

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

مشروع خطة أطروحة للتسجيل لدرجة الدكتوراه

إعداد الباحث:

2025 / 1446هـ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

المحتويات

4	المقدمة:
5	مشكلة الدراسة:
7	أهمية الدراسة
9	أهداف الدراسة
10	فرضيات الدراسة
11	نموذج الدراسة:
13	مصطلحات الدراسة وتعريفاتها الإجرائية:
16	منهج الدراسة:
17	أداة الدراسة
17	مجتمع الدراسة:
19	عينة الدراسة
19	مصادر البيانات في الدراسة
20	المعالجات الإحصائية المقترحة:
21	حدود الدراسة
22	الدراسات السابقة:
31	الفجوة البحثية
34	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، 2021).

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، 2024).

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 2024، مع معدل نمو سنوي مركب يُقدر بـ 9.3% حتى عام 2033. (Market Data Forecast, 2024). كما أشارت تقارير أمنية حديثة إلى أن متوسط تكلفة الهجمة السيبرانية على المؤسسات في الشرق الأوسط يبلغ حوالي 8.75 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 :

1. ما مستوى تطبيق تقنيات التعلم الآلي بأبعادها المختلفة في بيئات النقل الذكية؟
2. ما واقع تقييم وإدارة مخاطر الأمن السيبراني في أنظمة النقل الذكية من حيث (الكشف، التقييم، الاستجابة، والتعافي)؟
3. ما طبيعة العلاقة بين التحليل التنبؤي وتقنيات التنبؤ بالتهديدات السيبرانية في أنظمة النقل الذكية؟

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

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

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

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

8. 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:

1. 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.
2. 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).
3. 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.
4. 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.
5. 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.
6. 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.

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

2. 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.
3. 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.
4. تساعد المؤسسات على تقليل الخسائر التشغيلية والتقنية الناتجة عن الهجمات الإلكترونية، من خلال بناء أنظمة قائمة على التحليل الذكي للمخاطر والاستجابة السريعة للتهديدات.
5. تُسهم في صياغة توصيات استراتيجية يمكن أن تُستثمر في تصميم أطر وطنية للأمن السيبراني في النقل الذكي، تدعم استدامة الأداء وتكامل البنية التحتية الذكية.
6. تفتح آفاقًا للتعاون البحثي التطبيقي بين الجامعات ومراكز الأبحاث وشركات التكنولوجيا في تطوير حلول واقعية قائمة على خوارزميات التعلم الآلي للأمن السيبراني.
7. 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 :

1. تحديد مستوى تبني واستخدام تقنيات التعلم الآلي بأبعادها (التحليل التنبؤي، الكشف الذكي عن الهجمات، التصنيف التلقائي للمخاطر، والتحسين الذاتي) في مكونات أنظمة النقل الذكية.
2. تحليل آليات تقييم مخاطر الأمن السيبراني بأبعادها (الكشف، التقييم، الاستجابة، والتعافي) في بيئات النقل الذكي، واستكشاف التحديات المرتبطة بتطبيقها في السياقات الرقمية المعقدة.
3. 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.
4. استقصاء إسهام تقنيات التعلم الآلي في بناء أنظمة استباقية قادرة على التنبؤ بالتهديدات السيبرانية قبل وقوعها، وتقليل زمن الاستجابة وتعزيز فعالية الدفاعات الرقمية.
5. 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.
6. 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:

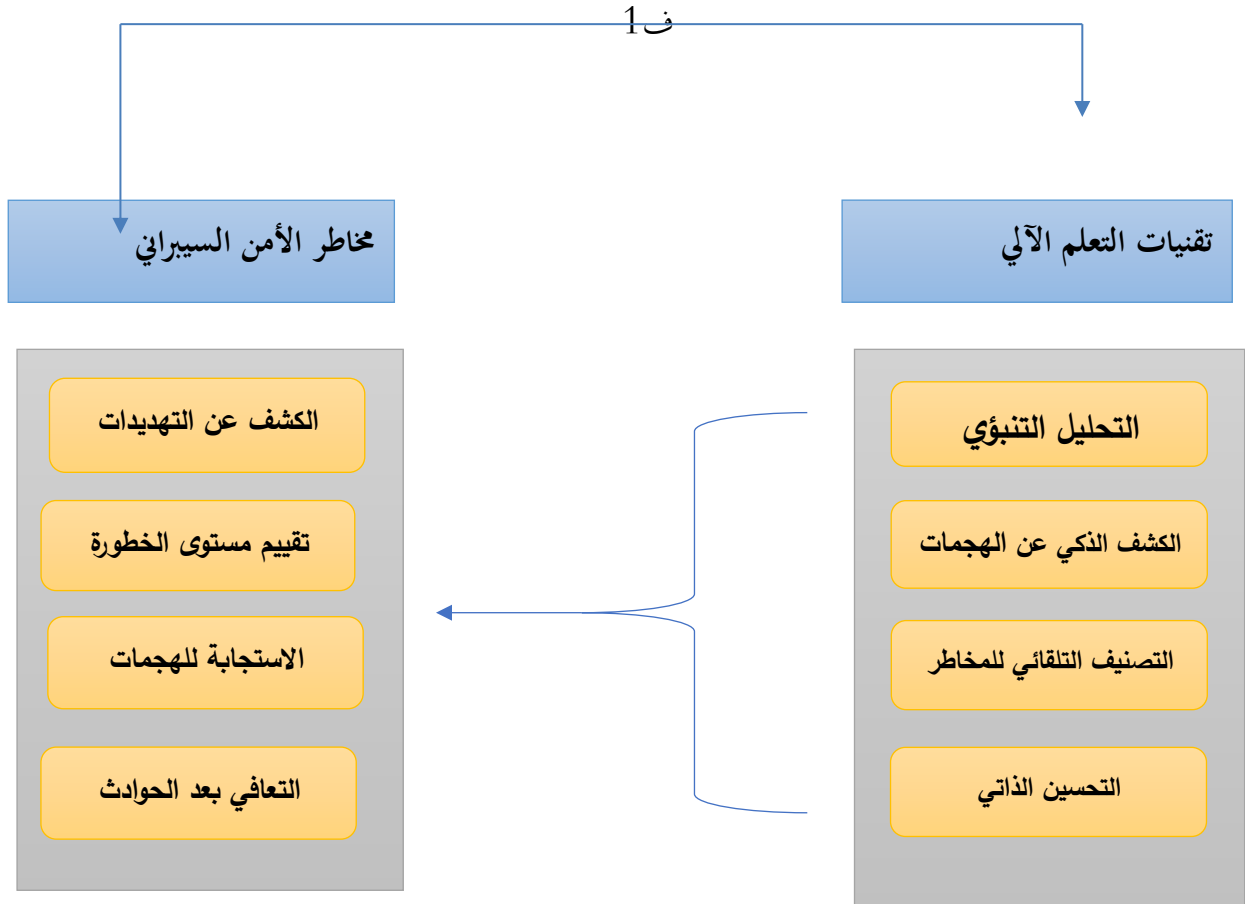
تقييم مخاطر الأمن السيبراني بأبعاده: (الكشف عن التهديدات - تقييم مستوى الخطورة - الاستجابة للهجمات - التعافي بعد الحوادث) بالاعتماد على دراسات (Şahinoglu, 2024) ؛ (Kalinin et al., 2021)؛ (Bitton et al., 2021)

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 (1) 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 تدخّل بشري مباشر، ويُستخدم لتوليد تنبؤات دقيقة واتخاذ قرارات مدعومة بالبيانات في البيئات المعقدة والمتغيرة. (Kayraklioglu et al., 2021)

إجراءيًا: 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)

إجراءيًا: 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)

إجراءيًا: 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.

وسيمثل 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 (600-800) 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 (800 - 600) 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 (600 - 800) فرد يُقدَّر بنحو (265 - 250) مفردة على الأقل لتحقيق مستوى ثقة إحصائية قدره (95%) وهامش خطأ لا يتجاوز (±5%).

وستستهدف الدراسة توزيع عدد (300) 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 2025.
- **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.

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 بـ دراسة الحدث، وتكونت العينة من عدد من ملاحظات الشركات السنوية (Firm–Year observations) التي بلغت 564 ملاحظة خلال الفترة من 2019 إلى 2022.

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 تطورهم المهني في عصر الذكاء الاصطناعي.

دراسة برارمة (2024) 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 1500 معاملة عقارية من 2019 إلى 2024، 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 89.55% 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 99% 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 تسهم 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.

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، 2021؛ برارمة، 2024؛ Ateya:2024 ، 2024) أن التعلم الآلي بأبعاده المختلفة كالتنبؤ والتحليل الذكي والتعلم المستمر – يُسهم 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؛ Kalinin ، Şahinoglu, 2024؛ et al., 2021) أهمية تطوير أساليب كمية ذكية لتقييم المخاطر السيبرانية بما يضمن تعزيز القدرة على التصدي للهجمات وتخفيف آثارها، 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. فمثلاً، 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 ركزت 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، لتقدم 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

تقدم 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 مثبّتًا لتطوير نماذج تعلم 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.

ثالثاً: 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 التعلم الآلي في تقييم المخاطر، وكيفية تحسين إجراءات الكشف والاستجابة والتعافي، كما تمثل الدراسة خطوة مهمة نحو وضع سياسات أكثر دقة وتخصصاً في مجال أمن النقل الذكي، تتوافق مع التحول الرقمي الوطني وأهداف رؤية المملكة 2030 في بناء بنى تحتية ذكية وآمنة وموثوقة.

قائمة المراجع:

- برارمة، ريمة. (2024). دور تطبيقات الذكاء الاصطناعي والتعلم الآلي في إدارة مخاطر المؤسسات الاقتصادية. *مجلة إدارة الأعمال والدراسات الاقتصادية*، مج10، ع2، 205 - 222. مسترجع من <http://search.mandumah.com/Record/1534182>
- بن التركي، زينب، موسى، سهام، و خالدي، فراح. (2021). دور التعلم الآلي في تحسين إدارة سلاسل التوريد اللوجستية. *مجلة العلوم الانسانية*، س21، ع2، 526 - 546. مسترجع من <http://search.mandumah.com/Record/1195620>
- شيت، عمر إبراهيم، و إبراهيم، لهيب محمد. (2023). تصميم وتنفيذ أداة التعلم الآلي لتقييم مخاطر الأمن السيبراني. *مجلة التربية والعلم*، مج32، ع2، 51 - 64. 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>