تتضمن آليات إبلاغ آلي فور اكتشاف الانتهاكات.

٢.٤ نقل البيانات خارج المملكة

يتضمّن النظام قيوداً على نقل البيانات الشخصية خارج المملكة، ويستلزم توافر ضمانات مناسبة لحمايتها. ويُلقي هذا الحكم بأثره على تصميم البنية التحتية الحاسوبية للإطار المقترح، إذ يستلزم اعتماد **الحوسبة السحابية السيادية** أو خيارات معالجة محلية، وهو ما يتّسق مع ما يُبرزه (Chowdhury 2025) من أن المنظومات القائمة على الذكاء الاصطناعي في القطاعات الحيوية باتت تتّجه نحو معماريات حوسبة سيادية استجابةً لاعتبارات الأمن الوطني.

٣. الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) ومبادئ أخلاقيات الذكاء الاصطناعي

٣.١ النشأة والاختصاص

أنشئت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) بموجب الأمر الملكي رقم (أ/٤٧١) بتاريخ ١٤٤١/٨/٢٣ هـ، بوصفها الجهة المرجعية للبيانات والذكاء الاصطناعي في المملكة، وترتبط برئيس مجلس الوزراء. وتضطلع الهيئة بمهام متعددة تشمل: صياغة الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي، وإصدار السياسات والمعايير، والإشراف على تطبيق نظام حماية البيانات الشخصية، وتطوير القدرات الوطنية في هذه المجالات.

٣.٢ الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي (NSDAI)

أطلقت سدايا الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي في عام ٢٠٢٠م، وتهدف إلى وضع المملكة في مصاف الدول العشر الأولى عالمياً في مجال الذكاء الاصطناعي بحلول عام ٢٠٣٠م. وتتضمن الاستراتيجية ستة محاور رئيسية: الطموحات، والمهارات، والسياسات والحوكمة، والاستثمار، والبحث والابتكار، والنظم البيئية. ويكتسب المحور الثالث السياسات والحوكمة أهمية خاصة في سياق الدراسة الحالية، إذ يُشكّل الإطار الحاكم لتطبيقات الذكاء الاصطناعي في القطاعات الوطنية.

٣.٣ مبادئ أخلاقيات الذكاء الاصطناعي (الإصدار الثاني، ٢٠٢٣)

أصدرت سدايا في عام ٢٠٢٣م الإصدار الثاني من "مبادئ أخلاقيات الذكاء الاصطناعي" الذي يُحدّد سبعة مبادئ حاکمة تلتزم بها جميع منظومات الذكاء الاصطناعي المُطبّقة في المملكة:

المبدأ الأول: العدالة (Fairness) ويقتضي عدم انطواء المنظومة على تحيّزات ضدّ أفراد أو فئات، وهو ما يستلزم في تصميم نماذج التعلم الآلي معالجة الانحياز الخوارزمي (Algorithmic Bias) الذي تُشير إليه العدوان (٢٠٢٢) بوصفه أحد أبرز التحديات المعرفية لهذه التقنية.

المبدأ الثاني: الخصوصية والأمن (Privacy & Security) ويستلزم حماية بيانات الأفراد وضمان أمن المنظومة ذاتها ضد الاختراق، وهو ما يتقاطع مباشرةً مع موضوع الدراسة الحالية.

المبدأ الثالث: الموثوقية والسلامة (Reliability & Safety) ويقتضي أن تعمل المنظومة بصورة موثوقة، وألا تُشكّل خطراً على السلامة الفيزيائية أو المعنوية للمستخدمين. ويكتسب هذا المبدأ حدة خاصة في أنظمة النقل الذكي التي يترتب على فشلها آثار سلامة مباشرة.

المبدأ الرابع: الشفافية والقابلية للتفسير (Transparency & Explainability) ويُمثّل هذا المبدأ **التحدي المنهجي المحوري** لأي إطار قائم على التعلم الآلي، إذ يُلزم النموذج بأن يكون قادراً على تفسير قراراته للمستخدمين والجهات الرقابية، وهو ما يستلزم توظيف تقنيات الذكاء الاصطناعي القابل للتفسير (XAI) و SHAP و LIME ضمن بنية الإطار المقترح. ويتقاطع هذا المبدأ مع تحدي "الصندوق الأسود" الذي رصدته العدوان (٢٠٢٢) بوصفه فجوة معرفية جوهرية بين دقة النماذج وقابلية الاعتماد عليها في القرارات الحساسة.

المبدأ الخامس: المساءلة والمسؤولية (Accountability & Responsibility) ويستلزم تحديد الجهات المسؤولة عن قرارات المنظومة، وهو ما يستدعي في التصميم التقني توفير **سجلات تدقيقية (Audit Trails)** تُوثّق مسار كل قرار خوارزمي، وهو ما يُشير إليه Chowdhury (2025) بوصفه شرطاً جوهرياً لأي منظومة ذكاء اصطناعي تعمل في قطاعات حيوية.

المبدأ السادس: القيم الإنسانية والاجتماعية. ويقتضي احترام القيم الاجتماعية والثقافية والدينية في تصميم المنظومات وتشغيلها.

المبدأ السابع: الاستدامة البيئية. ويستلزم مراعاة الأثر البيئي للمنظومات، ومنها استهلاك الطاقة في مراكز البيانات والتدريب.

٣.٤ إطار حوكمة أخلاقيات الذكاء الاصطناعي

أصدرت سدايا لاحقاً "إطار حوكمة أخلاقيات الذكاء الاصطناعي" الذي يُحوّل المبادئ السبعة السابقة إلى منظومة عملية للتقييم والمراجعة، تشمل أدوات لتقييم مستوى المخاطر الأخلاقية للمنظومات، وإجراءات للاعتماد، ومتطلبات للمراجعة الدورية، ويستلزم هذا الإطار أن تخضع منظومات الذكاء الاصطناعي في القطاعات الحيوية ومنها أنظمة النقل الذكي لتقييم أخلاقي منتظم يُوثّق مطابقتها للمبادئ.

٤. الاستراتيجية الوطنية للنقل والخدمات اللوجستية ومحاور تقاطعها مع رؤية ٢٠٣٠

٤.١ الإطار الاستراتيجي العام

تنبثق منظومة الأمن السيبراني السعودية من رؤية المملكة ٢٠٣٠ التي تُشكّل الوثيقة المرجعية العليا للتحويل الوطني. وتتقاطع الرؤية مع موضوع الدراسة الحالية في محورين استراتيجيين رئيسيين:

المحور الأول: برنامج التحول الوطني، الذي يستهدف تعزيز قدرات البنية التحتية للاقتصاد الرقمي وتحسين الخدمات الحكومية عبر التقنية، ويشمل مبادرات تطوير قطاع النقل الذكي.

المحور الثاني: الاستراتيجية الوطنية للنقل والخدمات اللوجستية، التي أطلقت عام ٢٠٢١م، وتستهدف تحويل المملكة إلى مركز لوجستي عالمي عبر رقمنة قطاع النقل بجميع فروعها (البري، والسككي، والبحري، والجوي). ويُشير التقرير المنشور في هارفارد بنس ريفيو (٢٠٢٥) — كما وردت الإشارة إليه في المبحث الثاني — إلى أن سوق أنظمة النقل الذكي في المملكة يُتَوَقَّع أن يتجاوز ملياري دولار بحلول عام ٢٠٣٠م، وهو ما يعكس حجم الاستثمار المتنامي في هذا القطاع.

٤.٢ التقاطع بين الاستراتيجيتين

يُشكّل التقاطع بين الاستراتيجية الوطنية للأمن السيبراني والاستراتيجية الوطنية للنقل الأرضية الاستراتيجية لأي إطار يجمع بين التعلم الآلي والأمن السيبراني في النقل الذكي. ويتسق ذلك مع ما يُبرزه Kure et al. (2022). الأمن أن الأطر الحديثة لإدارة المخاطر السيبرانية في البنى التحتية الحيوية باتت تتطلب اندماجاً استراتيجياً بين الرؤية الوطنية الشاملة والتصميم التقني، بحيث لا يُنظر إلى الإطار التقني بوصفه مشروعاً معزولاً، بل بوصفه استجابة علمية لأولوية وطنية موثقة.

٥. الجهات القطاعية المرجعية في قطاع النقل

٥.١ وزارة النقل والخدمات اللوجستية

تختص الوزارة بالإشراف على جميع أنماط النقل وتنظيم السياسات والاستراتيجيات القطاعية. وتعمل الوزارة على تطبيق مبادرات تشمل توظيف تقنيات الذكاء الاصطناعي في قطاع النقل، وإصدار الأطر التنظيمية للمركبات ذاتية القيادة، وتجربة تشغيلها في مدن سعودية مختارة.

٥.٢ الهيئة العامة للنقل

تختص الهيئة بتنظيم قطاعات النقل البري وخدمات النقل، وإصدار التصاريح، ومراقبة الامتثال. وتُمثّل الهيئة الجهة الأقرب للتفاعل التشغيلي مع أي إطار للأمن السيبراني يُطبّق في منظومة النقل الذكي.

٥.٣ الهيئات المتخصصة الأخرى

تشمل الهيئة السعودية للفضاء، والهيئة العامة للطيران المدني، والهيئة العامة للموانئ، والهيئة السعودية للمواصفات والمقاييس والجودة، وكلّ منها يُشكّل حلقة في المنظومة التنظيمية الشاملة لقطاع النقل.

ويتّضح ممّا سبق أن تطبيق أي إطار للأمن السيبراني في أنظمة النقل الذكية السعودية يستلزم استيعاب ثلاث طبقات تنظيمية متتالية ومتداخلة:

الطبقة الأولى: طبقة الضوابط الفنية الإلزامية الصادرة عن الهيئة الوطنية للأمن السيبراني (ECC) 2018:1 و(CSCC-1:2019)، وتُشكّل الحد الأدنى الفني الملزم.

الطبقة الثانية: طبقة المتطلبات القانونية المُقرّرة في نظام حماية البيانات الشخصية، وتشمل مبادئ محدودية الغرض، وتقليل البيانات، والإفصاح، والحق في التفسير، ومتطلبات الإبلاغ عن الانتهاكات، وقيود نقل البيانات.

الطبقة الثالثة: طبقة المبادئ الأخلاقية-التقنية الصادرة عن سدايا، وتُلزم منظومات الذكاء الاصطناعي بالمبادئ السبعة الحاكمة، ولا سيّما مبدأ القابلية للتفسير الذي يستلزم توظيف تقنيات XAI ضمن التصميم التقني.

جدول رقم (٤): البنية الثلاثية للامتثال التنظيمي السعودي للإطار المقترح

الطبقة	الجهة المرجعية	الوثيقة	متطلبات التصميم التقني
الفنية	الهيئة الوطنية للأمن السيبراني	ECC-1:2018 و CSCC-1:2019	ضوابط الحماية والكشف والاستجابة والصمود
القانونية	سدايا (النظام)	نظام حماية البيانات الشخصية (م/١٩)	تقليل البيانات، الإفصاح، الحق في التفسير، الإبلاغ خلال ٧٢ ساعة

الأخلاقية - التقنية	سدايا	مبادئ أخلاقيات الذكاء الاصطناعي (٢٠٢٣)	XAI، سجلات تدقيقية، معالجة الانحياز، حوكمة أخلاقية
------------------------	-------	--	--

تتبنى الدراسة الحالية هذا التوطين بوصفه بُعداً جوهرياً في تصميم الإطار المقترح، مما يجعله إطاراً مُدمجاً في المنظومة التنظيمية الوطنية لا مجرد ترجمة تقنية للنماذج الدولية. وتتبع هذه الرؤية في تصميم الطبقة الرابعة للنموذج المقترح (طبقة التوافق التنظيمي) التي ستعرض تفصيلاً في المبحث الثالث، والتي تربط مخرجات الطبقة الخوارزمية بمتطلبات الطبقات التنظيمية الثلاث المذكورة، بحيث يخرج قرار النموذج مصحوباً بمعلومات الامتثال التي تُيسر مراجعته من قِبَل الجهات الرقابية، وتحفظ حقوق أصحاب البيانات، وتضمن مطابقته للمبادئ الأخلاقية الوطنية.

وبهذا التوطين، تُقدّم الدراسة إسهاماً نظرياً أصيلاً يتسق مع ما دعا إليه Ali et al. (2025) من ضرورة أن تتجاوز الأطر الحديثة للأمن السيبراني في البنى التحتية الحيوية مرحلة استيراد النماذج الدولية إلى مرحلة إنتاج أطر توطينية تستوعب الخصوصيات الوطنية.

سادساً: مفهوم أنظمة النقل الذكية (ITS) وفلسفتها التشغيلية

تُمثّل أنظمة النقل الذكية (Intelligent Transportation Systems) ثمرة التقاء التقنيات الرقمية بمنظومة النقل التقليدية، وتُعدّ إحدى أبرز تجليات التحول الرقمي في البنى التحتية الحيوية، ويُعرّف المشرفاوي والركابي (٢٠٢١) أنظمة النقل الذكية بأنها منظومة متكاملة تُوظف تقنيات المعلومات والاتصالات في إدارة شبكة النقل، بهدف رفع كفاءة الحركة وتقليل الازدحام وتعزيز السلامة المرورية وخفض الأثر البيئي.

و يطرح شنبي وآخرون (٢٠٢١) رؤية تُبرز البُعد الاستراتيجي لأنظمة النقل الذكية، مؤكدين أنها لا تُمثّل مجرد ترقية تقنية لمنظومات النقل التقليدية، بل تحولاً جوهرياً في فلسفة إدارة قطاع النقل، يقوم على دمج البيانات والاستشعار والاتصال واتخاذ القرار في منظومة موحّدة، وتنطوي هذه الفلسفة على عدة ركائز:

- **الاستخدام المكثّف للبيانات**، إذ تتدفّق البيانات من مصادر متعددة (أجهزة استشعار، كاميرات، أنظمة GPS، تطبيقات المستخدمين (لنكون قاعدة معلوماتية ضخمة تُغذي نظم اتخاذ القرار).
- **التكامل بين الوسائط**، حيث لا تقتصر على نمط نقل واحد بل تُتيح التنسيق بين النقل البري والسككي والبحري والجوي.

- **التركيز على المستخدم**، إذ تسعى إلى تقديم خدمات نقل مخصصة تستجيب لاحتياجات المستخدم في الزمن الحقيقي.

- **الاستدامة البيئية**، عبر تقليل الانبعاثات وتحسين كفاءة استخدام الطاقة.

ويُكمل (Leungbootnak & Heaslip (2025) هذا الطرح برؤية تُركّز على البُعد الوظيفي لأنظمة النقل الذكية، مُشيرين إلى أنها تتألف من ثلاث طبقات رئيسية: طبقة الاستشعار التي تُجمع فيها البيانات من البيئة، وطبقة الاتصال التي تنتقل عبرها البيانات بين العناصر المختلفة، وطبقة الذكاء التي يجري فيها تحليل البيانات وإصدار القرارات، ويتفاعل هذا التقسيم الوظيفي مع المنظور الأمني، إذ تُمثل كل طبقة من هذه الطبقات نقطة تعرّض محتملة للتهديدات السيبرانية، مما يستلزم تصميم منظومات حماية متعددة المستويات.

ويُتّضح من تأمل هذه التعريفات والمنظورات أن أنظمة النقل الذكية تتجاوز كونها أدوات تقنية إلى كونها منظومة استراتيجية تتشابه فيها الأبعاد التقنية والتشغيلية والاجتماعية والبيئية، وهو ما يجعل حمايتها سيبرانياً مسألة بالغة التعقيد تتطلب مقاربات متعدّدة الأبعاد، وأدوات تقييم متطورة قادرة على استيعاب هذا التعقيد.

سابعاً: المكونات الجوهرية لأنظمة النقل الذكية

تتكوّن أنظمة النقل الذكية من جملة من المكونات المتفاعلة التي تتضافر في تكوين منظومة متكاملة. ويُحدّد (Galego & Pascoal (2021 المكونات الجوهرية لهذه الأنظمة في أربعة محاور رئيسية تتفاعل فيما بينها وتُشكّل في مجموعها بنية النقل الذكي.

المكوّن الأول: المركبات المتصلة وذاتية القيادة (Connected and Autonomous Vehicles)

تُمثّل المركبات المتصلة العنصر الديناميكي في منظومة النقل الذكي، وتتميّز بقدرتها على التواصل مع المركبات الأخرى ومع البنية التحتية والمستخدمين، ويُبرز (He et al. (2020 أن هذه المركبات تحتوي على عشرات الوحدات الإلكترونية المُدمجة (ECUs) التي تتولّى وظائف متعددة، تتراوح بين التحكم في المحرك ووظائف القيادة المتقدمة والمساعدة في القيادة. وتعتمد هذه المركبات اعتماداً جوهرياً على بيانات الاستشعار الواردة من رادارات وكاميرات وأجهزة LIDAR ، مما يجعلها بنوياً عُرضةً للتهديدات السيبرانية التي قد تستهدف هذه القنوات.

المكوّن الثاني: البنية التحتية الذكية للطرق (Smart Road Infrastructure)

تشمل هذه البنية الإشارات المرورية الذكية، وأنظمة جمع الرسوم الإلكترونية، ومحطات الشحن للسيارات الكهربائية، وأنظمة المراقبة المرورية. وتُتيح هذه البنية تفاعلاً ثنائي الاتجاه مع المركبات، حيث تُرسل معلومات عن حالة المرور وتتلقّى بيانات عن حركة المركبات.

المكوّن الثالث: الشبكات والاتصالات (Networks and Communications)

يُمثّل هذا المكوّن العمود الفقري الذي تسيّر عليه البيانات بين عناصر المنظومة. وتشمل قنوات الاتصال: الاتصال بين المركبات (V2V)، والاتصال بين المركبة والبنية التحتية (V2I)، والاتصال بين المركبة والشبكة السحابية (V2N)، والاتصال بين المركبة والمشاة (V2P). وتعتمد هذه الاتصالات على تقنيات الجيل الخامس وما يليه، التي توفّر زمن استجابة منخفض وعرض حزمة عالٍ.

المكوّن الرابع: منظومة إنترنت الأشياء والمنصات السحابية

تُمثّل هذه المنظومة الفضاء الذي تتدفّق فيه البيانات وتُعالج. ويُبرز Kumar et al. (2021) أن المنصات السحابية تُمثّل قلب منظومة النقل الذكي، إذ تتولّى تخزين ومعالجة البيانات الضخمة المتدفقة من مختلف المصادر، وتُتيح تطبيق خوارزميات تحليلية متقدمة لاتخاذ القرارات التشغيلية.

ويُضاف إلى هذه المكونات الرئيسية مكونات مساندة كأنظمة الدفع الإلكتروني، وتطبيقات المستخدم، ولوحات المعلومات لإدارة العمليات. وتتفاعل هذه المكونات في منظومة معقدة تُمثّل في مجموعها بنية النقل الذكي.



شكل (3): المكونات الجوهرية لأنظمة النقل الذكية - من إعداد الباحث

ثامناً: الفجوات الأمنية ونقاط الضعف في أنظمة النقل الذكية

تتطوي أنظمة النقل الذكية على عدد من الفجوات الأمنية البنيوية التي تجعلها هدفاً مغرياً للتهديدات السيبرانية. وترصد دراسة Sabaliauskaite et al. (2018) جملة من نقاط الضعف الجوهرية في هذه الأنظمة، تتوزع على مستوى المركبات والبنية التحتية وقنوات الاتصال. وتنشأ هذه الفجوات من تشابك عاملين رئيسيين: التعقيد البنيوي للمنظومة، وتعدد الموردين والمصنّعين للمكونات المختلفة.

ومن أبرز نقاط الضعف، هشاشة قنوات الاتصال اللاسلكية بين المركبات وبين المركبات والبنية التحتية، إذ تستخدم هذه القنوات بروتوكولات قد تتطوي على ثغرات تشفيرية يمكن استغلالها لاعتراض البيانات أو التلاعب بها، ويؤكد Vogt et al. (2021) أن هذه القنوات تمثل أحد أبرز نقاط الاختراق، نظراً لانفتاحها على الفضاء العام بطبيعتها، مما يجعل مراقبتها وحمايتها أمراً تقنياً معقداً.

وتشمل نقاط الضعف الأخرى الضعف في معايير حماية الأجهزة الطرفية، إذ تُصنّع الأجهزة المتصلة بإنترنت الأشياء من جهات متعددة لا تلتزم جميعها بمعايير حماية موحدة، ويبرز Galego & Pascoal (2021) أن هذه الفجوة تخلق ما يُعرف بـ"الحلقة الأضعف" في سلسلة الحماية، حيث يكفي اختراق جهاز واحد ضعيف الحماية للنفاذ إلى المنظومة بأكملها.

كما يُضاف إلى ذلك الفجوات الناتجة عن عدم تحديث الأنظمة المُدمجة في المركبات والبنية التحتية بصورة منتظمة، إذ تتراكم الثغرات المعروفة دون معالجة في كثير من الأنظمة العاملة في الميدان. ويُشير Khan et al. (2024) إلى أن هذه الفجوة تتفاقم بسبب صعوبة إجراء تحديثات على الأنظمة المُدمجة دون تعطيل تشغيلها، مما يؤدي إلى تأخير تطبيق الإصلاحات الأمنية.

وعلى صعيد البيانات، تتعرض المنظومة لمخاطر انتهاك خصوصية بيانات المستخدمين، إذ تتدفق بيانات حساسة حول حركة الأفراد ومواقعهم وعاداتهم. وتنشأ هذه الفجوة من غياب أطر حوكمة واضحة لتداول هذه البيانات، أو من ضعف آليات إخفاء الهوية المُطبقة عليها.

وأخيراً، تبرز الفجوة في الاستجابة للحوادث بوصفها نقطة ضعف تنظيمية، إذ تفتقر كثير من المؤسسات المُشغلة لأنظمة النقل الذكية إلى خطط استجابة مُختبرة ومتكاملة للحوادث السيبرانية، مما يؤخر التعافي ويُضخم الآثار. ويُشكل تجاوز هذه الفجوات مدخلاً جوهرياً لتعزيز كفاءة تقييم المخاطر السيبرانية، وهو ما يُمثل أحد المبررات الجوهرية لتبني أطر قائمة على تقنيات التعلم الآلي تتسم بقدرة استباقية على رصد هذه الفجوات قبل استغلالها.

تاسعاً: واقع أنظمة النقل الذكية في المملكة العربية السعودية ضمن رؤية ٢٠٣٠

اتجهت المملكة العربية السعودية خلال السنوات الأخيرة نحو تبني أنظمة النقل الذكية بوصفها رافداً استراتيجياً لتحقيق مستهدفات رؤية ٢٠٣٠، حيث تتقاطع هذه الأنظمة مع التوجه الوطني نحو بناء مدن ذكية مستدامة وتعزيز التحول الرقمي في البنى التحتية الحيوية.

ووفقاً لتقرير منشور في مجلة هارفارد بزنس ريفيو (٢٠٢٥)، فقد قُدِّر سوق أنظمة النقل الذكي في المملكة العربية السعودية في عام ٢٠٢٣ بنحو ١.١٩ مليار دولار، ويُتَوَقَّع أن يتجاوز ملياري دولار بحلول عام ٢٠٣٠. ويعكس هذا النمو حجم الاستثمار المتنامي في هذا القطاع، الذي تتجاوز قيمته الإجمالية ٣٠٠ مليار دولار مُخصَّصة لتطوير شبكات النقل الذكية والموانئ والطرق. ويُلاحظ كذلك أن نسبة سكان المناطق الحضرية في المملكة تبلغ نحو ٩٢٪، مما يجعل تطوير منظومة نقل ذكية حضرية ضرورة استراتيجية لتلبية احتياجات هذه الكثافة السكانية.

و أنشأت الحكومة وزارة النقل والخدمات اللوجستية بوصفها الجهة المسؤولة عن الإشراف على كافة أنماط النقل، بما في ذلك النقل البري والبحري والجوي والسككي. وتعمل الوزارة وفقاً لمصادرها الرسمية على تطبيق

مبادرات نوعية تشمل: تطبيق أساليب النقل الجديدة، والاستفادة من تقنيات الذكاء الاصطناعي ذات الصلة بقطاع النقل والخدمات اللوجستية، وإطلاق أطر تنظيمية لتقنيات المركبات ذاتية القيادة والمركبات ذات الطاقة النظيفة، فضلاً عن العمل على إصدار إطار تنظيمي لاستخدام طائرات الدرونز في القطاع اللوجستي. كما أطلقت الوزارة تجربة لاستخدام المركبات ذاتية القيادة في مدينة الرياض، وتمتد إلى سبعة مواقع رئيسية تصل سرعتها فيها إلى ١٠٠ كيلومتر/ساعة.

وعلى صعيد إنجازات قطاع النقل، أظهرت مؤشرات وزارة النقل والخدمات اللوجستية (٢٠٢٥) أن حجم الاستثمارات المنفذة في القطاع بلغ نحو ٢٨٠ مليار ريال سعودي، شملت مشاريع الطرق والموانئ والمطارات والسكك الحديدية والمناطق اللوجستية. كما عالج قطاع التوصيل في المملكة أكثر من ١٠١ مليون طلبية في الربع الثاني من عام ٢٠٢٥، مما يعكس حجم النشاط اللوجستي الذي تخدمه المنظومة الذكية.

وعلى صعيد السلامة المرورية بوصفها أحد المؤشرات الجوهرية لنجاح منظومة النقل الذكية، أعلنت اللجنة الوزارية للسلامة المرورية في تقريرها السنوي (٢٠٢٤) أن المملكة نجحت في خفض وفيات الحوادث المرورية بنسبة ٣٥٪ خلال خمس سنوات، حيث انخفض عدد الوفيات من ٩,٣١١ حالة (٢٨.٨ لكل ١٠٠,٠٠٠ نسمة) في عام ٢٠١٦ إلى ٦,٦٥١ حالة (١٨.٥ لكل ١٠٠,٠٠٠ نسمة) في عام ٢٠٢١، وهو ما يعكس التزام المملكة بالوصول إلى الهدف العالمي المتمثل في خفض الوفيات بنسبة ٥٠٪ بحلول عام ٢٠٣٠.

ومن منظور التهديدات السيبرانية، تتعرض هذه المنظومة المتنامية لتهديدات متصاعدة. وتُشير شركة Positive Technologies (2024) في تقريرها عن المشهد السيبراني في الشرق الأوسط إلى تصاعد حدة الهجمات السيبرانية في المنطقة، خاصة تلك التي تستهدف القطاعات الحيوية كالنقل والطاقة. كما يكشف تقرير Market Data Forecast (2024) عن نمو متسارع لسوق الأمن السيبراني في الشرق الأوسط، تستجابةً للحاجة المتنامية إلى حماية البنى التحتية الحيوية.

ويُشير هذا الواقع إلى أن المملكة تقف عند نقطة استراتيجية تتطلب تكاملاً بين التوسع في تبني أنظمة النقل الذكية والاستثمار الموازي في منظومات حمايتها سيبرانياً، وهو ما يُوطّر الحاجة العلمية والتطبيقية للدراسة الحالية.

عاشراً: الكشف (Detection) آليات رصد التهديدات والاختراقات

يُمثِّل الكشف البُعد الأول من أبعاد تقييم مخاطر الأمن السيبراني المعتمدة في الدراسة، ويتمحور حول القدرة على رصد التهديدات والاختراقات في أسرع وقت ممكن، ويُعرَّف (Nikoloudakis et al. (2021 عملية الكشف بأنها مجموعة الأنشطة والآليات التي تستهدف الاستشعار المبكر للأنشطة المريبة في المنظومة الرقمية، وتمييزها عن الأنشطة المشروعة.

وتنقسم آليات الكشف إلى ثلاث فئات رئيسية:

الفئة الأولى: الكشف القائم على التوقيع (Signature-Based Detection)

ويعتمد هذا النوع على قاعدة بيانات للأنماط المعروفة للهجمات، حيث تُقارَن الأنشطة المرصودة بهذه الأنماط لتحديد ما إذا كانت تنطوي على تهديد، ويتميّز هذا النوع بسرعته ودقته في الكشف عن التهديدات المعروفة، غير أنه عاجز عن رصد التهديدات الجديدة التي لم تُوثَّق بعد.

الفئة الثانية: الكشف القائم على الشذوذ (Anomaly-Based Detection)

ويعتمد هذا النوع على بناء بصمة سلوكية للنشاط الطبيعي في المنظومة، ثم رصد أي انحراف عن هذه البصمة بوصفه مؤشراً على تهديد محتمل، وتُشير (Bui et al. (2023 إلى أن هذا النوع يكتسب أهمية متزايدة في بيئات الأمن السيبراني المعاصرة، لأنه قادر على رصد التهديدات الجديدة (Zero-Day) التي لم يسبق توثيقها.

الفئة الثالثة: الكشف القائم على السلوك (Behavior-Based Detection)

ويجمع هذا النوع بين النهجين السابقين، حيث يُحلَّل سلوك المستخدمين والأنظمة عبر الزمن، ويرصد التحوُّلات السلوكية المريبة، وتتضمَّن آليات هذا النوع تحليل سلوك المستخدمين (UBA) وتحليل سلوك الكيانات (EBA).

ويؤكد (Wang et al. (2021 أن فاعلية منظومة الكشف لا تتحقَّق إلا من خلال التكامل بين هذه الفئات الثلاث، إذ يُوفَّر كل منها زاوية مختلفة لرصد التهديدات. وفي بيئة النقل الذكي، يكتسب الكشف أهمية مضاعفة نظراً للطبيعة الحرجة للقرارات التي تتخذها هذه الأنظمة في الزمن الحقيقي، مما يستلزم آليات كشف عالية الدقة وسريعة الاستجابة.

عاشراً: التقييم – (Assessment) قياس مستوى المخاطر وتحديد أولوياتها

يُمثِّل التقييم البُعد الثاني من أبعاد تقييم المخاطر، ويتجاوز مرحلة الكشف إلى تقدير مستوى الخطر الفعلي ومستوى أولوية الاستجابة له. وتُعرِّف (Şahinoglu (2024 عملية التقييم بأنها العملية المنهجية لقياس المخاطر السيبرانية وفق معايير محدّدة، تتضمّن: احتمالية وقوع التهديد، وحجم الأثر المحتمل، ومدى انكشاف الأصول للتهديد.

وتقوم منهجيات التقييم على معادلة جوهرية مفادها: $\text{المخاطرة} = \text{التهديد} \times \text{الانكشاف} \times \text{الأثر}$ ، وتوفّر هذه المعادلة إطاراً كمياً لترتيب المخاطر وفق أولوياتها. ويُكمل (Kalinin et al. (2021 هذا الطرح برؤية تطبيقية في سياق البنى التحتية للمدن الذكية، حيث يطرحون منهجية لتقييم المخاطر تأخذ في الاعتبار التشابك بين العناصر المختلفة للمنظومة، وما يترتب على ذلك من آثار متتالية في حالة تعرّض أحد العناصر للاختراق.

ويتمتع التقييم في بيئة النقل الذكي بطابع خاص، نظراً للترابط الوثيق بين المخاطر السيبرانية ومخاطر السلامة الفيزيائية للأشخاص والممتلكات. ويُبرز (Sabaliauskaite et al. (2018 أهمية التحليل المتكامل للسلامة والأمن السيبراني في أنظمة النقل الذكية التعاونية، مؤكدين أن تقييم المخاطر في هذه البيئات لا يمكن أن يقتصر على البُعد الرقمي وحده، بل يستلزم استيعاب الأبعاد الفيزيائية والتشغيلية للمخاطر.

ويتطلّب التقييم الفاعل توافر مؤشرات قياس واضحة، تشمل: مؤشرات تقنية كعدد الثغرات المرصودة وزمن الكشف عنها، ومؤشرات تشغيلية كزمن الاستجابة للحوادث ومعدّل التعافي منها، ومؤشرات استراتيجية كمستوى النضج السيبراني للمؤسسة.

حادي عشر: الاستجابة — (Response) آليات الاحتواء والمواجهة الفورية للحوادث السيبرانية

يُمثِّل بُعد الاستجابة البُعد الثالث من أبعاد تقييم مخاطر الأمن السيبراني المعتمدة في الدراسة، وينتقل بالمنظومة من مرحلة التشخيص إلى مرحلة الفعل، إذ يُعنى بتنفيذ الإجراءات التقنية والتنظيمية اللازمة لاحتواء التهديد وتقليل أثره فور اكتشافه وتقييمه. ويكتسب هذا البُعد أهمية استراتيجية بوصفه **الحلقة العملية** التي تُترجم قدرات الكشف والتقييم إلى قيمة فعلية للمنظومة الأمنية؛ إذ إن أدقّ منظومات الكشف تفقد

قيمتها إذا لم تُقترن بمنظومة استجابة فاعلة، وأنجح تقييمات المخاطر تتحوّل إلى وثائق مفهومة دون أن تُثمر حماية فعلية ما لم تُترجم إلى فعل ميداني.

١١.١ التأصيل المفاهيمي لمنظومة الاستجابة السيبرانية

يُعرّف (Nikoloudakis et al. (2021) الاستجابة السيبرانية بأنها منظومة الإجراءات المُوجّهة لعزل التهديد ومنع انتشاره، وحماية الأصول المُعرّضة للخطر، وتقليل النافذة الزمنية التي يُلحق فيها المهاجم الضرر بالمنظومة. ويُضيف — (Kure et al. (2022) في إطارهم المتكامل لإدارة المخاطر السيبرانية لحماية البنية التحتية الحيوية — بُعداً منهجياً مفاده أن الاستجابة السيبرانية تجاوزت في تطورها المعاصر مفهوم "ردّ الفعل" إلى مفهوم "الفعل المُوجّه"، بحيث تعمل ضمن منظومة قرار متكاملة تستفيد من نتائج التقييم لتوجيه الاستجابة نحو الأصول الأكثر تعرّضاً وفق أولويات محدّدة سلفاً.

ويطرح (Ali et al. (2025) رؤية موسّعة للاستجابة، إذ يُشرون إلى أن الاستجابة السيبرانية في البنية التحتية الوطنية الحيوية باتت تُشكّل منظومة متعددة المستويات تشمل مستوى المكوّن (Component-Level) الذي يستهدف عزل المكوّن المُصاب، ومستوى النظام (System-Level) الذي يستهدف حماية النظام الكلي من الانتشار، ومستوى المنظومة الوطنية (National-Level) الذي يستهدف حماية المنظومات المترابطة من الأثر السيبراني المتتالي. (Cascading Effect)

١١.٢ فئات آليات الاستجابة وفق مستوى الأتمتة

تنقسم آليات الاستجابة إلى ثلاث فئات رئيسية تختلف في درجة أتمتتها ومستوى التدخل البشري فيها، ولكلٍ منها مواطن قوّة ومحدوديات:

الفئة الأولى: الاستجابة اليدوية (Manual Response)

تعتمد هذه الفئة على تدخّل المحلل السيبراني في اتخاذ قرارات الاحتواء وتنفيذها، ويُقدّم فيها المحلل تقييماً بشرياً للحادث ثم يُنفّذ الإجراءات المناسبة يدوياً. وتوفّر هذه الفئة مرونة عالية في التعامل مع الحالات المعقّدة التي تستلزم حكماً بشرياً، وتُتيح فحصاً دقيقاً قبل اتخاذ إجراءات قد تُعطّل خدمات مشروعة، غير أنها تُعاني — كما يُبرز — (Saba et al. (2024) من بطء الاستجابة الذي يُطيل زمن الإصابة (Dwell Time)، وهو ما يُضاعف الأثر في البيانات التي تتسم بسرعة انتشار الهجوم. ويُشير (Chowdhury (2025) إلى أن دراسات صناعية متعدّدة توثّق أن متوسط زمن الاستجابة اليدوية للحوادث

السيبرانية يتجاوز الساعات، بينما يستغرق بعض أنواع الهجمات (كهجمات الفدية) دقائق معدودة لتنفيذ ضربتها الكاملة.

الفئة الثانية: الاستجابة شبه الآلية (Semi-Automated Response)

تقوم هذه الفئة على تنفيذ الاستجابة عبر منظومات مؤتمتة يُشرف عليها المحلل البشري ويعتمد قراراتها، بحيث تقترح المنظومة إجراءات الاستجابة استناداً إلى تقييم آلي، ويعتمدها المحلل أو يُعدّلها قبل التنفيذ. ويُبرز (Kure et al. (2022 أن هذه الفئة تُمثّل المستوى الأنسب للبيئات الحرجة كأنظمة النقل الذكية، إذ توفّر التوازن بين سرعة الاستجابة والحفاظ على المساءلة البشرية، بما يتّسق مع مبدأ الإنسان في الحلقة (Human-in-the-Loop) الذي تدعو إليه أطر أخلاقيات الذكاء الاصطناعي، ومنها مبادئ سدائيا التي أُشير إليها في القسم السابق.

الفئة الثالثة: الاستجابة الآلية بالكامل (Fully Automated Response)

تعتمد هذه الفئة على منظومات ذكية قادرة على تنفيذ إجراءات الاحتواء دون تدخل بشري، وتُعرف بمنظومات التنسيق (Orchestration) بين أدوات الحماية المختلفة، والأتمتة (Automation) لإجراءات الاستجابة، والاستجابة (Response) نفسها. ويُشير (Ali et al. (2025 إلى أن هذه المنظومات تكتسب أهمية متزايدة في بيئات النقل الذكي التي تتطلب استجابة زمنية دون المئة مئة ثانية، وهي عتبة يستحيل بلوغها عبر التدخل البشري، لا سيّما في مواجهة هجمات V2V السريعة التي تستهدف المركبات ذاتية القيادة أثناء تشغيلها.

ويُضيف (Nikoloudakis et al. (2021 في دراستهم لإطار الوعي الظرفي للأمن السيبراني القائم على التعلم الآلي أن الاستجابة الآلية بالكامل باتت ضرورة لا خياراً في بيئات تتسم بسرعة تدفق البيانات وحرية القرار، غير أنهم يُنبّهون إلى أن هذه الفئة تستلزم مستوى عالياً من موثوقية النموذج لتجنّب "الاستجابات الخاطئة" التي قد تُلحق أضراراً أكبر من الهجوم ذاته.

١١.٣ الإجراءات التقنية للاستجابة في أنظمة النقل الذكية

تشمل الإجراءات التقنية التي تتدرج ضمن الاستجابة السيبرانية في أنظمة النقل الذكية جملةً من الأدوات، يستعرضها (Kumar et al. (2021 في إطار تعلم عميق للاستخبارات السيبرانية للتهديدات في أنظمة

النقل البحري الذكية، و (He et al. (2020) في إطار كشف الهجمات السيبرانية على المركبات المتصلة وذاتية القيادة:

• **العزل الشبكي (Network Isolation)** للعُد المُصابة عبر قواعد جدران الحماية الديناميكية، بحيث يُمنع المكوّن المُصاب من الاتصال بالمنظومة حتى تُعالج إصابته.

• **إسقاط الحزم الخبيثة (Malicious Packet Dropping)** عند بوابات الشبكة استناداً إلى تصنيف الحزم في الزمن الحقيقي.

• **إعادة توجيه المرور (Traffic Rerouting)** بعيداً عن المسارات المُختَرقة، وهو ما يُتيح استمرار الخدمة عبر مسارات بديلة أثناء معالجة الحادث.

• **تفعيل التوقيعات الرقمية البديلة** لصدّ هجمات الانتحال (Spoofing) عبر آليات مصادقة أكثر تعقيداً.

• **إبطال جلسات الاتصال المُشْتَبه فيها** بين المركبات والبنية التحتية عبر آليات إدارة الجلسات الديناميكية.

• **التقييد التلقائي لامتيازات (Automated Privilege Restriction)** للحسابات المُشْتَبه في اختراقها.

• **تفعيل الوضع الآمن التشغيلي (Fail-Safe Mode)** للمكوّنات الحرجة، بحيث تعود إلى وضع تشغيلي أكثر تحفظاً يضمن السلامة الفيزيائية على حساب بعض الوظائف المتقدمة.

١١.٤ الاستجابة في المنظومة السيبرانية-الفيزيائية

يكتسب بُعد الاستجابة في بيئة النقل الذكي أهمية مضاعفة تتجاوز الأبعاد التقليدية، وذلك لسببين جوهريين يرصدهما Sabaliauskaite et al. (2018) في تحليلهم المتكامل للسلامة والأمن السيبراني في أنظمة النقل التعاونية:

السبب الأول: الترابط بين الأمن والسلامة؛ إذ إن التأخر في الاستجابة قد لا يقتصر أثره على الأضرار الرقمية، بل قد يمتدّ إلى أضرار فيزيائية مباشرة على سلامة المركبات والركاب. فاختراق نظام التحكم في

الفرملة قد يُؤدّي إلى حوادث فيزيائية خلال ثوانٍ، ممّا يستلزم استجابة تُقاس بالميلي ثانية، لا بالدقائق أو الساعات كما في المنظومات المعلوماتية التقليدية.

السبب الثاني: التأثير المتسلسل (Cascading Impact) ؛ إذ إن إخفاق الاستجابة في إحدى المركبات قد يمتدّ إلى مركبات أخرى مرتبطة بها عبر قنوات V2V ، ثم إلى شبكة الطرق بأكملها عبر قنوات V2I ، ممّا يُوجد ما يُعرف بـ"الأثر المتسلسل" الذي يُضاعف حجم الضرر بسرعة أسّيّة.

١١.٥ الاستجابة في السياق التنظيمي السعودي

يستلزم أي إطار للاستجابة السيبرانية في المملكة الالتزام بمتطلبات ضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني، التي تُخصّص محوراً كاملاً للاستجابة للحوادث ضمن مكوّن "صمود الأمن السيبراني". كما يستلزم الالتزام بمتطلبات الإبلاغ عن الحوادث السيبرانية إلى الهيئة، وبمتطلبات الإبلاغ عن انتهاكات البيانات المُقرّرة في نظام حماية البيانات الشخصية خلال ٧٢ ساعة، وبمبادئ سدايا التي تستلزم أن تكون الاستجابات الآلية مصحوبةً بسجلات تدقيقية تُوثّق مسار القرار.

١١.٦ تكامل الاستجابة مع البُعد المستقل للتعلم الآلي

تتقاطع منظومة الاستجابة في الإطار المقترح مع بُعد التصنيف التلقائي للمخاطر في المتغير المستقل، إذ إن تصنيف مستوى الخطورة (منخفض/متوسط/عالي/حرج) يُشكّل المُدخل الذي تستند إليه منظومة الاستجابة في اختيار الفئة المناسبة (يدوية/شبه آلية/آلية) وفي تحديد شدّة الإجراءات المُتخذة. وبذلك يتحوّل التصنيف من مجرد تسمية للمخاطر إلى محرّك قرار يُوجّه منظومة الاستجابة بصورة ذكية، وهو ما يُميّز الإطار المقترح عن الأطر التقليدية التي تفصل بين التصنيف والاستجابة.

ثاني عشر: التعافي — (Recovery) استعادة الخدمة وبناء الصمود السيبراني

يُمثّل التعافي البُعد الرابع والختامي من أبعاد تقييم مخاطر الأمن السيبراني، ويُعنى بإعادة المنظومة إلى حالتها التشغيلية الطبيعية بعد الحادث السيبراني، مع الاستفادة من الدروس المستخلصة في تعزيز الصمود المستقبلي. وقد شهد هذا البُعد تطوراً مفاهيمياً جوهرياً خلال العقد الأخير، إذ انتقل من مفهوم "الاستعادة" (Restoration) الضيق إلى مفهوم "الصمود" (Resilience) الأشمل، الذي لا يقتصر على إعادة المنظومة إلى ما كانت عليه، بل يسعى إلى جعلها أفضل ممّا كانت قبل الحادث.

١٢.١ التأصيل المفاهيمي لمنظومة التعافي السيبراني

يُعرّف (Vogt et al. (2021 في إطارهم الشامل لإدارة مخاطر أمن المعلومات في أنظمة النقل الذكية التعافي السيبراني بأنه العملية المنهجية لاستعادة الخدمات المتأثرة، واستعادة سلامة البيانات، وترميم الثقة المؤسسية، وتطوير المنظومة استناداً إلى الحادث المُعاش، ويُضيف (Ali et al. (2025 بُعداً مفاهيمياً محورياً مفاده أن التعافي السيبراني في البنية التحتية الوطنية الحيوية لا يُقاس بسرعة العودة إلى الوضع السابق فحسب، بل يُقاس أيضاً بقدرة المنظومة على تجنب تكرار الحادث في المستقبل، وهو ما يستلزم إدماج التعلّم في قلب منظومة التعافي.

ويطرح (Chowdhury (2025 في نموذجهِ للتقييم اللحظي للمخاطر السيبرانية في الأنظمة المؤسسية باستخدام التعلم العميق رؤيةً موسّعة تدمج التعافي مع بُعد التحسين الذاتي، إذ يرى أن نماذج التعلم الآلي المعاصرة تُتيح إمكانية "التعافي الذكي" الذي يستفيد من كل حادث لتدريب النموذج على أنماط جديدة، ممّا يجعل كل حادث سيبراني فرصةً معرفيةً بدلاً من كونه مجرد كارثة تشغيلية.

١٢.٢ محاور التعافي السيبراني

يقوم التعافي في الأدبيات المعاصرة على أربعة محاور متكاملة يستعرضها الباحثون بمستويات مختلفة من التفصيل:

المحور الأول: الاستعادة التشغيلية (Operational Restoration)

يتضمّن هذا المحور استئناف الخدمات المُعطّلة، وإعادة تفعيل المكونات المُصابة، والتأكد من عودة الأداء إلى مستوياته الطبيعية، ويُبرز (Chowdhury (2025 أن هذا المحور يستلزم توافر خطط استعادة معتمدة (Recovery Plans) مع تحديد مؤشرات أداء واضحة، أبرزها:

- **زمن الاسترداد المستهدف (Recovery Time Objective – RTO)** وهو الحدّ الأقصى المقبول للزمن الذي تكون فيه الخدمة معطّلة، ويكون قصيراً جداً في أنظمة النقل الذكية الحرجة (يُقاس أحياناً بالثواني).
- **نقطة الاسترداد المستهدفة (Recovery Point Objective – RPO)** وهي الحدّ الأقصى المقبول لفقدان البيانات الذي يمكن للمنظومة تحمّله.

ويستلزم هذا المحور توافر نسخ احتياطية دورية للأنظمة والبيانات، مع اختبار هذه النسخ دورياً للتأكد من فاعليتها، فضلاً عن تصميم المنظومات ذات التوافر العالي (**High Availability Systems**) التي تحتفظ بنسخ تشغيلية موازية جاهزة للانتقال إليها فور وقوع الحادث، وهو ما يُشير إليه Kumar et al. (2021) بوصفه شرطاً تقنياً في أنظمة النقل الذكية عالية الحرجية.

المحور الثاني: استعادة سلامة البيانات (Data Integrity Restoration)

يُعنى هذا المحور بالتحقق من عدم تعرّض البيانات للتلاعب خلال الحادث، واستعادة النسخ السليمة عند اللزوم. ويُشير Bitton et al. (2023) في دراستهم لتقييم المخاطر السيبرانية لأنظمة إنتاج التعلم الآلي في العالم الواقعي إلى أن هذا المحور يكتسب تعقيداً خاصاً في بيئات التعلم الآلي، إذ قد يمتدّ الحادث ليشمل تسميم بيانات التدريب (**Data Poisoning**) الذي يُفسد أداء النموذج بصورة تراكمية، ممّا يستلزم إعادة تدريب النماذج على بيانات نقيّة، وقد يستلزم كذلك إعادة التحقق من صحة النماذج المُدرّبة سابقاً للتأكد من عدم تعرّضها للتلوث.

ويُضيف Wang et al. (2021) في دراستهم لتقييم المخاطر السيبرانية لأنظمة التحكم الصناعي بنموذج شجرة الهجوم والدفاع بُعداً منهجياً يتعلّق باستخدام تقنيات التوقيع الرقمي والتجزئة التشفيرية للتحقق من سلامة البيانات، بحيث يُمكن اكتشاف أي تلاعب فور وقوعه، وليس فقط عند الحاجة إلى الاستعادة.

المحور الثالث: التعافي المؤسسي والقانوني (Institutional and Legal Recovery)

يتضمّن هذا المحور إبلاغ الجهات الرقابية، والامتثال لمتطلبات الإفصاح، وإدارة التواصل مع الأطراف المتأثرة. وفي السياق السعودي، يستلزم هذا المحور — كما أُشير سابقاً — الالتزام بمتطلبات الإبلاغ الصادرة عن الهيئة الوطنية للأمن السيبراني، ومتطلبات الإفصاح عن انتهاكات البيانات المقرّرة في نظام حماية البيانات الشخصية خلال ٧٢ ساعة.

ويُشير Ganesan et al. (2022) في دراستهم لتقييم المخاطر السيبرانية في مؤسسات التعليم العالي إلى أن التعافي المؤسسي بات يُشكّل بُعداً حرجاً من أبعاد إدارة الأزمات السيبرانية، إذ إنّ الفشل في التواصل الصحيح مع الجهات الرقابية والجمهور قد يُنتج ضرراً سُمعياً يفوق ضرر الحادث التقني ذاته. ويُبرز Kure et al. (2022) أن التعافي المؤسسي يستلزم توافر **خطط اتصال أزمة (Crisis Communication Plans)** مُعدّة سلفاً، تُحدّد ماذا يُقال، ومتى، ولمن، وبأي قناة.

المحور الرابع: التعلّم التنظيمي وبناء الصمود (Organizational Learning and Resilience Building)

يُمثّل هذا المحور البُعد الأكثر تطوُّراً في التعافي المعاصر، إذ ينقل المنظومة من مرحلة "إصلاح ما وقع" إلى مرحلة "التطور من خلال ما وقع". ويؤكد (Ali et al. (2025 أن هذا المحور يقوم على مبدأ الصمود السيبراني (Cyber Resilience) الذي يتجاوز الاستعادة إلى بناء منظومة قادرة على التكيف مع التهديدات المستقبلية بصورة أفضل، وذلك عبر:

- تحليل جذور الحادث (Root Cause Analysis – RCA) للوصول إلى الأسباب البنيوية العميقة لا الأعراض السطحية.
- تحديث السياسات والإجراءات استناداً إلى الدروس المستفادة.
- تحديث النماذج التنبؤية والكشفية استناداً إلى الحادث الجديد، بحيث تتعلّم المنظومة من كل حادث.
- تحديث برامج التوعية والتدريب للكوادر البشرية.
- مشاركة الدروس المستفادة مع الجهات المماثلة عبر منصّات تبادل المعلومات الاستخباراتية السيبرانية.

ويرصد (Nikoloudakis et al. (2021 أن هذا المحور يُشكّل النقلة النوعية من "الأمن السيبراني الوقائي" إلى "الأمن السيبراني التطوّري" (Evolutionary Cybersecurity) الذي تتعلّم فيه المنظومة من كل تفاعل، بحيث تُصبح أقوى مع مرور الوقت بدلاً من أن تظلّ ثابتة بين التحديثات.

١٢.٣ الصمود السيبراني بوصفه المفهوم الجامع للتعافي المعاصر

تجاوز مفهوم التعافي في الأدبيات الحديثة صيغته التقليدية ليندمج في المفهوم الأشمل للصمود السيبراني (Cyber Resilience) الذي يُعرّفه (Kure et al. (2022 بأنه قدرة المنظومة على الاستمرار في تقديم خدماتها الأساسية في مواجهة الأحداث السيبرانية المعاكسة، سواء أكانت هجمات مقصودة أم أخطاء بشرية أم أعطال تقنية. ويقوم الصمود السيبراني على أربع قدرات جوهرية:

- قدرة التوقّع: (Anticipate) استشراف التهديدات قبل وقوعها.

• **قدرة المواجهة: (Withstand)** الحفاظ على الوظائف الأساسية أثناء الحادث.

• **قدرة الاستعادة: (Recover)** العودة إلى الأداء الطبيعي بعد الحادث.

• **قدرة التكيف: (Adapt)** تطوير المنظومة استناداً إلى الحادث.

ويتضح من هذه القدرات الأربع أن الصمود السيبراني هو المفهوم الجامع الذي يُوحّد أبعاد تقييم المخاطر الأربعة في الدراسة الحالية، إذ يُقابل الكشف قدرة التوقع، ويُقابل التقييم قدرة المواجهة، ويُقابل الاستجابة قدرة الاستعادة، ويُقابل التعافي قدرة التكيف، وهو ما يُعزّز الاتساق المنهجي للإطار النظري للدراسة.

١٢.٤ التكامل بين التعافي والتحسين الذاتي — الحلقة النظرية الكبرى

يتقاطع محور التعلّم التنظيمي في التعافي بصورة مباشرة وبنوية مع بُعد التحسين الذاتي في المتغير المستقل للدراسة، إذ تُوفّر خوارزميات التعلّم الآلي المعزّز (Reinforcement Learning) آليةً منهجيةً لتحويل الحوادث السيبرانية إلى **مدخلات تعليمية** تُحسّن أداء المنظومة تلقائياً، دون تدخل بشري في كل مرة. ويشير (Saba et al. (2024 في إطار عمل ذكي ثنائي المرحلة لتعزيز الأمن السيبراني في تطبيقات إنترنت الأشياء إلى أن هذه العلاقة تُنشئ ما يُمكن تسميته بـ **الحلقة السيبرانية المُتعلّمة** ***** (Learning Cybersecurity Loop)**، بحيث يُغذّي كل حادث المنظومة ببيانات جديدة تُدرّب عليها النماذج، فتُصبح أكثر قدرة على منع حوادث مشابهة مستقبلاً.

ويُشكّل هذا التكامل النظري بين التعافي والتحسين الذاتي أحد أبرز الإسهامات المفاهيمية للدراسة الحالية، إذ يُقدّم رؤية تتجاوز النموذج التقليدي القائم على فصل مراحل تقييم المخاطر عن مراحل بناء القدرات، لصالح نموذج **موحد ودائري** تتغذى فيه كل مرحلة من المرحلة السابقة وتُغذي المرحلة التالية، فيتحوّل الحادث السيبراني من نهاية مؤسفة لدورة الحماية إلى بداية نافعة لدورة تعلّم جديدة.

١٢.٥ تحديات التعافي في أنظمة النقل الذكية

تواجه منظومة التعافي في أنظمة النقل الذكية تحديات متخصصة تختلف عن نظيراتها في القطاعات الأخرى، يرصدها (Khan et al. (2024 في تحليلهم الشامل لتحديات الأمن السيبراني في صناعة النقل:

• **تحدي الاستمرارية:** إذ لا يمكن تعطيل خدمات النقل لإجراء التعافي كما يمكن في القطاعات

الأخرى، ممّا يستلزم آليات تعافٍ "أثناء التشغيل". (Recovery-in-Service)

• **تحدي التوزع الجغرافي:** إذ تنتشر مكونات النقل الذكي على نطاق جغرافي واسع، مما يُصعّب التدخل المادي الفوري.

• **تحدي التعدد المؤسسي:** إذ تُدير منظومة النقل الذكي جهات متعددة (وزارة النقل، والهيئة العامة للنقل، وشركات القطاع الخاص)، مما يستلزم تنسيقاً معقداً في التعافي.

• **تحدي التبعية على النماذج:** إذ إن الاعتماد المتزايد على نماذج التعلم الآلي في اتخاذ القرارات التشغيلية يجعل التعافي مشروطاً بسلامة هذه النماذج، وهو ما يُعقّد إجراءات الاستعادة.

المبحث الثالث : توظيف التعلم الآلي في تقييم مخاطر الأمن السيبراني بأنظمة النقل الذكية

تمهيد

يُمثّل هذا المبحث الركيزة النظرية المركزية للدراسة، إذ يربط بين المتغيرين الجوهريين اللذين تناولهما المبحثان السابقان (تقنيات التعلم الآلي، وتقييم مخاطر الأمن السيبراني)، ويؤطر للنموذج المقترح في الدراسة الحالية. ويتدرّج المبحث من تأسيس الأرضية النظرية للتكامل بين التقنيتين، إلى تفصيل العلاقات التفاعلية بين أبعادهما، فعرض النموذج المقترح ومتطلبات تطبيقه، وانتهاءً باستعراض الدراسات السابقة وتحديد موقع الدراسة الحالية منها.

أولاً: الأسس النظرية للتكامل بين الذكاء الاصطناعي والأمن السيبراني

يقوم التكامل بين الذكاء الاصطناعي والأمن السيبراني على جملة من الأسس النظرية التي تُؤطر هذه العلاقة وتُحدّد ملامحها. ويرتكز هذا التكامل على فرضية جوهرية مفادها أن المشهد السيبراني المعاصر تجاوز قدرات الإنسان على المتابعة والاستجابة الفورية، مما يستلزم أدوات تحليلية ذكية قادرة على معالجة كم هائل من البيانات في الزمن الحقيقي.

ويؤسّس (Ali et al. (2025) لهذا التكامل من منظور البنى التحتية الحيوية الوطنية، حيث يطرحون رؤية مفادها أن دمج الذكاء الاصطناعي في منظومات تقييم المخاطر السيبرانية لا يُمثّل خياراً تطويرياً بل ضرورة استراتيجية، نظراً لتسارع وتيرة التهديدات وتعدّد بنيتها. ويرى الباحثون أن هذا التكامل يستند إلى ثلاث ركائز نظرية:

- **التحوّل من النموذج الستاتيكي إلى النموذج الديناميكي في الأمن السيبراني**، إذ يُتيح الذكاء الاصطناعي بناء منظومات تتطوّر ذاتياً مع تطوّر التهديدات، بدلاً من الاعتماد على قواعد ثابتة سرعان ما تتقادم.
- **الانتقال من الدفاع المحيطي إلى الدفاع المتعدد المستويات**، حيث يُمكن الذكاء الاصطناعي من بناء طبقات حماية متفاعلة تتعاون فيما بينها لتوفير دفاع شامل.
- **الانتقال من الاستجابة إلى الاستباق**، إذ يُتيح الذكاء الاصطناعي التنبؤ بالتهديدات قبل وقوعها، مما يُحوّل فلسفة الأمن السيبراني من ردّ الفعل إلى الفعل الاستباقي.

و يُسلّط Kure et al. (2022) الضوء على الأسس النظرية لإدارة المخاطر السيبرانية في حماية البنى التحتية الحيوية، مُبرزين أن التكامل بين الذكاء الاصطناعي والأمن السيبراني يقوم على ما يُعرف بـ"دورة إدارة المخاطر الذكية"، التي تربط بين التحديد والتحليل والمعالجة والمراقبة في حلقة متصلة، ويُمثّل الذكاء الاصطناعي في هذه الدورة الأداة التي تُتيح الانتقال السلس بين هذه المراحل، وتحوّلها من ممارسات منفصلة إلى منظومة متكاملة.

ويُكمل Sahinoglu (2024) هذا الطرح بتأكيد البُعد الكمي للتكامل بين التقنيتين، مُشيراً إلى أن نمذجة المخاطر السيبرانية كمياً تستلزم قدرات تحليلية متقدمة لا تتوفّر إلا في خوارزميات الذكاء الاصطناعي. وتُؤسّس هذه الرؤية لمفهوم "التقييم الكمي للذكاء للمخاطر"، الذي يجمع بين الدقة الرياضية للنماذج الإحصائية والمرونة التكيفية لخوارزميات التعلم الآلي.

ثانياً: المبررات النظرية والمنهجية لتوظيف خوارزميات التعلم الآلي في منظومات تقييم المخاطر السيبرانية

يستند توظيف خوارزميات التعلم الآلي في منظومات تقييم المخاطر السيبرانية إلى منظومة متشعبة من المبررات النظرية والمنهجية والتطبيقية، تُمثّل في مجموعها الأساس العلمي الذي يُوطّر لهذا التحوّل النوعي في فلسفة الأمن السيبراني المعاصر، ولا يُمكن اعتبار هذه المبررات مجرد دواعٍ تقنية، بل تتجاوز ذلك لتُمثّل استجابة معرفية عميقة لتحولات هيكلية شهدتها المشهد السيبراني العالمي خلال العقد الأخير، وأفرزت فجوة متنامية بين قدرات الأدوات التقليدية وبين متطلبات الواقع الجديد.

الانفجار المعلوماتي وتجاوز قدرات المعالجة التقليدية

يُمثّل التضخم غير المسبوق في حجم البيانات السيبرانية أحد أبرز المبررات الجوهرية لتوظيف التعلم الآلي. ويُسلّط Chowdhury (2025) الضوء على هذا البُعد، مُشيراً إلى أن المنظومات الرقمية المعاصرة تُولّد كميات هائلة من سجلات الأحداث وبيانات حركة الشبكة وتسجيلات الاستشعار، تتجاوز قدرات الكوادر البشرية والأدوات الإحصائية التقليدية على المعالجة والتحليل. ويتفاقم هذا التحدي في بيئات النقل الذكي، إذ تتدفّق البيانات بصورة لحظية من مصادر متعددة تشمل المركبات المتصلة، والبنية التحتية الذكية، وأجهزة الاستشعار المرورية، ومنصات الدفع الإلكتروني، مما يُولّد ضغطاً معلوماتياً يصعب معه استخلاص الإشارات الأمنية ذات القيمة وسط الضوضاء البيانية الهائلة.

وتنشأ من هذا الانفجار المعلوماتي ظاهرة "إجهاد التنبيهات (Alert Fatigue)" التي يُعاني منها المحللون السيبرانيون، حيث تتراكم آلاف التنبيهات اليومية التي يصعب معالجتها يدوياً. ويُتيح التعلم الآلي تجاوز هذه الإشكالية عبر آليات الفرز التلقائي والترتيب الذكي للتنبيهات وفق مستوى أولويتها، مما يُمكن الكوادر البشرية من التركيز على التهديدات الجوهرية.

التطور المتسارع للتهديدات السيبرانية وتعدّد بنيتها

يُشكّل التطور المتسارع للتهديدات السيبرانية مبرراً جوهرياً آخر يدعم توظيف التعلم الآلي. ويُؤكد Ali et al. (2025) أن المشهد السيبراني المعاصر شهد تحولاً نوعياً في طبيعة التهديدات، إذ لم تعد محصورة في الأنماط البدائية المعروفة، بل تطوّرت لتشمل تهديدات متعددة المراحل (APT)، وتهديدات هجينة تجمع بين عدة تقنيات هجوم، وتهديدات قائمة على الذكاء الاصطناعي ذاته (Adversarial AI). وتتميّز هذه التهديدات بقدرتها على التخفي وتجنّب أنظمة الكشف التقليدية القائمة على التوقع، مما يستلزم منظومات كشف ذكية تعتمد على التحليل السلوكي والكشف عن الشذوذ، وهي وظائف لا يُمكن تأديتها بكفاءة دون توظيف خوارزميات التعلم الآلي.

ويُضاف إلى ذلك أن التهديدات الحديثة تُوظّف ذاتها تقنيات الذكاء الاصطناعي في تصميم هجماتها، مما يُوجد سباقاً تقنياً يستلزم من الجانب الدفاعي الاستعانة بأدوات بمستوى تقني مكافئ. وهنا يكتسب التعلم الآلي أهميته بوصفه أداة قادرة على مجاراة هذا التطور والتعلّم من أنماط الهجوم الجديدة بصورة ذاتية.

قصور النماذج الإحصائية التقليدية في تمثيل العلاقات المعقدة

يُمثّل القصور البنوي للنماذج الإحصائية التقليدية مبرراً منهجياً قوياً لتوظيف التعلم الآلي. ويُسلّط Yao & García de Soto (2024) الضوء على هذا البُعد، مُشيرين إلى أن النماذج الإحصائية الكلاسيكية تنطوي على افتراضات مقيدة (كالخطية والاستقلال والتوزيع الطبيعي) لا تتسق مع الطبيعة الواقعية لمشهد المخاطر السيبرانية. فالعلاقات بين متغيرات المخاطر السيبرانية تتسم بكونها غير خطية ومتشابكة ومتعددة الأبعاد، مما يستلزم أدوات نمذجة أكثر مرونة قادرة على استيعاب هذا التعقيد.

وتُتيح خوارزميات التعلم الآلي تجاوز هذا القصور عبر بناء نماذج لا تشترط افتراضات مسبقة حول طبيعة العلاقات بين المتغيرات، بل تستخلصها من البيانات ذاتها. كما تُمكن هذه الخوارزميات من التعامل مع

المتغيرات عالية الأبعاد (High-Dimensional) التي تتجاوز فيها أعداد المتغيرات أعداد الملاحظات، وهي حالة شائعة في تحليلات الأمن السيبراني.

الفجوة في الكوادر البشرية المتخصصة

تُمثّل الفجوة العالمية في الكوادر البشرية المتخصصة في الأمن السيبراني مبرراً عملياً قوياً لتوظيف التعلم الآلي. ويشير (Rafaiani et al. (2023 إلى أن الطلب على المتخصصين السيبرانيين يفوق العرض المتاح بصورة مطّردة، مما يُوجد ضغطاً على المؤسسات لإيجاد بدائل تقنية تُعوّض هذه الفجوة. ويُتيح التعلم الآلي أتمّة كثير من المهام الروتينية في تقييم المخاطر، مما يُحرّر الكوادر البشرية للتركيز على المهام الاستراتيجية والقرارات عالية الأهمية، ويُمكن المؤسسات من تحقيق كفاءة تشغيلية أعلى بموارد بشرية محدودة.

الحاجة إلى الاستجابة في الزمن الحقيقي

يُمثّل عامل الزمن في الأمن السيبراني عاملاً حاسماً، إذ تتراجع قيمة الاستجابة كلما زاد التأخر فيها. ويُؤكد (Saba et al. (2024 أن الزمن الذي يفصل بين بدء الهجوم واكتشافه (Dwell Time) يُمثّل مؤشراً محورياً لجودة منظومة الحماية، وأن خفضه إلى الحد الأدنى يستلزم آليات معالجة آلية فائقة السرعة، لا تتوقّر إلا في خوارزميات التعلم الآلي. وفي بيئات النقل الذكي تحديداً، تكتسب هذه السرعة أهمية مضاعفة، إذ قد يترتب على التأخر في الاستجابة لتهديد سيبراني عواقب فيزيائية مباشرة على سلامة المركبات والمستخدمين.

ضرورة الموضوعية وقابلية المقارنة في تقييم المخاطر

تُمثّل الموضوعية وقابلية المقارنة بُعداً منهجياً جوهرياً يدعم توظيف التعلم الآلي. ويشير Sahinoglu (2024) إلى أن التقييم البشري للمخاطر السيبرانية يخضع لتحيزات إدراكية متعددة، تشمل التحيز التأكيدي وتحيز التوافر والتحيز نحو الحالات الحديثة، مما يُؤثر على دقة التقييم واتساقه عبر الزمن. وتُتيح خوارزميات التعلم الآلي بناء تقييمات أكثر موضوعية تستند إلى معايير كميّة واضحة، وقابلة للتكرار والمقارنة بين المؤسسات والقطاعات، مما يدعم الحوكمة الرشيدة لإدارة المخاطر السيبرانية.

التكامل مع منظومات الاستجابة الآلية

يُتيح توظيف التعلم الآلي تكاملاً سلساً بين تقييم المخاطر ومنظومات الاستجابة الآلية. ويؤكد (Nikoloudakis et al. (2021 أن هذا التكامل يُمثل المرحلة المتقدمة في تطور الأمن السيبراني، إذ تتحوّل منظومة التقييم من مجرد أداة تشخيصية إلى محرّك لمنظومة دفاع متكاملة قادرة على اتخاذ إجراءات استجابة آلية دون الانتظار للتدخل البشري. وتتجلّى أهمية هذا التكامل في بيئات النقل الذكي التي تتطلّب استجابة فورية للحفاظ على استمرارية الخدمات الحيوية.

ثالثاً: النموذج المفاهيمي المقترح للدراسة إطار متعدد الطبقات لتقييم مخاطر الأمن السيبراني القائم على

التعلم الآلي

استناداً إلى التأسيس النظري الذي عرضه المبحثان السابقان، وإلى المُحصلة النقدية للنماذج الدولية التي كشفت عن خمس محدوديات جوهرية (الطابع الاستاتيكي، وغياب البُعد التنبؤي الكمي، والقصور في استيعاب البيئة السيبرانية-الفيزيائية، وعدم تغطية تهديدات التعلم الآلي ذاته، وعدم التوطين السياقي)، وإلى استيعاب المنظومة التنظيمية السعودية بطبقاتها الثلاث، وإلى المبررات النظرية والمنهجية الست لتوظيف خوارزميات التعلم الآلي في تقييم المخاطر تطرح الدراسة الحالية نموذجاً مفاهيمياً متعدد الطبقات يتجاوز الأطر السائدة عبر دمج بُعدين لم يجتمعا في إطار موحد في الأدبيات المتاحة حتى تاريخ إعداد هذه الدراسة: **الديناميكية الخوارزمية والتوطين السياقي.**

ويُشكّل هذا القسم **الإسهام النظري الأصيل** للدراسة، إذ ينتقل بها من كونها دراسةً تصف الأدبيات إلى كونها دراسةً تُقدّم بنيةً معرفيةً جديدة، تُضاف إلى الأطر القائمة بوصفها الجيل التالي من أطر الأمن السيبراني القائم على التعلم الآلي في البنى التحتية الحيوية.

٣.١ المسوّغات النظرية لبنية النموذج

يستند النموذج المقترح إلى ثلاث ركائز نظرية:

الركيزة الأولى: نظرية الأنظمة السيبرانية-الفيزيائية (Cyber-Physical Systems Theory) التي تُبرزها دراسة (Sabaliauskaite et al. (2018، وتقضي التعامل مع أنظمة النقل الذكية بوصفها منظومة مزدوجة يتفاعل فيها الرقمي بالفيزيائي، ممّا يستلزم أن يستوعب أي إطار للأمن السيبراني هذا التفاعل بدلاً من الاقتصار على البُعد الرقمي.

الركيزة الثانية: نظرية الصمود السيبراني متعدد المستويات (Multi-Level Cyber Resilience)

Theory) التي يطرحها (Ali et al. (2025) و (Kure et al. (2022)، وتقتضي أن يعمل الإطار على

مستويات متعددة (المكون، والنظام، والمنظومة الوطنية) في تناغم مُنسّق.

الركيزة الثالثة: نظرية التعلم التكيفي المستمر (Continuous Adaptive Learning Theory)

التي يُبرزها (Chowdhury (2025) و (Phiri et al. (2025)، وتقتضي أن يتضمّن الإطار آلية تعلّم

مستمر تُحدّث النماذج ذاتياً استجابةً للتغيّرات في بيئة التهديد.

٣.٢ البنية الطبقيّة للنموذج المقترح

يقوم النموذج المقترح على أربع طبقات متتالية ومتفاعلة، تُشكّل كل طبقة منها مُدخلًا للطبقة التالية

ومُعالجاً لبيانات الطبقة السابقة، بحيث تتكامل في منظومة موحّدة:

الطبقة الأولى: طبقة اكتساب البيانات ومعالجتها الأولية (Data Acquisition and Pre-

processing Layer)

تُعنى هذه الطبقة بجمع البيانات التشغيلية من مصادرها المتعدّدة في منظومة النقل الذكي، وتشمل:

• بيانات ناقل **CAN** من المركبات: وتوفّر تدفقاً مستمراً لرسائل التحكم الداخلي في المركبات، وتُشكّل

وفق (He et al. (2020) أحد أهم مصادر الكشف عن اختراق المركبات المتصلة.

• بيانات **V2X** من قنوات الاتصال: وتشمل $V2V$ و $V2I$ و $V2P$ و $V2N$ ، وتقدّم صورة عن

التفاعلات بين المركبات وبيئتها.

• سجلّات الشبكة من البنية التحتية: وتوفّر رؤية عن حركة البيانات على مستوى الشبكة.

• بيانات المراقبة من المنصات المركزية: وتقدّم منظوراً كلياً على مستوى المنظومة.

وتتضمّن هذه الطبقة آليات معالجة أولية:

• التحقق من سلامة البيانات عبر التوقيعات الرقمية والتجزئة التشفيرية، لضمان عدم تعرّض

البيانات للتلاعب في مسارها.

• معالجة القيم المفقودة والشاذة عبر تقنيات KNN-Imputation و Isolation Forest.

• **التطبيع (Normalization)** لتوحيد مقاييس المتغيرات.

• **هندسة الخصائص (Feature Engineering)** لاستخلاص المتغيرات ذات الأثر التنبؤي، وهو

ما يُبرزه Bui et al. (2023) بوصفه شرطاً لتحقيق دقة الكشف العالية في حركة المرور المشبوهة.

الطبقة الثانية: الطبقة الخوارزمية الرباعية (Quadruple Algorithmic Layer) قلب النموذج

تُشكل هذه الطبقة قلب النموذج، إذ توظف الأبعاد الأربعة للمتغير المستقل في معالجة البيانات، مع ربط بنيوي مُحكم بأبعاد المتغير التابع:

الوحدة الأولى: وحدة التحليل التنبؤي (Predictive Analytics Module)

• **الوظيفة:** استشراف التهديدات المحتملة استناداً إلى الأنماط التاريخية.

• **الخوارزميات:** نماذج السلاسل الزمنية (ARIMA) و (Prophet)، والشبكات العصبية الطويلة قصيرة المدى (LSTM) مع طبقات Attention.

• **الأساس النظري:** يستند إلى ما طرحه Yao & García de Soto (2024) في إطارهم لتقييم المخاطر السيبرانية في قطاع البناء، و Phiri et al. (2025) في إطار التقييم القائم على التعلم الآلي في الأسواق المتقلبة.

• **الربط بالمتغير التابع:** يُوفّر مُدخلًا لُبُعد الكشف عبر رصد الإشارات الضعيفة السابقة للحوادث.

الوحدة الثانية: وحدة الكشف الذكي عن الهجمات (Intelligent Attack Detection Module)

• **الوظيفة:** رصد التهديدات الفعلية في الزمن الحقيقي عبر الكشف السلوكي والكشف عن الشذوذ.

• **الخوارزميات:** الشبكات الالتفافية أحادية البعد (1D-CNN) لتحليل تدفقات CAN ، والمُشغرات التلقائية (Autoencoders) للكشف عن الشذوذ.

• **الأساس النظري:** يستند إلى ما قدّمه He et al. (2020) في إطار كشف الهجمات على المركبات

المتصلة، و Bui et al. (2023) في إطار كشف حركة HTTPS الخبيثة، و Saba et al. (2024) في إطار الأمن السيبراني الذكي لإنترنت الأشياء.

- الربط بالمتغير التابع: يُغذّي بُعد التقييم بمُدخلات دقيقة عن طبيعة التهديد المُكتشَف.

الوحدة الثالثة: وحدة التصنيف التلقائي للمخاطر (Automated Risk Classification Module)

- الوظيفة: تحديد مستوى الخطورة (منخفض/متوسط/عالي/حرج) وأولوية المعالجة.
- الخوارزميات: XGBoost و Random Forest للتصنيف الإشرافي، و DBSCAN للكشف عن الفئات غير المعروفة، وفق سلّم Common Vulnerability Scoring System (CVSS 3.1 بوصفه المرجع الدولي المعياري).
- الأساس النظري: يستند إلى ما طرحه (Rafaiani et al. (2023) في إطار تقييم المخاطر السيبرانية بالتعلم الآلي في القطاع الصحي، و (Franco et al. (2022) في إطار SecRiskAI للتعنُّر بالمخاطر السيبرانية للمؤسسات، وشيت وإبراهيم (٢٠٢٣) في أداة التعلم الآلي لتقييم مخاطر الأمن السيبراني.

- الربط بالمتغير التابع: يربط بُعد التقييم ببُعد الاستجابة، إذ يُوجّه مخرجه اختيار فئة الاستجابة المناسبة.

الوحدة الرابعة: وحدة التحسين الذاتي (Self-Optimization Module)

- الوظيفة: تحديث النموذج ذاتياً في ضوء الحوادث السابقة، ومعالجة ظاهرة الانحراف المفاهيمي (Concept Drift).
- الخوارزميات: التعلم المعزّز العميق (Deep Q-Learning – DQN)، مع آليات تحسين المعلمات التلقائية. (Automated Hyperparameter Tuning)
- الأساس النظري: يستند إلى ما طرحه (Chowdhury (2025) في نماذج التعلم العميق للتقييم اللحظي للمخاطر، و (Saba et al. (2024) في المرحلة الثانية من إطارهم ذي الخطوتين.
- الربط بالمتغير التابع: يُغذّي بُعد التعافي بقدرة مستمرة على التطور والتكيف، ويُنشئ ما أشار إليه القسم السابق بـ"الحلقة السيبرانية المُتعلّمة".

الطبقة الثالثة: طبقة التوطين السياقي (Contextual Localization Layer)

تُمثِّل هذه الطبقة أحد الإسهامات الأصلية للنموذج المقترح، إذ تُميِّزه عن الأطر الدولية العامة. وتتضمَّن هذه الطبقة آليات تكيف مخرجات الطبقة الخوارزمية مع الخصوصيات البنوية لبيئة النقل الذكي في المملكة، وتشمل:

• **آلية إعادة التقييس (Recalibration Mechanism):** تُعدِّل توزيعات المتغيرات في النماذج المُدرَّبة على بيانات دولية لتطابق أنماط القيادة والحركة في المدن السعودية الكبرى (الرياض، وجدة، والدمام).

• **آلية حقن البيانات التركيبية المحلية (Local Synthetic Data Injection):** تُؤلِّد سيناريوهات تُحاكي الخصائص التشغيلية للبنية التحتية السعودية، بما فيها الظروف الحرارية المرتفعة، والمسافات الطويلة بين نقاط الاتصال، وأنماط الازدحام في المواسم الدينية والسياحية.

• **آلية نقل التعلم (Transfer Learning Mechanism):** تُتيح الاستفادة من النماذج المُدرَّبة على البيانات الدولية دون خسارة الخصوصية المحلية، عبر تجميد الطبقات الأولى وإعادة تدريب الطبقات النهائية على البيانات المُكيَّفة.

ويستند التوطين السياقي في أساسه النظري إلى ما دعا إليه (Ali et al. (2025 من ضرورة أن تتجاوز الأطر الحديثة مرحلة استيراد النماذج الدولية إلى مرحلة إنتاج أطر توطينية.

الطبقة الرابعة: طبقة التوافق التنظيمي (Regulatory Alignment Layer)

تضمن هذه الطبقة أن تكون مخرجات النموذج متوافقة مع المنظومة التنظيمية السعودية بطبقاتها الثلاث المُستعرضة سابقاً، وتشمل:

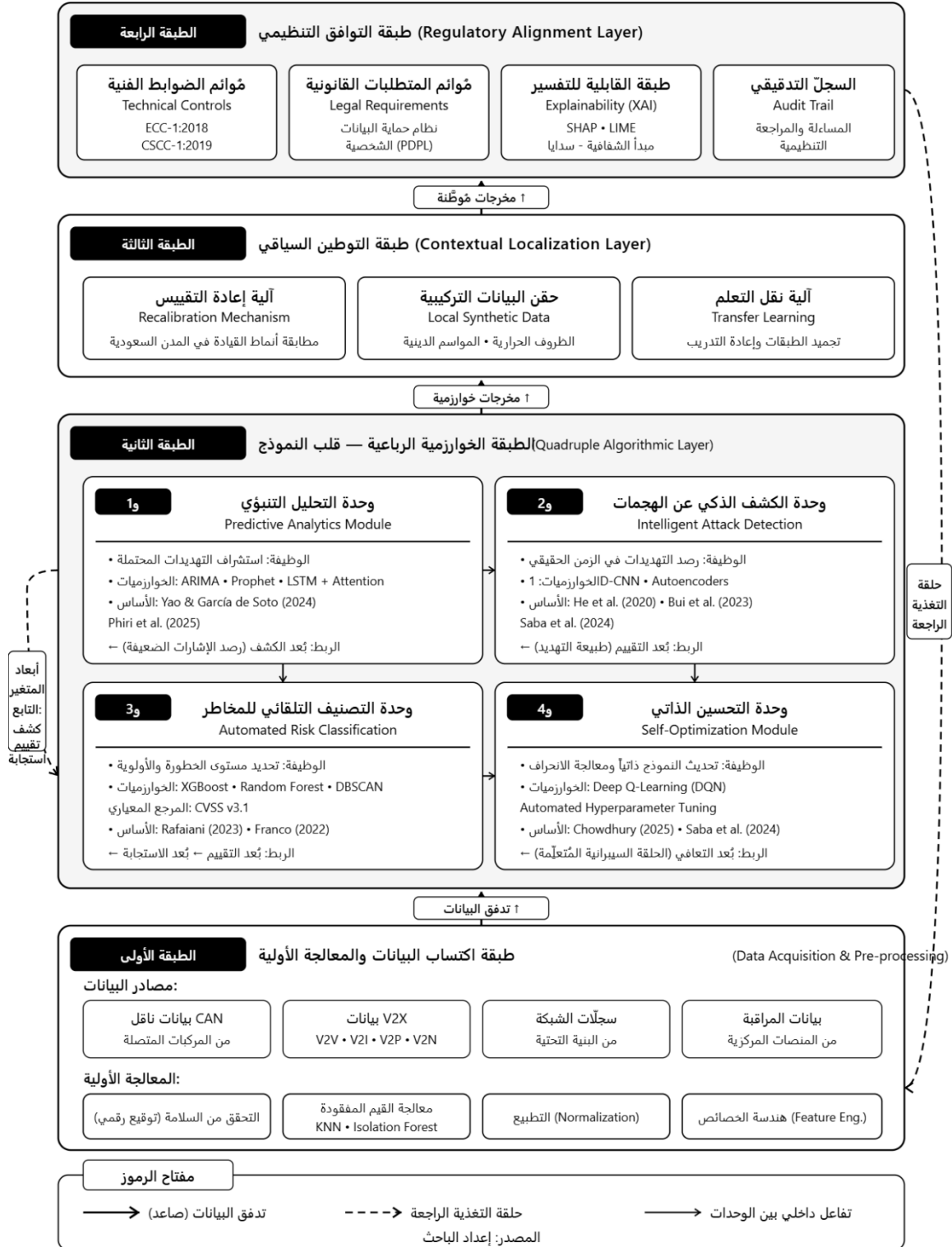
• **مُوائم الضوابط الفنية (Technical Controls Aligner):** يربط قرارات النموذج بضوابط الهيئة الوطنية للأمن السيبراني (ECC-1:2018) و (CSCC-1:2019).

• **مُوائم المتطلبات القانونية (Legal Requirements Aligner):** يضمن الامتثال لنظام حماية البيانات الشخصية، بما في ذلك آلية إبلاغ آلي في حالات الانتهاك خلال المهلة القانونية.

• **طبقة القابلية للتفسير (Explainability Layer):** توظِّف تقنيات (SHAP) و (LIME) لتقديم تفسير مفهوم لقرارات النموذج، تنفيذاً لمبدأ الشفافية والقابلية للتفسير الصادر عن سدايا.

- **السجل التدقيقي (Audit Trail):** يُوثق كل قرار خوارزمي بما يُتيح المساءلة والمراجعة التنظيمية، تنفيذاً لمبدأ المساءلة الصادر عن سدايا.

الشكل رقم (2): البنية الطبقية للنموذج المقترح
إطار الأمن السيبراني الذكي لمنظومة النقل الذكي - المملكة العربية السعودية



٣.٤ خصائص النموذج المميّزة عن الأطر السائدة

يتميّز النموذج المقترح عن الأطر السائدة في الأدبيات بخمس خصائص جوهرية:

الخاصية الأولى: الدمج بين الأنواع الثلاثة للتعليم الآلي في خط أنابيب موحد. فبينما تعاملت الدراسات السابقة كإطار Franco et al. (2022) وإطار Kure et al. (2022) مع أنواع التعلم الآلي بمعزل، يدمج الإطار المقترح التعلم الإشرافي (لكشف الهجمات المعروفة)، وغير الإشرافي (للتصنيف والكشف عن الشذوذ)، والمعزّز (للتحسين الذاتي) في منظومة موحّدة.

الخاصية الثانية: التخصيص لبيئة النقل الذكي بالتقاطع مع البنية السيبرانية-الفيزيائية. إذ يُصمّم النموذج ليستوعب البروتوكولات المتخصصة (V2V) و (V2I) و (IEEE 802.11p) والتفاعل المزدوج بين المكونات الرقمية والفيزيائية، وهو ما لم تُحقّقه أطر مثل SecRiskAI (Franco et al. (2022) المُصمّم للمؤسسات العامة، أو إطار Rafaiani et al. (2023) المُصمّم للقطاع الصحي.

الخاصية الثالثة: استيعاب تهديدات التعلم الآلي ذاته. يتضمّن النموذج آليات لحماية النماذج من الهجمات العدائية (Adversarial Attacks) عبر التدريب العدائي (Adversarial Training) والتحقّق من سلامة بيانات التدريب، وهو ما ينبّه إليه Bitton et al. (2023) و Jziga et al. (2024) بوصفه فجوة في الأطر القائمة.

الخاصية الرابعة: التوطين المتعدد الطبقات. يستوعب النموذج طبقات الامتثال التنظيمي السعودي الثلاث، بحيث يُنتج قرارات مُطابقة تنظيمياً بصورة تلقائية.

الخاصية الخامسة: الحلقة المُعلّمة الدائرية. يربط النموذج بين مخرجات التعافي ومُدخلات التحليل التنبؤي، بحيث يتحوّل كل حادث إلى مادة تعلّمية تُطوّر النموذج، وهو ما يُنشئ منظومة تتحسّن بالخبرة لا منظومة تظلّ ثابتة بين التحديثات.

٣.٥ إطار التحقّق من صحة النموذج المعايير المرجعية في الأدبيات

تمهيد

يستلزم أي إطار قائم على التعلم الآلي في مجال الأمن السيبراني اجتياز معايير أداء صارمة تُحدّدها الأدبيات المتخصصة، وذلك حتى يكتسب مشروعية علمية تُتيح تبنيّه في البيئات التشغيلية. وقد استقرّت

الدراسات على مجموعة من المقاييس الكمية المرجعية التي يُقاس بها أداء الإطار، وتُقارن بخطوط الأساس (Baselines) المستمدة من الأبحاث المرجعية في المجال. ويعرض هذا القسم هذه المعايير بوصفها الإطار النظري للتحقق الذي ستستند إليه المرحلة التطبيقية للدراسة.

٣.٥.١ مقاييس الأداء المرجعية

جدول رقم (٥): مقاييس الأداء المرجعية لتقييم أطر التعلم الآلي في الأمن السيبراني للنقل الذكي

المقياس	الرمز	التعريف	العتبة المرجعية	المصدر
الدقة الإجمالية	Accuracy	نسبة التصنيفات الصحيحة إلى مجموع التصنيفات	$\geq 95\%$	He et al. (2020)
الضبط	Precision	نسبة التنبيهات الحقيقية إلى مجموع التنبيهات	$\geq 93\%$	Kumar et al. (2021)
الاستدعاء	Recall / Sensitivity	نسبة التهديدات المكتشفة إلى مجموع التهديدات الفعلية	$\geq 95\%$	Franco et al. (2022)
مقياس F1	F1-Score	المتوسط التوافقي للضبط والاستدعاء	$\geq 94\%$	Bui et al. (2023)
المساحة تحت المنحنى	ROC-AUC	المساحة تحت منحنى تشغيل المستقبل	$\geq 97\%$	Nikoloudakis et al. (2021)
معدل الإيجابيات الخاطئة	FPR	نسبة التنبيهات الكاذبة إلى الحالات السليمة	$\leq 2\%$	He et al. (2020)

ETSI ITS-معايير	$100 \leq$	الزمن بين الحدث والتنبيه	Detection	زمن الاكتشاف
G5	ملي ثانية		Latency	
Kumar et al.	$500 \leq$	الزمن بين التنبيه واتخاذ	Response	زمن الاستجابة
(2021)	ملي ثانية	الإجراء	Time	

٣.٥.٢ خطوط الأساس المرجعية (Baselines)

يقتضي التحقق العلمي من صحة أي إطار مقارنته بخطوط أساس مرجعية موثقة في الأدبيات، وتعتمد الدراسة الحالية أربع خطوط أساس:

- **خط الأساس الأول:** إطار (2020) He et al. للكشف عن الهجمات على المركبات المتصلة، بوصفه المرجع في مجال أمن المركبات.
- **خط الأساس الثاني:** إطار DLTIF (2021) Kumar et al. لاستخبارات التهديدات القائمة على التعلم العميق في أنظمة النقل البحري الذكية.
- **خط الأساس الثالث:** إطار SecRiskAI (2022) Franco et al. للتنبؤ بالمخاطر السيبرانية في المؤسسات، بوصفه مرجعاً في تقييم المخاطر بالتعلم الآلي.
- **خط الأساس الرابع:** الأساليب التقليدية القائمة على NIST SP 800-30 وتقييم الخبراء دون تعلم آلي، بوصفها معياراً لقياس القيمة المضافة الحقيقية للذكاء الاصطناعي.

الدراسات السابقة :

يتناول الباحث بهذا الجزء مجموعة من الدراسات السابقة ذات الصلة بموضوع الدراسة ، وقد مت تقسيم تلك الدراسات إلى ثلاث مجموعات رئيسية، وهي:

- المجموعة الأولى: الدراسات التي تناولت التعلم الآلي وعلاقته بالمتغيرات الأخرى.
- المجموعة الثانية: الدراسات التي تناولت مخاطر الامن السيبراني وعلاقته بالمتغيرات الأخرى.
- المجموعة الثالثة: الدراسات التي تناولت التعلم الآلي و مخاطر الامن السيبراني .

المجموعة الأولى: الدراسات التي تناولت التعلم الآلي وعلاقته بالمتغيرات الأخرى.

دراسة (2024) Ateya. بعنوان:

The Impact of Machine Learning Algorithms on Improving the Predictive Ability of Accounting Information as Business Partners:

هدفت الدراسة إلى التعرف على تأثير خوارزميات التعلم الآلي (بأبعادها) أشجار القرار، ناقلات الدعم، K-Nearest Neighbor) على المقدرة التنبؤية للمعلومات المحاسبية في التنبؤ بأسعار الأسهم و الاحتفاظ بالنقدية، واستخدمت الدراسة المنهج الوصفي التحليلي، حيث تم استخدام مدخل دراسة الحالة مقارنة ب دراسة الحدث، وتكونت العينة من عدد من ملاحظات الشركات السنوية (Firm-Year observations) التي بلغت ٥٦٤ ملاحظة خلال الفترة من ٢٠١٩ إلى ٢٠٢٢.

وتوصلت نتائج الدراسة إلى أن المقدرة التنبؤية للمعلومات المحاسبية أكثر دقة من خوارزميات التعلم الآلي عند التنبؤ بأسعار الأسهم، مما يشير إلى أن استخدام خوارزميات التعلم الآلي لا يؤدي بالضرورة إلى تنبؤات مالية أكثر دقة، كما أظهرت الدراسة أن دمج خوارزميات التعلم الآلي مع المعلومات المحاسبية يحسن من القدرة التنبؤية للبيانات المالية.

وأوصت الدراسة بضرورة تكامل خوارزميات التعلم الآلي مع المعلومات المحاسبية في نماذج التنبؤات المالية، كما أوصت بضرورة أن يتقن المحاسبون مهارات التعلم الآلي لضمان تطوّرهم المهني في عصر الذكاء الاصطناعي.

دراسة برارمة (٢٠٢٤) بعنوان: دور تطبيقات الذكاء الاصطناعي والتعلم الآلي في إدارة مخاطر المؤسسات الاقتصادية.

هدفت الدراسة إلى تحديد دور تقنيات الذكاء الاصطناعي والتعلم الآلي بأبعادهما (الشبكات العصبية، المتجهات الدعم الآلي) في إدارة مخاطر المؤسسات الاقتصادية، واستخدمت الدراسة المنهج الوصفي التحليلي لتسليط الضوء على مفاهيم الخطر وإدارة المخاطر وأهمية دور هذه التقنيات في التنبؤ بالمخاطر الاقتصادية. وتكونت العينة من عدد من المؤسسات الاقتصادية التي تعتمد على تقنيات الذكاء الاصطناعي في إدارة المخاطر

وتوصلت نتائج الدراسة إلى أن الذكاء الاصطناعي والتعلم الآلي يحسنان بشكل كبير دقة التوقعات المتعلقة بالمخاطر الاقتصادية، كما أن النماذج القائمة على التعلم الآلي يمكن أن تكشف عن المخاطر المحتملة مبكرًا، بما في ذلك التهديدات المالية والأمنية، وأوصت الدراسة بضرورة استخدام تقنيات الذكاء الاصطناعي بشكل موسع في إدارة المخاطر في المؤسسات الاقتصادية، مع التركيز على التحديات التي قد تواجه هذه التقنيات لتحقيق أفضل نتائج.

دراسة (Kayraklioglu et al., 2021) بعنوان:

A Machine–Learning–Based Framework for Productive Locality

Exploitation

هدفت الدراسة إلى التعرف على إطار عمل معتمد على التعلم الآلي بأبعاده (الاستغلال التلقائي للمحلية، استخدام المسجل، تحسين حركة البيانات) على تحسين استغلال المحلية في تطبيقات الذاكرة الموزعة، واستخدمت الدراسة المنهج التحليلي التطبيقي، حيث تم تطوير إطار العمل هذا باستخدام لغة شايبل . وتكونت العينة من تطبيقات تم تمييز كتلتها الحرجة زمنيًا باستخدام البراغما .وتوصلت نتائج الدراسة إلى أن نموذج Elastic Net هو المسجل الأمثل لحالتي، وأن التطبيقات التي تستخدم هذا النموذج يمكن أن تؤدي أداءً مشابهًا للإصدارات التي تم تحسينها يدويًا بواسطة المبرمجين، وأوصت الدراسة بضرورة استخدام هذا النموذج المعتمد على التعلم الآلي في تحسين استغلال المحلية لتطبيقات الذاكرة الموزعة، حيث يمكن تدريب المسجلات في وقت قصير على الأنظمة الموزعة أو محطات العمل.

دراسة (Phiri et al., 2025) بعنوان:

A Machine Learning Based Enhanced Property Valuation Framework for Volatile Markets. .

هدفت الدراسة إلى التعرف على إطار تقييم العقارات المعتمد على التعلم الآلي بأبعاده) التعلم الموجه، نماذج الغابات العشوائية، نماذج (XGBoost على تحسين دقة التنبؤ في أسواق العقارات المتقلبة وذات البيانات المحدودة في قطاع العقارات في زيمبابوي، واستخدمت الدراسة منهج CRISP-DM، وتم تجميع بيانات تضم ١٥٠٠ معاملة عقارية من ٢٠١٩ إلى ٢٠٢٤، مع تضمين متغيرات هيكلية وجغرافية وماكرو اقتصادية، وتكونت العينة من هذه البيانات العقارية التي تم استخدامها لتدريب وتقييم أربع نماذج: الانحدار الخطي، شجرة القرار، الغابات العشوائية، و XGBoost.

وتوصلت نتائج الدراسة إلى أن نموذج الغابات العشوائية كان الأكثر فعالية، حيث حقق أعلى دقة تنبؤية (MAE = 7,420.10؛ RMSE = 9,864.27؛ $R^2 = 1.000$ ، يليه نموذج XGBoost ($R^2 = 0.88$). وأوصت الدراسة باستخدام النماذج المركبة مثل الغابات العشوائية و XGBoost في تطوير نماذج التقييم الآلي في أسواق العقارات المتقلبة، مع التركيز على تطبيقاتها في تحليل مخاطر الرهن العقاري واستراتيجيات التسعير وصياغة السياسات في زيمبابوي والأسواق الناشئة المشابهة.

دراسة (Saba et al., 2024) بعنوان:

A Machine Learning-Based Intelligent Framework With Two-Step Process For Leveraging Cybersecurity In Internet Of Things Use Cases

هدفت الدراسة إلى التعرف على إطار عمل معتمد على التعلم الآلي بأبعاده) اكتشاف الهجمات، تصنيف الهجمات (على تحسين أمان تطبيقات إنترنت الأشياء. (IoT) واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير خوارزمية LbCDC التي تعتمد على التعلم الآلي للكشف عن الهجمات وتصنيفها باستخدام مجموعة بيانات UNSW-NB15 وتكونت العينة من البيانات التي تحتوي على أنواع مختلفة من الهجمات السيبرانية لاختبار فعالية النظام.

وتوصلت نتائج الدراسة إلى أن النظام تمكن من اكتشاف الهجمات بدقة ٨٩.٥٥% وتصنيف الهجمات بدقة 95.97%. وأوصت الدراسة بدمج هذا الإطار في منصات الأمان الحالية للمنظمات لتعزيز أمان تطبيقات إنترنت الأشياء في مواجهة التهديدات السيبرانية.

دراسة (Bui et al., 2023) بعنوان :

A Machine Learning–Based Framework for Detecting Malicious HTTPS Traffic.

هدفت الدراسة إلى التعرف على اختيار مجموعة الميزات المناسبة باستخدام التعلم الآلي بأبعاده) الميزات المعتمدة على التدفق، ميزات بروتوكولات (TLS/SSL على تحسين دقة وكفاءة الكشف عن حركة المرور الخبيثة، واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير إطار عمل لاختيار الميزات بهدف تحسين دقة الكشف وتقليل الوقت اللازم للتنفيذ، وتكونت العينة من عدة مجموعات بيانات مثل CTU-13، MCFP، و CIC-AndMal201 لاختبار فعالية النظام.

وتوصلت نتائج الدراسة إلى أن الإطار المقترح حقق دقة تصل إلى ٩٩ % في الكشف عن حركة المرور الخبيثة في السيناريوهات المدروسة. وأوصت الدراسة باستخدام هذه التقنية لتحسين أنظمة الكشف عن التسلل في الوقت الفعلي، مما يساهم في زيادة كفاءة هذه الأنظمة في مواجهة التهديدات الأمنية. المجموعة الثانية: الدراسات التي تناولت إدارة المخاطر السيبرانية وعلاقته بالمتغيرات الأخرى.

دراسة (Stelkens–Kobsch et al., 2024) بعنوان :

Towards Cybersecurity Risk Assessment for Future ATM – First Steps

هدفت الدراسة إلى التعرف على تقييم المخاطر الأمنية السيبرانية بأبعاده (الأنظمة والمعدات الأساسية والداعمة، التهديدات والتقنيات الناشئة) على إدارة حركة الطيران (ATM) في قطاع الطيران. واستخدمت الدراسة المنهج البحثي الاستكشافي من خلال مشروع SEC-AIRSPACE، الذي يتضمن حالات استخدام للتحقق من صحة النتائج، حيث تم تطوير منهجية جديدة لتقييم المخاطر الأمنية السيبرانية في إدارة حركة الطيران، وتكونت العينة من حالات استخدام مختلفة تتعلق بالبنية التحتية المستقبلية للاتصالات والخدمات المستقلة للمراكز الافتراضية التي تقدم خدمات إدارة حركة الطيران.

وتوصلت نتائج الدراسة إلى أن المنهجية المقترحة تساهم في تحسين أساليب تقييم المخاطر الأمنية، وتوفير تصنيف محدث للأصول والتهديدات في أنظمة إدارة حركة الطيران، وأوصت الدراسة بضرورة تطوير أدوات

وتقنيات لدعم تحليل المخاطر الأمنية في إدارة حركة الطيران، مع التركيز على التقنيات الناشئة والخدمات المستقبلية..

دراسة (Dawodu et al., 2023) بعنوان:

Cybersecurity risk assessment in banking: methodologies and best practices..

هدفت الدراسة إلى التعرف على تقييم المخاطر الأمنية السيبرانية بأبعاده) التهديدات الداخلية والخارجية، تقنيات الذكاء الاصطناعي، التدريب والتوعية الأمنية (على البنوك في قطاع المصارف، واستخدمت الدراسة المنهج التحليلي، حيث تم استكشاف المنهجيات المختلفة وأفضل الممارسات المستخدمة لحماية المؤسسات المالية ضد التهديدات السيبرانية المتطورة، وتكونت العينة من ممارسات الصناعة والإرشادات التنظيمية المتعلقة بالأمن السيبراني في قطاع المصارف، مع التركيز على الاقتصادات النامية مثل نيجيريا وتوصلت نتائج الدراسة إلى أن تقييم المخاطر السيبرانية في البنوك يتطلب دمج تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي، بالإضافة إلى التدريب المستمر وبرامج التوعية للتعامل مع الأخطاء البشرية والهجمات الهندسية الاجتماعية، وأوصت الدراسة بضرورة تطبيق أساليب تقييم المخاطر المعتمدة على الصناعة والتقنيات الحديثة لضمان التوافق مع اللوائح التنظيمية وتعزيز أمن المعلومات وحماية البيانات في البنوك.

دراسة (Wang et al., 2021) بعنوان:

Cybersecurity risk assessment method of ICS based on attack–defense tree model .

هدفت الدراسة إلى التعرف على تقييم المخاطر الأمنية السيبرانية بأبعاده) نظرية الغموض، نموذج شجرة الهجوم والدفاع، تقنية التقييم الاحتمالي للمخاطر السيبرانية (على نظام التحكم التلقائي في إمدادات الوقود في المطار .واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير نموذج تقييم المخاطر بناءً على الغموض

ونموذج شجرة الهجوم والدفاع، وتم تطبيقه على نظام التحكم التلقائي لإمدادات الوقود في المطار .وتكونت العينة من بيانات النظام الأمنية وتهديدات الأمن السيبراني المحتملة .

وتوصلت نتائج الدراسة إلى أن النموذج المطبق يمكنه تقييم المخاطر بشكل شامل، مما يساعد على حل المشكلات العملية التي يواجهها المطار ويوفر أساساً مهماً لخطة حماية الأمن السيبراني في صناعة الطاقة، وأوصت الدراسة باستخدام نموذج تقييم المخاطر هذا لتقليل التأثيرات الذاتية للخبراء وجعل نتائج التقييم أكثر موضوعية ومعقولة، مع التركيز على تطبيق النموذج في أنظمة التحكم الصناعية الأخرى.

دراسة (Şahinoglu, 2024) بعنوان:

Cyber Security Risk Assessment and Optimal Risk Management of a National Vulnerability Database.

هدفت الدراسة إلى التعرف على تقييم المخاطر الأمنية السيبرانية الكمي بأبعاده) خوارزمية Security Meter (SM)، البرمجة الخطية(LP)، إدارة المخاطر الأمنية (على قاعدة البيانات الوطنية للثغرات الأمنية .واستخدمت الدراسة المنهج الكمي، حيث تم تطوير خوارزمية SM لتقييم المخاطر الأمنية وحساب مؤشرات الأمان الحيوية في قاعدة بيانات الثغرات الوطنية. كما تم تحسين إدارة المخاطر باستخدام البرمجة الخطية(LP)، حيث تم مقارنة نتائج الخوارزمية مع حلول EXCEL Solver. وتكونت العينة من بيانات الثغرات الأمنية والتهديدات المرتبطة بها .

وتوصلت نتائج الدراسة إلى أن خوارزمية SM أكثر فعالية من حيث التكلفة مقارنة بحلول EXCEL Solver، مع تحقيق أهداف تخفيض المخاطر بطريقة أكثر كفاءة، وأوصت الدراسة باستخدام الخوارزميات الكمية في إدارة المخاطر الأمنية السيبرانية كحلول أكثر تكلفة وفعالية مقارنة بالأساليب التقليدية غير الكمية.

دراسة(Ganesan et al., 2022) بعنوان :

Cybersecurity Risk Assessment Modeling Factors Associated with Higher Education Institutions

هدفت الدراسة إلى التعرف على نموذج تقييم المخاطر السيبرانية بأبعاده) الأطر النظرية للأمن السيبراني، تقييم المخاطر، تحديد شدة المخاطر، مستوى قبول المخاطر) على المؤسسات التعليمية العليا، واستخدمت الدراسة المنهج التحليلي المقارن، حيث تم مراجعة الأطر الحالية للأمن السيبراني لتحديد مدى ملاءمتها وقيودها في المؤسسات التعليمية، بالإضافة إلى تقييم الأساليب الحالية لتقييم المخاطر السيبرانية في الجامعات، وتكونت العينة من دراسات وممارسات موجودة حول تقييم المخاطر السيبرانية في المؤسسات التعليمية العليا. وتوصلت نتائج الدراسة إلى أن النموذج المقترح يمكن أن يساعد العاملين في الجامعات في تحليل المخاطر، قياس شدة المخاطر، وتحديد مستوى قبول المخاطر، مما يُحسن صناعة القرارات الخاصة بإدارة المخاطر. وأوصت الدراسة بضرورة تطوير نماذج تقييم المخاطر التي تدمج بين الحلول التقنية والتعليمية لتحسين إدارة المخاطر السيبرانية في المؤسسات التعليمية العليا

دراسة (Kalinin et al., 2021) بعنوان :

Cybersecurity Risk Assessment in Smart City Infrastructures.

هدفت الدراسة إلى التعرف على إدارة المخاطر السيبرانية بأبعاده) تصنيف الأجسام، استخراج البيانات، التقييم الكمي للمخاطر (على البنية التحتية للمدينة الذكية. واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير نهج جديد لإدارة المخاطر السيبرانية باستخدام الشبكات العصبية الاصطناعية لتحليل المخاطر بشكل آلي وموضوعي للبنية التحتية الرقمية المتغيرة في المدينة الذكية. وتكونت العينة من شبكات الأجهزة المتصلة مثل IoT ، VANET ، و WSN في المدن الذكية.

وتوصلت نتائج الدراسة إلى أن الشبكات العصبية الاصطناعية تسمح بتقييم المخاطر السيبرانية بشكل تلقائي ودقيق لأنواع مختلفة من الأجسام في البنية التحتية الرقمية للمدينة الذكية، وأوصت الدراسة باستخدام النهج المقترح كأداة فعالة لتقييم المخاطر السيبرانية في البنية التحتية الذكية المتطورة، مما يعزز من إدارة الأمن السيبراني في المدن الذكية.

المجموعة الثالثة: الدراسات التي تناولت التكنولوجيا الذكية وعلاقته بالمتغيرات الأخرى.

دراسة (Bitton et al., 2021) بعنوان :

A Framework for Evaluating the Cybersecurity Risk of Real World, Machine Learning Production Systems

هدفت الدراسة إلى التعرف على تحليل المخاطر السيبرانية بأبعاده (الهجمات على أنظمة التعلم الآلي، توليد وتحليل الرسوم البيانية للهجوم، تقييم التأثير والمخاطر) على أنظمة الإنتاج المعتمدة على التعلم الآلي. واستخدمت الدراسة المنهج التطبيقي، حيث تم توسيع إطار MuIVAL لتوليد وتحليل الرسوم البيانية للهجوم ليشمل الهجمات على أنظمة الإنتاج المعتمدة على التعلم الآلي، وتكونت العينة من بيانات تحتوي على مكونات تعلم آلي لاختبار فعالية النموذج.

وتوصلت نتائج الدراسة إلى أن النموذج المقترح يوفر أداة عملية لخبراء الأمن السيبراني لتقييم تأثير الهجمات على أنظمة التعلم الآلي وتحديد المخاطر المرتبطة بها، وأوصت الدراسة بضرورة اعتماد هذا الإطار لتحليل وتقييم المخاطر في أنظمة الإنتاج المعتمدة على التعلم الآلي لضمان تعزيز الأمان السيبراني وحماية هذه الأنظمة من الهجمات المحتملة.

دراسة (Yao & García de Soto, 2024) بعنوان:

Cyber Risk Assessment Framework for the Construction Industry Using Machine Learning Techniques.

هدفت الدراسة إلى التعرف على إطار تقييم المخاطر السيبرانية بأبعاده (تقنيات التعلم الآلي، جمع البيانات الموجهة، النماذج اللغوية المتقدمة) على صناعة البناء، واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير إطار لتقييم المخاطر السيبرانية باستخدام تقنيات التعلم الآلي، مع دمج الثغرات الخاصة بالصناعة في تقييم المخاطر، وتكونت العينة من مراجعات أدبية متعلقة بأمن السيبراني في صناعة البناء ومقابلات شبه هيكلية مع اثنين من الخبراء في الصناعة

وتوصلت نتائج الدراسة إلى أن النموذج المقترح يمكن أن يساهم في تحسين تقييم المخاطر السيبرانية في صناعة البناء من خلال تحليل البيانات المستمر والنماذج القابلة للتكيف. وأوصت الدراسة بضرورة اعتماد هذا الإطار في صناعة البناء لتحسين إدارة المخاطر السيبرانية بشكل مستمر وفعال.

دراسة (Franco et al., 2022) بعنوان:

SecRiskAI: a Machine Learning–Based Approach for Cybersecurity Risk Prediction in Businesses. .

هدفت الدراسة إلى التعرف على تقييم والتنبؤ بالمخاطر السيبرانية بأبعاده (الذكاء الاصطناعي، التعلم الآلي، تحليل خصائص الأعمال) على الشركات، واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير نهج SecRiskAI الذي يعتمد على التعلم الآلي لتقييم المخاطر السيبرانية باستخدام بيانات صناعية تمثل خصائص أعمال مختلفة مثل عدد الموظفين، قطاع الأعمال، والثغرات المعروفة. وتكونت العينة من بيانات تمثل شركات بمختلف الأحجام والقطاعات لاختبار فعالية النهج.

وتوصلت نتائج الدراسة إلى أن النموذج حقق دقة عالية في التنبؤ بالمخاطر السيبرانية مع أداء منخفض، مما يجعله أداة فعالة في تسهيل عملية التنبؤ بالمخاطر عبر واجهة مستخدم ويب، وأوصت الدراسة باستخدام نهج SecRiskAI في تقييم المخاطر السيبرانية للشركات كأداة مساعدة للقرارات في مواجهة تهديدات الأمن السيبراني.

دراسة (Popova et al., 2023) بعنوان:

Assessment of relationships between smart technologies, corporate sustainability, and economic behavior of companies.

هدفت الدراسة إلى التعرف على تقييم وتنبؤ المخاطر السيبرانية باستخدام التعلم الآلي بأبعاده (تحليل البيانات، استخدام خوارزميات التعلم الآلي، تقييم المخاطر) على الشركات، واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير نهج SecRiskAI الذي يعتمد على أربع خوارزميات تعلم آلي لتقييم المخاطر السيبرانية باستخدام بيانات صناعية تمثل خصائص شركات مختلفة مثل عدد الموظفين، قطاع الأعمال، والثغرات المعروفة، وتكونت العينة من بيانات صناعية تمثل شركات بمختلف الأحجام والقطاعات لاختبار فعالية النموذج.

وتوصلت نتائج الدراسة إلى أن النموذج حقق دقة عالية في التنبؤ بالمخاطر السيبرانية مع أداء منخفض في التنفيذ، مما يسهل عملية التنبؤ بالمخاطر عبر واجهة ويب. وأوصت الدراسة باستخدام نهج SecRiskAI كأداة فعالة لتقييم المخاطر السيبرانية في الشركات ودعمه في اتخاذ القرارات المتعلقة بالأمن السيبراني..

دراسة (Rafaiani et al., 2023) بعنوان:

A Machine Learning-based Method for Cyber Risk Assessment

هدفت الدراسة إلى التعرف على تقييم المخاطر السيبرانية باستخدام التعلم الآلي بأبعاده (التحليل باستخدام المعلومات القابلة للحصول بسهولة، مثل النضج، التعقيد، والجاذبية) على المنظمات في قطاع الرعاية الصحية. واستخدمت الدراسة المنهج التطبيقي، حيث تم تطوير نهج يعتمد على التعلم الآلي لتقييم المخاطر السيبرانية باستخدام معلومات بسيطة تمثل الوضع الأمني السيبراني للمنظمة، وتكونت العينة من ثلاث منظمات في قطاع الرعاية الصحية، تمت دراستها بناءً على قيم مختلفة للنضج والتعقيد.

وتوصلت نتائج الدراسة إلى أن النموذج المقترح يمكن استخدامه بنجاح لتحديد فئة المخاطر السيبرانية لكل منظمة حتى في القطاعات الحساسة مثل الرعاية الصحية. وأوصت الدراسة بضرورة اعتماد هذه الطريقة كأداة فعالة لتقييم المخاطر السيبرانية في القطاعات الحيوية.

النقد التحليلي للدراسات السابقة

بعد عرض الدراسات السابقة موزعةً على مجموعاتها الثلاث، يقدم الباحث في هذا الجزء قراءة نقدية معمقة تتجاوز الإطار الوصفي-المقارن الذي درجت عليه الأدبيات، وتستطرق الدراسات المستعرضة عبر أربعة محاور تحليلية تُشكّل — مجتمعةً — العمود الفقري لأي بناء علمي رصين في مجال دمج التعلّم الآلي بتقييم مخاطر الأمن السيبراني، وهي: (١) منهجية اشتقاق الفرضيات من البيانات الميدانية، (٢) طبيعة تحليل البيانات المعتمد، (٣) آلية تحديد العلاقة بين المتغيرات، (٤) المعايير الكمية لقياس الأثر بين الأبعاد. ويكشف تطبيق هذه المحاور على مجموعات الدراسات الثلاث عن قصور نظامي يُبرّر التوجّه البحثي للدراسة الحالية.

المحور الأول: نقد منهجية اشتقاق الفرضيات من البيانات الميدانية

يُعدّ اشتقاق الفرضيات من بيانات ميدانية موثقة معياراً جوهرياً في الدراسات التطبيقية، إذ يضمن أن العلاقات المُختبرة إحصائياً تعكس واقعاً تشغيلياً لا تصوّراً نظرياً مجرداً.

في المجموعة الأولى (الدراسات التي تناولت التعلّم الآلي وعلاقته بمتغيرات أخرى)، اعتمدت أغلب الدراسات على فرضيات مبنية على أدبيات نظرية سابقة دون إجراء مسح ميداني تمهيدي؛ فدراسة (Ateya, 2024) استمدّت فرضياتها من نماذج محاسبية جاهزة على بيانات ثانوية لـ ٥٦٤ مشاهدة سنوية، دون تحرّ ميداني لخصائص القرار المحاسبي في السياق المصري. وبالمثل، لم تُوثّق دراسة (Phiri et al., 2025) دراسة استطلاعيةً على السوق الزيمبابوي قبل صياغة فرضيات نموذجها العقاري، مما يجعل تعميم النتائج على

أسواق مختلفة مُشكِلاً منهجياً. أما دراسة (Kayraklioglu et al., 2021) فقد اقتصرَت فرضياتها على افتراضات هندسية داخلية لبيئة لغة Chapel، دون إسناد ميداني.

في المجموعة الثانية (الدراسات التي تناولت الأمن السيبراني وعلاقته بمتغيرات أخرى)، تظهر فجوة موازية؛ إذ اعتمدت دراسة (Ganesan et al., 2022) على مراجعة أطر عمل نظرية قائمة لصياغة نموذجها للمؤسسات التعليمية العليا دون بيانات ميدانية من عاملين فعليين في تلك المؤسسات، بينما بنت دراسة (Wang et al., 2021) فرضياتها على نموذج شجرة الهجوم والدفاع بمعالجة نظرية للغموض دون تحقق ميداني من واقع نظام الوقود في المطار. ودراسة (Şahinoglu, 2024) — رغم استنادها لقاعدة الثغرات الوطنية — لم تُوثّق آلية اشتقاق فرضياتها من مسح ميداني على المستهدفين من نتائجها.

في المجموعة الثالثة (الدراسات التي دمجت التعلّم الآلي بالأمن السيبراني)، يتكرر النمط ذاته بصورة أشد؛ إذ اقتصرَت دراسة (García de Soto, 2024 & Yao) على مقابلات شبه هيكلية مع اثنين فقط من الخبراء في قطاع البناء — وهو عدد لا يفي بأدنى متطلبات التمثيل الميداني ولا يسمح بالتحقق من صدق البناء (Construct Validity). وبنت دراسة (Franco et al., 2022) نموذج SecRiskAI على بيانات صناعية مُولّدة (Synthetic Data) دون التحقق من مطابقتها للواقع التشغيلي عبر مسح ميداني تكميلي. أما دراسة (Rafaiani et al., 2023) فقد قصرت عيّنتها على ثلاث مؤسسات فقط في قطاع الرعاية الصحية، وهو حجم لا يكفي لاستنباط فرضيات قابلة للتعميم.

التركيب الكلي للمحور الأول: يكشف الفحص عبر المجموعات الثلاث عن نمط غالب يتمثل في اشتقاق الفرضيات من الأدبيات النظرية أو من بيانات ثانوية جاهزة، دون بناء منهجية تدرّجية تربط المسح الميداني التمهيدي بالصياغة النهائية للفرضيات. ولا تتجو من هذا القصور إلا حالات نادرة تعتمد مقابلات محدودة العدد. ويُفضي هذا النمط إلى فجوة يصعب معها إثبات أن الفرضيات المُختبرة تعكس فعلياً هاجساً تشغيلياً قائماً، لا اقتراحاً نظرياً مُستقًى من دراسات أُجريت في سياقات مغايرة.

المحور الثاني: نقد طبيعة تحليل البيانات (تجريبي حاسوبي مقابل كمّي وصفي)

يشترط البحث المنهجي الرصين تحديداً صريحاً لنوع التحليل المُعتمد، وضبطاً واضحاً للحدود التي تفصل بين التحليل التجريبي الحاسوبي (Computational Experimental) القائم على المحاكاة والخوارزميات، والتحليل الكمّي الوصفي-الاستدلالي القائم على الاستبانات والمعالجة الإحصائية.

في المجموعة الأولى، اعتمدت غالبية الدراسات مساراً أحادياً؛ فقد اقتصرَت دراسات (Bui et al., 2023) و(Saba et al., 2024) و(Kayraklioglu et al., 2021) على تحليل تجريبي حاسوبي بحت داخل بيئات مغلقة، دون تعزيز هذا المسار بتحقيق كمي وصفي يقيس مدى قبول الممارسين للنموذج. وفي المقابل، اعتمدت دراسة (Ateya, 2024) على منهج وصفي-تحليلي كمي دون شق تجريبي حاسوبي، رغم أن موضوع خوارزميات التعلم الآلي يستدعي الجمع بين المسارين. ولا تُصرَح دراسة (برارمة, ٢٠٢٤) بحسم واضح بين طبيعة المنهج التحليلي المُتَّبَع وطبيعة البيانات المُعالَجة، مما يُوقع القارئ في التباس منهجي.

في المجموعة الثانية، يتكرّر القصور نفسه من زاوية أخرى؛ فدراسة (Stelkens-Kobsch et al., 2024) اعتمدت منهجاً استكشافياً قائماً على حالات استخدام (Use Cases) دون تصريح باعتماد تحليل تجريبي حاسوبي أو تحليل كمي وصفي بأدواته المعيارية، بينما وصفت دراسة (Ganesan et al., 2022) منهجها بـ"التحليلي المقارن" دون توضيح ما إذا كان هذا التحليل يستند إلى بيانات كمية أم إلى مقارنة نظرية، وهو ما يُضعف قابلية النتائج للتكرار (Replicability). ودراسة (Dawodu et al., 2023) اقتصرَت على استكشاف نظري لممارسات الصناعة والإرشادات التنظيمية، دون بناء مسار تجريبي أو كمي محدد المعالم.

في المجموعة الثالثة، تظهر معالجة تجريبية حاسوبية غالبية لكن دون تكامل مع الشق الكمي الوصفي؛ فدراسات (Bitton et al., 2021) و(Franco et al., 2022) و(Rafaiani et al., 2023) اعتمدت المسار التجريبي الحاسوبي منفرداً، مما يترك نتائجها معلقةً بين الجودة الخوارزمية المثبتة داخل بيئة الاختبار والفاعلية التشغيلية غير المثبتة في الميدان. أما دراسة (García de Soto, 2024 & Yao) فحاولت دمج الشقين لكن بتمثيل ميداني قاصر (خبيران فقط) لا يرقى لمستوى التحقق الكمي.

التركيب الكلي للمحور الثاني: يبرز في مجموع الدراسات الثلاث غياب التصميم المختلط التسلسلي (Sequential Mixed-Methods Design) الذي يجمع بين تحليل تجريبي حاسوبي صارم على المتغيرات الخوارزمية وتحليل كمي وصفي-استدلالي على استجابات الممارسين. ويُفضي هذا الانفصال إلى أن كثيراً من النماذج المطروحة تُثبت جدارتها في مختبرات الاختبار دون أن تُثبتها في بيئات التطبيق، وهو ما يُشكّل ثغرةً منهجيةً تُبرّر التصميم المزدوج المُعتمد في الدراسة الحالية.

المحور الثالث: نقد آلية تحديد العلاقة بين المتغيرات

يستدعي البحث الصارم تحديداً واضحاً لطبيعة العلاقة بين كل متغير مستقل ومتغير تابع، وتفكيك هذه العلاقة عند مستوى الأبعاد الفرعية (Sub-dimensions) لا الاكتفاء بمعالجتها عند مستوى المتغيرات الرئيسية.

في المجموعة الأولى، عالج أغلب الدراسات المتغير المستقل (التعلم الآلي) بوصفه كتلة واحدة في علاقته بالمتغير التابع، دون تفكيكه إلى أبعاد وتتبع أثر كل بُعد على مستوى مستقل. فدراسة (Phiri et al., 2025) قارنت أداء أربعة نماذج (الانحدار الخطي، شجرة القرار، الغابات العشوائية، XGBoost) لكنها لم تُفكك أثر الأبعاد التقنية داخل كل نموذج (كأثر عدد الأشجار، أو عمق الشجرة، أو استراتيجية التقسيم) على دقة التقييم. وبالمثل، درست (Bui et al., 2023) العلاقة بين اختيار الميزات (Feature Selection) ودقة الكشف بوصفها علاقة ثنائية بسيطة، دون فحص التفاعلات بين ميزات التدفق وميزات بروتوكولات TLS/SSL. وقصرت دراسة (برارمة, ٢٠٢٤) في تحديد آلية العلاقة بين الشبكات العصبية ومُتجهات الدعم من جهة، والمخاطر الاقتصادية من جهة أخرى، حيث بقيت العلاقة موصوفة وصفيًا لا مقياسًا كميًا.

في المجموعة الثانية، عالج دراسة (Kalinin et al., 2021) العلاقة بين الشبكات العصبية الاصطناعية والمخاطر السيبرانية بوصفها علاقة كلية، دون تفكيكها بحسب نوع الأجسام في البنية التحتية (IoT مقابل VANET مقابل WSN). ولم تُقدّم دراسة (Wang et al., 2021) مصفوفة تأثير كمية بين أبعاد نموذج شجرة الهجوم-الدفاع ومكونات تقييم المخاطر، بل اكتفت بتقييم إجمالي. أما دراسة (Şahinoglu, 2024) — رغم اعتمادها خوارزمية Security Meter — فلم تُبين العلاقة الكمية بين مكونات الخوارزمية (SM) ومكونات إدارة المخاطر، بل اكتفت بمقارنة الأداء الكلي مقابل EXCEL Solver.

في المجموعة الثالثة، يتكرّر النقص نفسه؛ إذ اعتمدت دراسة (Franco et al., 2022) في SecRiskAI معالجة إجمالية لأربع خصائص عمل (عدد الموظفين، قطاع العمل، الثغرات المعروفة) في علاقتها بالمخاطر السيبرانية، دون فحص التفاعل بين الخصائص أو بناء مصفوفة تأثير متقاطع. وبالمثل، لم تُقدّم دراسة (Bitton et al., 2021) تفكيكاً كميًا لأثر كل نوع من هجمات التعلم الآلي (Poisoning,)

Rafaiani et al.,) ودراسة (Evasion, Model Inversion) على مكونات تقييم المخاطر منفصلة. ودراسة (2023) اعتمدت ثلاث معلمات (النضج، التعقيد، الجاذبية) دون بيان الوزن النسبي لكل معلمة في العلاقة النهائية.

التركيب الكلي للمحور الثالث: تعاني الدراسات السابقة في مجموعاتها الثلاث من قصور نظامي في تفكيك العلاقة بين المتغيرات إلى مصفوفة تأثير متقاطع (Cross-Impact Matrix) تربط كل بُعد مستقل بكل مكون تابع بصورة "بُعد إلى بُعد". وتبقى العلاقة في معظم الحالات مُعالَجة بوصفها كتلة واحدة، مما يُقيد قدرة الباحثين اللاحقين على تحديد الأبعاد الأكثر تأثيراً، ويُضعف الأساس العلمي للمفاضلة بين الخوارزميات. ويُبرز هذا القصور ضرورة أن تعتمد الدراسة الحالية مصفوفة تأثير رباعية $\times$ رباعية $\times$ (4 $\times$ 4) بين أبعاد التعلّم الآلي ومكونات تقييم مخاطر الأمن السيبراني.

المحور الرابع: نقد المعايير الكمية لقياس الأثر بين الأبعاد

يستدعي البحث الصارم اعتماد معايير كمية دقيقة لقياس الأثر بين المتغيرات، تشمل معايير قوة العلاقة (Association Strength)، ومعايير الدلالة الإحصائية (Statistical Significance)، ومعايير الأداء الخوارزمي (Algorithmic Performance).

في المجموعة الأولى، اقتصرَت دراسة (Phiri et al., 2025) على ثلاثة مقاييس أداء (MAE, RMSE, R^2) دون تعزيزها بمقاييس أخرى كمعامل F1 أو مقاييس حجم الأثر (Effect Size). واعتمدت دراسة (Saba et al., 2024) على الدقة (Accuracy) بوصفها المعيار الأساسي دون تعزيزها بمعامل Matthews (MCC) أو معامل توافق كوهين (Cohen's Kappa)، وهذا الاختزال يُشكّل قصوراً معروفاً في أدبيات التقييم عند التعامل مع بيانات غير متوازنة (Imbalanced Data)، وهو ما ينطبق بحكم الطبيعة على بيانات الهجمات السيبرانية النادرة نسبياً. ولم تُقدّم دراسة (Ateya, 2024) معايير كمية صريحة لحجم الأثر (β معياري أو Cohen's f^2) بين خوارزميات التعلّم الآلي والقدرة التنبؤية للمعلومات المحاسبية.

في المجموعة الثانية، لم تُصرّح دراسة (Dawodu et al., 2023) بأي معايير كمية موحدة، مكثّفة بمراجعة نوعية لممارسات الصناعة. أما دراسة (Ganesan et al., 2022) فقد اعتمدت معايير "التحليل التحليلي المقارن" دون بيان الحدود العددية الدنيا لقبول العلاقات، كعُتبات معاملات الارتباط أو دلالة

كاي-تربيع. ودراسة (Wang et al., 2021) اعتمدت مقارنة تشغيلية دون تحديد عتبة كمية لأدنى قوة علاقة مقبولة (مثل $r \geq 0.30$ أو $R^2 \geq 0.40$).

في المجموعة الثالثة، لم تُقدّم دراسة (Bitton et al., 2021) عتبات كمية صريحة تُميّز بين "مخاطر عالية" و"متوسطة" و"منخفضة"، بل اكتفت بمعالجة نوعية-مرتبية. واقتصرت دراسة (Franco et al., 2022) على "الدقة العالية" و"الأداء المنخفض" في التنفيذ دون تحديد أرقام مرجعية دنيا. وأغفلت دراسة (Rafaiani et al., 2023) ذكر معايير الدلالة الإحصائية (مستوى α وحجم الأثر) في تحديد فئات المخاطر، مما يُضعف موضوعية التصنيف.

التركيب الكلي للمحور الرابع: تُظهر مجموعات الدراسات الثلاث اعتماداً متفاوتاً على معايير كمية جزئية، ونادراً ما تعتمد الدراسات أو أيّ منها منظومةً معياريةً مثلثةً تربط بين قوة العلاقة (r , R^2 , β) والدلالة الإحصائية (α , Power, Effect Size) والأداء الخوارزمي (Precision, Recall, F1, MCC, ROC-AUC, FPR)، ويُفضي هذا القصور إلى صعوبة المقارنة بين نتائج الدراسات، وإلى ضعف الأساس العلمي للحكم على قوة العلاقة بين الأبعاد، مما يستدعي أن تعتمد الدراسة الحالية منظومة معايير كمية مثلثة الفئات.

خاتمة النقد التحليلي وتحديد الفجوة البحثية

يُفضي التحليل النقدي عبر المحاور الأربعة إلى تشخيص فجوة بحثية مركبة لا تقتصر على الفجوة السياقية (غياب النقل الذكي السعودي) أو الفجوة النظرية (غياب النموذج التكاملي الرباعي)، وإنما تمتد لتشمل — وهذا هو الجديد الذي يكشفه النقد المعمق — فجوةً منهجيةً متعدّدة الأبعاد تتمثل في: (١) غياب المنهجية التدرّجية لاشتقاق الفرضيات من مسح ميداني موثّق، (٢) غياب التصميم المختلط التسلسلي الذي يجمع بين التحليل التجريبي الحاسوبي والتحليل الكمي الوصفي-الاستدلالي، (٣) غياب مصفوفة التأثير المتقاطع (4×4) بين أبعاد المتغيرين، (٤) غياب المنظومة المعيارية الكمية مثلثة لقياس الأثر. وتضع هذه الفجوة المُشخّصة الأساس العلمي الذي يستدعي في الدراسة الحالية صياغة فرضيات فرعية تفصيلية تتبثق من بيانات ميدانية سعودية، وتُختبر عبر تصميم مختلط تسلسلي، وتُقاس عبر مصفوفة تأثير رباعية 4×4 رباعية، بمعايير كمية مثلثة الفئات وجميعها تفاصيل مُنفّذة في قسم الخطّة (الفرضيات، المنهجية، المعالجات الإحصائية).

الفجوة البحثية

اتفقت الدراسات السابقة مع الدراسة الحالية في التأكيد على أن تقنيات التعلم الآلي تُعد من أبرز الأدوات الحديثة في دعم التحول الرقمي وتحسين كفاءة الأداء المؤسسي. فقد أوضحت معظم الدراسات (بن تركي وسهام، ٢٠٢١؛ برارمة، ٢٠٢٤؛ Ateya، ٢٠٢٤ ، ٢٠٢٤) أن التعلم الآلي بأبعاده المختلفة كالتنبؤ والتحليل الذكي والتعلم المستمر – يُساهم في رفع كفاءة العمليات التشغيلية وتحسين القدرة على اتخاذ القرار في بيئات معقدة تعتمد على البيانات، كما تتفق هذه الدراسات مع الدراسة الحالية في النظر إلى التعلم الآلي كمنهج تحليلي قادر على اكتشاف الأنماط الخفية في البيانات الضخمة بما يعزز التنبؤ بالمخاطر والتهديدات المستقبلية.

كما اتفقت الدراسات السابقة مع الدراسة الحالية في أن الأمن السيبراني أصبح مكونًا استراتيجيًا أساسيًا في الأنظمة الرقمية الذكية، وأن حماية البيانات والبنى التحتية التقنية تتطلب نماذج تقييم متقدمة قائمة على الذكاء الاصطناعي، فقد أكدت دراسات مثل (Dawodu et al., 2023؛ Sahinoglu, 2024؛ Kalinin et al., 2021) أهمية تطوير أساليب كمية ذكية لتقييم المخاطر السيبرانية بما يضمن تعزيز القدرة على التصدي للهجمات وتخفيف أثارها، وتلتقي هذه النتائج مع توجه الدراسة الحالية التي تسعى إلى دمج تقنيات التعلم الآلي في عمليات تقييم المخاطر السيبرانية كآلية للحد من التهديدات الرقمية وتحسين كفاءة أنظمة الأمن في بيئات النقل الذكي.

إلا أن الدراسات السابقة اختلفت عن الدراسة الحالية في مجال التطبيق والسياق البيئي؛ إذ ركزت أغلب الدراسات على قطاعات مثل القطاع المصرفي، والتعليم العالي، والطاقة، والرعاية الصحية، في حين لم تتناول قطاع النقل الذكي رغم كونه من أكثر القطاعات تعرضًا للهجمات السيبرانية بسبب طبيعته المعتمدة على الاتصال اللحظي والأنظمة المترابطة. ومن هنا تبرز خصوصية الدراسة الحالية التي تختبر هذا الأثر في بيئة أنظمة النقل الذكية، وهو مجال بحثي ما يزال في طور التأسيس ضمن الأدبيات العربية والعالمية. كذلك، تختلف الدراسة الحالية عن معظم الدراسات السابقة من حيث منهجية الربط بين المتغيرات؛ فبينما تناولت البحوث السابقة التعلم الآلي أو الأمن السيبراني كلاً على حدة، فإن هذه الدراسة تسعى إلى دمج المتغيرين في نموذج تفسيري واحد يربط بين أبعاد تقنيات التعلم الآلي (التحليل التنبؤي، الكشف الذكي،

التصنيف التلقائي، والتحسين الذاتي) وبين مكونات تقييم المخاطر السيبرانية (الكشف، التقييم، الاستجابة، والتعافي). وبذلك تُقدّم الدراسة منظورًا تكامليًا جديدًا لم تتناوله الدراسات السابقة بهذا الشكل الشمولي.

تكشف مراجعة الأدبيات أن استخدام تقنيات التعلم الآلي في تقييم مخاطر الأمن السيبراني قد تناولته عدة دراسات، إلا أن معظمها ركّز على قطاعات لا تمت بصلة مباشرة إلى بيئات النقل الذكية، كما لم تقدّم نماذج تكاملية ذات وعي بالسياق أو قدرة على التكيف الديناميكي. فمثلًا، تناولت دراسة (Ateya (2024 التعلم الآلي في المجال المحاسبي وقدرته على تحسين التنبؤ المالي، بينما ركّزت دراسة Brarama (2024) على المخاطر الاقتصادية في المؤسسات، ودراسة (Phiri et al. (2025 على تقييم العقارات في الأسواق المتقلبة. وعلى الرغم من مساهمتها في توضيح فاعلية خوارزميات التعلم الآلي، فإنها لا تعالج الجوانب الخاصة ببيئات النقل الذكي ولا تتعرض لتعقيدات بيانات الحركة في الزمن الحقيقي أو التهديدات المرتبطة بالبنية التحتية للنقل.

وفي سياق الأمن السيبراني، تناولت دراسات مثل (Dawodu et al. (2023 تقييم المخاطر السيبرانية في القطاع البنكي، بينما ركّزت دراسة (Şahinoglu (2024 على تقييم الثغرات الوطنية باستخدام الخوارزميات الكمية، ودرست (Wang et al. (2021 المخاطر في أنظمة التحكم الصناعية. وتوضح هذه الدراسات أن نماذج تقييم المخاطر المتاحة غالبًا ما تكون مصممة لقطاعات محددة (البنوك، الصناعة، الطاقة) ولا تشمل على آليات تتوافق مع طبيعة النقل الذكي، الأمر الذي يعزز وجود فجوة سياقية بين التطبيقات الحالية ومتطلبات منظومة النقل الذكي التي تعتمد على اتصالات V2V و V2I وتدفقات بيانات حساسة في الزمن الحقيقي.

كما تناولت دراسات أخرى العلاقة بين التعلم الآلي والأمن السيبراني، مثل إطار (Bitton et al. (2021 الذي ركّز على المخاطر المتعلقة بأنظمة التعلم الآلي نفسها، ودراسة (Franco et al. (2022 التي قدمت نماذج للتنبؤ بالمخاطر السيبرانية في الشركات، ودراسة (Yao & García de Soto (2024 في قطاع البناء باستخدام تقنيات التعلم الآلي، وعلى الرغم من أهميتها، فإن هذه الدراسات تقدم نماذج عامة أو ثابتة لا تستجيب للطبيعة الديناميكية المتغيرة للأنظمة الذكية، ولا تعالج التفاعل اللحظي بين المركبات والبنية التحتية في أنظمة النقل الذكية، مما يؤكد وجود فجوة نظامية تتمثل في غياب النماذج التي تجمع بين التحليل التنبؤي، والكشف الذكي، والتصنيف التلقائي، والتحسين الذاتي في إطار واحد متكامل.

إضافة إلى ذلك، تُظهر دراسات مثل (Kalinin et al. (2021 التي تناولت المخاطر السيبرانية في البنية التحتية للمدن الذكية، أن هناك توجهاً نحو تقييم المخاطر في الأنظمة المتصلة، ولكنها ركزت على المدن الذكية عمومًا ولم تستهدف النقل الذكي تحديدًا، كما أن نماذجها لم تُبنَ بهدف التعامل مع الهجمات الخاصة ببيئات النقل مثل هجمات تعطيل الخدمة على أنظمة المرور، أو التلاعب ببيانات المركبات الذكية، أو استهداف أجهزة الاستشعار، وهذا يشير إلى محدودية في الوعي بالسياق التشغيلي لأنظمة النقل، مما يعمق الحاجة إلى إطار مصمم خصيصًا لهذه البيئة.

وعليه، فإن التحليل المقارن للدراسات السابقة يؤكد أن غالبية الأبحاث ركزت على سياقات تنظيمية أو اقتصادية أو صناعية مختلفة تمامًا عن النقل الذكي، كما أن النماذج المطروحة غالبًا ما تكون نماذج عامة أو ثابتة لا تواكب ديناميكية النقل الذكي ولا تتكيف مع بياناته في الزمن الحقيقي، ومن هنا تتجلى الفجوة البحثية التي تعالجها الدراسة الحالية، وذلك من خلال تطوير إطار تكاملي قائم على التعلم الآلي، يتمتع بوعي بالسياق السعودي، وقدرة على التكيف الديناميكي، وطبيعة استباقية ذاتية التحسين، وبما يحاكي فعليًا التهديدات السيبرانية ومتطلبات الأمن في أنظمة النقل الذكية.

المساهمات المتوقعة

تهدف هذه الدراسة إلى تقديم مجموعة من المساهمات العلمية والمنهجية والعملية التي تتجاوز مجرد تحليل العلاقة بين المتغيرات، لتقديم إطارًا معرفيًا وتطبيقيًا متكاملًا يمكن الاستفادة منه في تطوير أنظمة النقل الذكية وتعزيز أمنها السيبراني في السياق السعودي. ويمكن تلخيص المساهمات المتوقعة على النحو الآتي:

أولاً: المساهمة النظرية

تقدم الدراسة إطار عمل مبتكرًا ومتكاملًا لتقييم مخاطر الأمن السيبراني في أنظمة النقل الذكية اعتمادًا على تقنيات التعلم الآلي. ويتميز الإطار المقترح بقدرته على تمثيل تقييم المخاطر بشكل ديناميكي واستباقي، استنادًا إلى طبقات تحليل متتابعة تشمل التنبؤ، والكشف، والتصنيف، والتحسين الذاتي، وتسهم هذه الإضافة في توسيع الأدبيات العلمية التي تدمج بين مجالي التعلم الآلي والأمن السيبراني في البنى التحتية الحيوية، وهو مجال يعاني ندرة واضحة في السياقات العربية والخليجية، وبذلك تدعم الدراسة الفجوة النظرية المتعلقة بنقص النماذج النظامية التي تراعي طبيعة البيانات التشغيلية واتصال الأنظمة في بيئات النقل الذكية.

ثانيًا: المساهمة المنهجية

تقدّم الدراسة نموذجًا منهجيًا متدرجًا يجمع بين التجارب الحاسوبية المبنية على بيانات حقيقية أو محاكاة، وبين الأسلوب الكمي القائم على الاستبانات المتخصصة، ويُعد هذا الدمج منهجية متقدمة في مجال البحوث التقنية، إذ توفر الدراسة نهجًا مثبتًا لتطوير نماذج تعلّم آلي واعية بالسياق (Context-Aware ML Models) يمكن اختبارها والتحقق من فاعليتها في بيئات النقل الذكية من خلال مقاييس الأداء المعتمدة علميًا مثل الدقة، والاستدعاء، ومعدل الإيجابيات الخاطئة، ومنحنى ROC. كما تطرح الدراسة خطوات قابلة لإعادة الاستخدام في الأبحاث المستقبلية، تشمل تصميم البيانات، وبناء النماذج، وإجراءات التحقق والتقييم. ويمثل ذلك مساهمة منهجية مهمة، خاصة في ظل ندرة الدراسات التي تجمع بين الجانب التجريبي التطبيقي والتقييم الكمي في مجال الأمن السيبراني للنقل.

ثالثًا: المساهمة العملية

توفر الدراسة أداة عملية وإرشادات تطبيقية يمكن لهيئات النقل السعودية، مثل الهيئة العامة للنقل، والمركز الوطني للأمن السيبراني، ووزارة النقل والخدمات اللوجستية، الاستفادة منها في تعزيز جاهزية الأنظمة الذكية ضد التهديدات السيبرانية، وتسهم نتائج الدراسة في دعم اتخاذ القرار من خلال تقديم معايير مدعومة بالأدلة حول كيفية دمج تقنيات التعلّم الآلي في تقييم المخاطر، وكيفية تحسين إجراءات الكشف والاستجابة والتعافي، كما تمثل الدراسة خطوة مهمة نحو وضع سياسات أكثر دقة وتخصصًا في مجال أمن النقل الذكي، تتوافق مع التحول الرقمي الوطني وأهداف رؤية المملكة ٢٠٣٠ في بناء بنى تحتية ذكية وآمنة وموثوقة.

قائمة المراجع:

- برارمة، ريمة. (٢٠٢٤). دور تطبيقات الذكاء الاصطناعي والتعلم الآلي في إدارة مخاطر المؤسسات الاقتصادية. *مجلة إدارة الأعمال والدراسات الاقتصادية*، مج ١٠، ع ٢، ٢٠٥ - ٢٢٢. مسترجع من <http://search.mandumah.com/Record/1534182>
- بن التركي، زينب، موسى، سهام، و خالدي، فراح. (٢٠٢١). دور التعلم الآلي في تحسين إدارة سلاسل التوريد اللوجستية. *مجلة العلوم الانسانية*، س ٢١، ع ٢، ٥٢٦ - ٥٤٦. مسترجع من <http://search.mandumah.com/Record/1195620>
- شيت، عمر إبراهيم، و إبراهيم، لهيب محمد. (٢٠٢٣). تصميم وتنفيذ أداة التعلم الآلي لتقييم مخاطر الأمن السيبراني. *مجلة التربية والعلم*، مج ٣٢، ع ٢، ٥١ - ٦٤. مسترجع من <http://search.mandumah.com/Record/1401361>
- العدوان، جعفر أحمد عبدالكريم. (٢٠٢٢). أدوار وتحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي: دراسة حالة. *المجلة الأردنية في إدارة الأعمال*، مج ١٨، ع ٣، ٤٣٧ - ٤٥٦. مسترجع من <http://search.mandumah.com/Record/1300089>
- نور الدين، برياش، و بو صلاح، النذير. (٢٠٢٥). دور الذكاء الاصطناعي والتعلم الآلي في تعزيز استراتيجيات التخطيط الرياضي بالجمعيات والنوادي الرياضية بالجزائر. *مجلة جامعة البيضاء*، مج ٧، ع ١، ١١٨٥ - ١١٩٨. مسترجع من <http://search.mandumah.com/Record/1568731>
- عبد ربه، أشرف أحمد حامد. (٢٠٢٤). دور استخدام لغة تعلم الآلة في التنبؤ بالتغيرات في أسعار سعر العملات الأجنبية. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، مج ١٦، عدد خاص ، ٩٤٤ - ٩٥٣. مسترجع من <http://search.mandumah.com/Record/1515177>
- شنب، صورية، بن لخضر، السعيد، و محمودي، حسين. (٢٠٢١). مشروع استراتيجية النقل الذكي لدعم استراتيجية النقل المستدام المقترحة لتطوير النقل البري في الجزائر وعوامل نجاحها.

مجلة الدراسات الاقتصادية المعاصرة، مج ٦، ١٤ ، ٣٠٩ - ٣٢٦. مسترجع من

<http://search.mandumah.com/Record/1669739>

- المشرفاوي، أسامة جاسم محمد، و الركابي، ندى خليفة محمد علي. (٢٠٢١). التطبيقات الرقمية للنقل الذكي ودورها في تعزيز رقمنة المجتمعات والتحول نحو المدن الذكية: مدينة الكوفة حالة دراسة. مجلة البحوث الجغرافية، ع ٣٣ ، ٤٧ - ٨٢. مسترجع من

<http://search.mandumah.com/Record/1167880>

- بن التركي، زينب، موسى، سهام، و خالدي، فراح. (٢٠٢١). دور التعلم الآلي في تحسين إدارة سلاسل التوريد اللوجستية. مجلة العلوم الانسانية، س ٢١، ع ٢٤ ، ٥٢٦ - ٥٤٦. مسترجع من

<http://search.mandumah.com/Record/1195620>

- شيت، عمر إبراهيم، و إبراهيم، لهيب محمد. (٢٠٢٣). تصميم وتنفيذ أداة التعلم الآلي لتقييم مخاطر الأمن السيبراني. مجلة التربية والعلم، مج ٣٢، ع ٢٤ ، ٥١ - ٦٤. مسترجع من

<http://search.mandumah.com/Record/1401361>

- Ateya, S. H. (2024). The impact of machine learning algorithms on improving the predictive ability of accounting information as business partners: An empirical evidence from Egyptian listed firms. *Journal of Accounting Research*, (3), 96–146. Retrieved from <http://search.mandumah.com/Record/1516289>
- Ben Turki, Z., Moussa, S., & Khaldi, F. (2021). The role of machine learning in improving the management of logistics supply chains. *Journal of Human Sciences*, 21(2), 526–546. Retrieved from <http://search.mandumah.com/Record/1195620>
- Bitton, R., Maman, N., Singh, I., Momiyama, S., Elovici, Y., & Shabtai, A. (2023). Evaluating the cybersecurity risk of real-world, machine learning

production systems. *ACM Computing Surveys*, 55(9), 1–36. <http://export.arxiv.org/pdf/2107.01806>

- Brarama, R. (2024). The role of artificial intelligence and machine learning applications in managing the risks of economic institutions. *Journal of Business Administration and Economic Studies*, 10(2), 205–222. Retrieved from <http://search.mandumah.com/Record/1534182>
- Bui, T., Duc, T., Linh Giang, N., Hien, N., Thanh, N., & Khanh, N. (2023, December). A machine learning–based framework for detecting malicious https traffic. In *Proceedings of the 12th International Symposium on Information and Communication Technology* (pp. 769–776).. <https://doi.org/10.1145/3628797.3628874>
- Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O., & Ewuga, S. K. (2023). Cybersecurity risk assessment in banking: methodologies and best practices. *Computer science & IT research journal*, 4(3), 220–243.. <https://doi.org/10.51594/csitrj.v4i3.659>
- Franco, M. F., Sula, E., Celdrán, A. H., Scheid, E. J., Granville, L. Z., & Stiller, B. (2022). SecRiskAI: A machine learning–based approach for cybersecurity risk prediction in businesses. *Conference on Business Informatics*, 01, 1–10. <https://doi.org/10.1109/CBI54897.2022.00008>
- Ganesan, R., Abu Bakar, A., Ramli, R., Abdul Rahim, F., & Zawawi, N. A. (2022). Cybersecurity risk assessment: Modeling factors associated with higher education institutions. *International Journal of Advanced Computer Science and Applications*, 13(8). <https://doi.org/10.14569/ijacsa.2022.0130843>

- Kalinin, M. O., Krundyshev, V., & Zegzhda, P. D. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, 9(4), 78. <https://doi.org/10.3390/MACHINES9040078>
- Kayraklioglu, E., Favry, E., & El-Ghazawi, T. (2021). A machine-learning-based framework for productive locality exploitation. *IEEE Transactions on Parallel and Distributed Systems*, 32(6), 1409–1424. <https://doi.org/10.1109/TPDS.2021.3051348>
- Khan, S., Rahman, M., & Li, Y. (2024). Cyber security challenges in the transportation industry: A comprehensive analysis and recommendations. *Transportation Digital Journal*, 7(1), 15–33.
- Market Data Forecast. (2024). *Middle East cyber security market report (2024–2033)*. Retrieved from <https://www.marketdataforecast.com>
- Phiri, E. V., Chikoore, R., & Hukuimwe, E. M. (2025). A machine learning-based enhanced property valuation framework for volatile markets. *International Journal of Computer Science and Mobile Computing*, 14(7), 97–107. <https://doi.org/10.47760/ijcsmc.2025.v14i07.010>
- Phiri, T., Moyo, P., & Dube, N. (2025). A machine learning-based enhanced property valuation framework for volatile markets. *Journal of Artificial Intelligence Applications*, 18(2), 76–94.
- Positive Technologies. (2024). *Cybersecurity threatscape in the Middle East 2023–2024*. Retrieved from <https://global.ptsecurity.com>
- Rafaiani, G., Battaglioni, M., Senigagliesi, L., Chiaraluce, F., & Baldi, M. (2023). A machine learning-based method for cyber risk assessment. *Proceedings of CBMS 2023*, 263–268. <https://doi.org/10.1109/CBMS58004.2023.00228>

- Saba, M., Terala, S., Khan, I., Rajaboina, N. B., Rekha, M. L. K., & Shravani, D. (2024). A machine learning–based intelligent framework with two–step process for leveraging cybersecurity in Internet of Things use cases. *Nanotechnology Perceptions*, 20(S1–4), 34–47. <https://nanontp.com/index.php/nano/article/view/2804>
- Şahinoglu, M. (2024). Cyber security risk assessment and optimal risk management of a national vulnerability database. *International Journal of Computer Theory and Engineering*, 16(4), 104–126. <https://doi.org/10.7763/ijcte.2024.v16.1359>
- Shīt, O. I., & Ibrāhīm, L. M. (2023). Design and implementation of a machine learning tool for cybersecurity risk assessment. *Journal of Education and Science*, 32(2), 51–64. Retrieved from <http://search.mandumah.com/Record/1401361>
- Stelkens–Kobsch, H., Morlang, F., Bernsmed, K., Meland, H. P., Boumann, H., Martintoni, D., Senni, V., Čanádyová, V., & Sharma, B. (2024). Towards cybersecurity risk assessment for future ATM – First steps. *IEEE DASC 2024 Conference Proceedings*, 1–8. <https://doi.org/10.1109/dasc62030.2024.10748983>
- The concept of assessing the risks of cybersecurity of the information system of the critical infrastructure object. (2022). *Radiotekhnika*, 209, 118–129. <https://doi.org/10.30837/rt.2022.2.209.12>
- Wang, S., Ding, L., Sui, H., & Gu, Z. (2021). Cybersecurity risk assessment method of ICS based on attack–defense tree model. *Journal of Intelligent and Fuzzy Systems*, 40(6), 10475–10488. <https://doi.org/10.3233/JIFS–201126>

- Yao, D., & García de Soto, B. (2024). Cyber risk assessment framework for the construction industry using machine learning techniques. *Buildings*, 14(6), 1561. <https://doi.org/10.3390/buildings14061561>
- Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 24(2), 2472–2481
- He, Q., Meng, X., Qu, R., & Xi, R. (2020). Machine learning-based detection for cyber security attacks on connected and autonomous vehicles. *Mathematics*, 8(8), 1311.
- Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol*, 11(1), 1–24.
- Ali, S. M., Razzaque, A., Yousaf, M., & Ali, S. S. (2025). A novel AI-based integrated cybersecurity risk assessment framework and resilience of national critical infrastructure. *IEEE Access*, 13, 12427–12446.
- Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18), 15241–15271
- Chowdhury, T. K. (2025). AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 675–704

- Nikoloudakis, Y., Kefaloukos, I., Klados, S., Panagiotakis, S., Pallis, E., Skianis, C., & Markakis, E. K. (2021). Towards a machine learning based situational awareness framework for cybersecurity: an SDN implementation. *Sensors*, 21(14), 4939.
- Franco, M. F., Sula, E., Huertas, A., Scheid, E. J., Granville, L. Z., & Stiller, B. (2022, June). SecRiskAI: a machine learning-based approach for cybersecurity risk prediction in businesses. In *2022 IEEE 24th Conference on Business Informatics (CBI)* (Vol. 1, pp. 1–10). IEEE
- Sabaliauskaite, G., Cui, J., Liew, L. S., & Zhou, F. (2018, December). Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. In *2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS)* (pp. 723–728). IEEE.
- Vogt, T., Spahovic, E., Doms, T., Seyer, R., Weiskirchner, H., Pollhammer, K., ... & Chlup, S. (2021). A comprehensive risk management approach to information security in intelligent transport systems. *SAE International Journal of Transportation Cybersecurity and Privacy*, 4(11-04-01-0003), 39–58
- Galego, N. M. C., & Pascoal, R. M. (2021). Cybersecurity in smart cities: Technology and data security in intelligent transport systems. In *Perspectives and Trends in Education and Technology: Selected Papers from ICITED 2021* (pp. 17–33). Singapore: Springer Singapore.
- Leungbootnak, N., & Heaslip, K. (2025). Review of Risk Assessment Methods for Cybersecurity Attacks on Road Network and Intelligent Transportation System Applications. *Transportation Research Record*, 2679(2), 949–959

