

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية: دراسة تطبيقية على شركات تقنية
المعلومات في المملكة العربية السعودية

اسم الطالب

روان فايز الشهري

الرقم الجامعي

232000926

مشروع تخرج - 1

كلية الإدارة - جامعة ميدأوشن

إشراف

د. عبدالرحيم نادر

عضو هيئة التدريس - كلية الإدارة - جامعة ميدأوشن

2026م

جدول المحتويات

1.	الفصل الأول: الإطار العام للدراسة.....	3
1.1.	المقدمة.....	4
1.2.	مشكلة الدراسة.....	7
1.2.1.	فجوات على المستوى النظري:.....	8
1.2.2.	فجوات على المستوى التطبيقي:.....	8
1.3.	أهمية الدراسة.....	9
1.3.1.	على المستوى النظري:.....	9
1.3.2.	على المستوى التطبيقي:.....	9
	المراجع:.....	11

1. الفصل الأول: الإطار العام للدراسة

1.1. المقدمة

يشهد العالم في العقود الأخيرة تحولاً رقمياً متسارعاً أدى إلى إعادة تشكيل بيئات الأعمال وأساليب الإدارة والإنتاج وتقديم الخدمات، حيث أصبحت التقنيات الرقمية والأنظمة الذكية جزءاً أساسياً من البنية التشغيلية للمؤسسات في مختلف القطاعات الاقتصادية. وقد أسهم هذا التحول في تعزيز كفاءة العمليات، ورفع الإنتاجية، وتحسين جودة الخدمات، وتسريع عملية اتخاذ القرار، إلا أنه في الوقت ذاته أدى إلى زيادة التحديات المرتبطة بأمن المعلومات والأمن السيبراني، نتيجة الاعتماد المتزايد على الأنظمة الرقمية، والحوسبة السحابية، وإنترنت الأشياء، والبيانات الضخمة، وتقنيات الذكاء الاصطناعي. ومع توسع استخدام هذه التقنيات، أصبحت المؤسسات، ولا سيما شركات تقنية المعلومات، أكثر عرضة للهجمات السيبرانية التي تستهدف البيانات والأنظمة الرقمية والبنية التحتية التقنية، مما جعل الأمن السيبراني أحد أهم الأولويات الاستراتيجية في العصر الرقمي.

ويشكل الذكاء الاصطناعي من أبرز التقنيات الحديثة التي أحدثت تحولاً نوعياً في مختلف المجالات، حيث أصبح يمثل أداة استراتيجية لتعزيز كفاءة المؤسسات وتحسين قدرتها على التعامل مع التحديات المعقدة. ويعتمد الذكاء الاصطناعي على مجموعة من الخوارزميات والنماذج الحاسوبية التي تمكن الأنظمة من التعلم من البيانات، والتعرف على الأنماط، والتنبؤ بالأحداث المستقبلية، واتخاذ القرارات بصورة تحاكي القدرات البشرية. وقد أدى التطور الكبير في تقنيات التعلم الآلي (Machine Learning)، والتعلم العميق (Deep Learning)، وتحليل البيانات الضخمة (Big Data Analytics)، إلى توسيع نطاق تطبيقات الذكاء الاصطناعي في مختلف القطاعات، ومن بينها قطاع الأمن السيبراني، الذي أصبح يعتمد بصورة متزايدة على الأنظمة الذكية للكشف عن التهديدات، وتحليل السلوكيات غير الطبيعية، والاستجابة للهجمات الإلكترونية في الوقت الفعلي.

ويشكل الأمن السيبراني أحد الركائز الأساسية لضمان استمرارية الأعمال الرقمية، وحماية الأصول المعلوماتية، والمحافظة على سرية البيانات وسلامتها وتوافرها. فمع تزايد الاعتماد على الخدمات الرقمية، ارتفعت معدلات الجرائم الإلكترونية، وتنوعت أساليب المهاجمين في استغلال الثغرات الأمنية، مما جعل الأساليب التقليدية للحماية غير كافية لمواجهة التهديدات الحديثة. ولذلك برزت الحاجة إلى توظيف تقنيات الذكاء الاصطناعي في تطوير أنظمة أمنية أكثر ذكاءً وقدرة على التنبؤ

بالمخاطر واكتشافها قبل وقوعها، وتحليل ملايين السجلات والبيانات في فترات زمنية قصيرة، والتعامل مع الهجمات الإلكترونية بصورة آلية وسريعة تقلل من حجم الأضرار والخسائر المحتملة.

تلعب شركات تقنية المعلومات دوراً محورياً في قيادة التحول الرقمي وتطوير الحلول التقنية التي تعتمد عليها المؤسسات الحكومية والخاصة، الأمر الذي يجعلها من أكثر القطاعات احتياجاً إلى أنظمة أمن سيبراني متقدمة. فهذه الشركات تتعامل مع كميات ضخمة من البيانات الحساسة، وتدير شبكات وأنظمة معلومات معقدة، وتوفر خدمات رقمية تعتمد عليها قطاعات حيوية مثل الصحة، والتعليم، والقطاع المالي، والطاقة، والتجارة الإلكترونية. ومن ثم، فإن تعرضها لأي اختراق أو هجوم سيبراني قد يؤدي إلى خسائر مالية وتشغيلية كبيرة، إضافة إلى الإضرار بسمعتها وفقدان ثقة العملاء. ومن هنا تبرز أهمية دمج تقنيات الذكاء الاصطناعي في منظومات الأمن السيبراني داخل شركات تقنية المعلومات، بما يساهم في تعزيز قدرتها على حماية أصولها الرقمية وضمان استمرارية خدماتها بكفاءة وأمان.

وقد أولت المملكة العربية السعودية اهتماماً بالغاً بتطوير منظومة الأمن السيبراني، انطلاقاً من إدراكها لأهمية حماية البنية التحتية الرقمية ودعم التحول الرقمي الوطني، وذلك في إطار مستهدفات رؤية المملكة العربية السعودية 2030، التي جعلت التحول الرقمي والابتكار التقني من أهم محاور التنمية الاقتصادية والاجتماعية. وقد انعكس هذا الاهتمام في إنشاء الجهات المختصة بالأمن السيبراني، ووضع الاستراتيجيات الوطنية، وإصدار الأطر التنظيمية والمعايير التي تهدف إلى رفع مستوى الجاهزية السيبرانية، وتعزيز حماية البيانات والأنظمة الرقمية في مختلف القطاعات. كما شجعت المملكة على تبني تطبيقات الذكاء الاصطناعي وتطوير الكفاءات الوطنية القادرة على توظيف هذه التقنيات في حماية الفضاء السيبراني، بما يعزز من مكانتها الإقليمية والعالمية في مجالات الأمن الرقمي والابتكار التقني.

وتتميز تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني بقدرتها على تحليل كميات هائلة من البيانات بصورة مستمرة، والتعرف على الأنماط غير الطبيعية التي قد تشير إلى محاولات اختراق أو نشاطات ضارة، إضافة إلى قدرتها على التنبؤ بالهجمات المستقبلية اعتماداً على تحليل البيانات التاريخية والسلوكيات الرقمية. كما تساهم هذه التقنيات في أتمتة العديد من العمليات الأمنية، مثل اكتشاف البرمجيات الخبيثة، وتحليل الثغرات الأمنية، وإدارة المخاطر، والاستجابة للحوادث

السيبرانية، مما يقلل من زمن الاستجابة، ويرفع مستوى الكفاءة التشغيلية، ويحد من الأخطاء البشرية التي قد تؤثر في فعالية أنظمة الحماية.

وعلى الرغم من المزايا الكبيرة التي يوفرها الذكاء الاصطناعي في مجال الأمن السيبراني، فإن تطبيقه داخل شركات تقنية المعلومات يواجه عدداً من التحديات، من أبرزها ارتفاع تكاليف الاستثمار في الحلول الذكية، والحاجة إلى بيانات عالية الجودة لتدريب النماذج، ونقص الكفاءات المتخصصة، بالإضافة إلى التحديات الأخلاقية والقانونية المرتبطة باستخدام الأنظمة الذكية في تحليل البيانات واتخاذ القرارات الأمنية. كما أن التطور المستمر في أساليب الهجمات الإلكترونية يفرض ضرورة تحديث خوارزميات الذكاء الاصطناعي بصورة دائمة، لضمان قدرتها على مواكبة التهديدات السيبرانية المتغيرة والحفاظ على فعاليتها في بيئات الأعمال الرقمية.

تشير الأدبيات الحديثة إلى وجود علاقة وثيقة بين مستوى تبني تقنيات الذكاء الاصطناعي وكفاءة منظومات الأمن السيبراني، حيث تسهم هذه التقنيات في تحسين سرعة اكتشاف التهديدات، وتقليل زمن الاستجابة للحوادث، وتعزيز دقة تحليل المخاطر، ورفع مستوى الاعتمادية في حماية الأنظمة الرقمية. كما أن التكامل بين الذكاء الاصطناعي والأمن السيبراني أصبح يمثل توجهاً استراتيجياً لدى المؤسسات التقنية الرائدة، لما يوفره من مزايا تنافسية تتمثل في تعزيز الثقة الرقمية، وتحسين جودة الخدمات، وتقليل الخسائر الناتجة عن الجرائم الإلكترونية، ودعم استدامة الأعمال في ظل بيئة تقنية تتسم بالتغير المستمر.

تأتي هذه الدراسة بهدف استكشاف الدور الذي تؤديه تطبيقات الذكاء الاصطناعي في رفع مستوى الأمن السيبراني داخل المشاريع الرقمية، وتحليل مدى إسهامها في تحسين قدرات الكشف المبكر عن التهديدات، والاستجابة الفعالة للهجمات الإلكترونية، وإدارة المخاطر السيبرانية، وتعزيز استمرارية الأعمال الرقمية. كما تسعى الدراسة إلى تقديم إطار علمي وتطبيقي يمكن أن يسهم في دعم صناع القرار ومديري شركات تقنية المعلومات عند تطوير استراتيجيات الأمن السيبراني، وتوسيع نطاق توظيف تقنيات الذكاء الاصطناعي بما يتوافق مع مستهدفات رؤية المملكة العربية السعودية 2030، ويعزز من بناء بيئة رقمية آمنة ومستدامة تدعم الابتكار والتحول الرقمي والاقتصاد المعرفي.

1.2. مشكلة الدراسة

يشهد قطاع تقنية المعلومات في المملكة العربية السعودية نمواً متسارعاً مدفوعاً بالتوسع في مشاريع التحول الرقمي، والحوسبة السحابية، والذكاء الاصطناعي، وإنترنت الأشياء، والاعتماد المتزايد على الخدمات الرقمية في مختلف القطاعات الحكومية والخاصة. وقد أسهم هذا التحول في تعزيز كفاءة الأعمال ورفع مستوى الابتكار، إلا أنه في المقابل أدى إلى زيادة حجم التهديدات السيبرانية وتعقيدها، حيث أصبحت الهجمات الإلكترونية أكثر تطوراً وقدرة على استهداف الأنظمة الرقمية والبنى التحتية الحيوية، الأمر الذي يفرض على شركات تقنية المعلومات تبني حلول أمنية متقدمة قادرة على مواجهة هذه التهديدات بصورة استباقية. وعلى الرغم من التطور الذي شهدته أدوات الأمن السيبراني التقليدية، فإنها لم تعد كافية للتعامل مع الهجمات الحديثة التي تعتمد على تقنيات متطورة وسريعة التغير، وهو ما أدى إلى تزايد الاهتمام بتطبيقات الذكاء الاصطناعي باعتبارها من أهم التقنيات القادرة على تعزيز قدرات الكشف المبكر عن التهديدات، وتحليل البيانات الأمنية، والاستجابة الذكية للحوادث السيبرانية.

ورغم إدراك المؤسسات السعودية لأهمية الذكاء الاصطناعي في تعزيز الأمن السيبراني، إلا أن مستوى توظيف هذه التقنيات لا يزال متفاوتاً بين شركات تقنية المعلومات، كما تختلف درجة الاستفادة منها في حماية المشاريع الرقمية وإدارة المخاطر السيبرانية. ويضاف إلى ذلك وجود تحديات متعددة، مثل ارتفاع تكاليف تطبيق الحلول الذكية، ونقص الكفاءات المتخصصة، وتعقيد دمج تقنيات الذكاء الاصطناعي مع البنى الأمنية القائمة، فضلاً عن التحديات المرتبطة بجودة البيانات والحوكمة والخصوصية. ومن ثم تمثل مشكلة الدراسة في الحاجة إلى التعرف بصورة علمية على مدى إسهام تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية داخل شركات تقنية المعلومات في المملكة العربية السعودية، وقياس طبيعة العلاقة بين تبني هذه التقنيات ومستوى فعالية الأمن السيبراني، بما يسهم في تقديم نتائج علمية تساعد صناعات القرار على تطوير استراتيجيات الحماية الرقمية، وتعزيز جاهزية المؤسسات لمواجهة التهديدات السيبرانية المتنامية.

1.2.1. فجوات على المستوى النظري:

تشير مراجعة الأدبيات العلمية إلى وجود اهتمام متزايد بدراسة الذكاء الاصطناعي والأمن السيبراني كلٌّ على حدة، إلا أن الدراسات التي تناولت العلاقة المباشرة بين تطبيقات الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية ما تزال محدودة، وخاصة في البيئة السعودية. كما ركزت العديد من الدراسات السابقة على الجوانب التقنية البحتة المتعلقة بخوارزميات التعلم الآلي أو أساليب اكتشاف الهجمات الإلكترونية، دون تقديم إطار نظري متكامل يفسر كيفية إسهام تطبيقات الذكاء الاصطناعي في رفع كفاءة الأمن السيبراني من منظور إداري وتنظيمي داخل شركات تقنية المعلومات. كذلك، فإن عدداً من الدراسات اعتمد على نماذج نظرية طُبِّقت في بيئات اقتصادية وتقنية تختلف عن البيئة السعودية، الأمر الذي يحد من إمكانية تعميم نتائجها على قطاع تقنية المعلومات في المملكة.

وتتمثل فجوة نظرية أخرى في محدودية الدراسات التي تناولت الأمن السيبراني باعتباره متغيراً متعدد الأبعاد يتأثر بمجموعة من العوامل المرتبطة بالذكاء الاصطناعي، مثل قدرة الأنظمة الذكية على الكشف المبكر عن التهديدات، والاستجابة الآلية للحوادث، وتحليل المخاطر، ودعم اتخاذ القرار الأمني. كما أن التطورات الحديثة في الذكاء الاصطناعي التوليدي، والتحليلات التنبؤية، والتعلم العميق، لم تحظَ بالاهتمام الكافي في تفسير أثرها على فعالية الأمن السيبراني داخل المشاريع الرقمية، وهو ما يبرز الحاجة إلى دراسة حديثة تسهم في بناء إطار معرفي متكامل يوضح طبيعة العلاقة بين هذه المتغيرات، ويثري الأدبيات العربية والسعودية في هذا المجال.

1.2.2. فجوات على المستوى التطبيقي:

على المستوى التطبيقي، ما زالت العديد من شركات تقنية المعلومات في المملكة العربية السعودية تواجه تحديات في التطبيق الفعلي لتقنيات الذكاء الاصطناعي في منظومات الأمن السيبراني، على الرغم من التطور الذي تشهده البنية الرقمية الوطنية. ويظهر ذلك في تفاوت مستويات النضج الرقمي والأمني بين الشركات، واختلاف قدراتها على دمج الحلول الذكية في أنظمة الحماية، فضلاً عن محدودية الاستثمار في التقنيات المتقدمة، ونقص الكفاءات البشرية المتخصصة في مجالي الذكاء الاصطناعي والأمن السيبراني. كما تعتمد بعض الشركات بصورة كبيرة على أدوات أمنية تقليدية تعتمد على التحديثات الدورية وقواعد البيانات الثابتة، مما يقلل من قدرتها على التعامل مع الهجمات الإلكترونية المتطورة التي تتغير بصورة مستمرة.

ومن جانب آخر، لا تزال الأدلة التطبيقية التي توضح حجم تأثير تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية داخل شركات تقنية المعلومات السعودية محدودة، الأمر الذي يصعب معه تحديد أكثر التطبيقات الذكية فاعلية في تحسين مستوى الحماية وتقليل المخاطر الإلكترونية. كما توجد حاجة إلى نتائج ميدانية تساعد الجهات الحكومية، والشركات التقنية، ومطوري الحلول الأمنية على بناء استراتيجيات أكثر كفاءة في توظيف الذكاء الاصطناعي، وتحديد أولويات الاستثمار في هذا المجال، ووضع برامج تدريب وتأهيل تستهدف رفع جاهزية الكوادر الوطنية، وتعزيز مرونة المشاريع الرقمية في مواجهة التهديدات السيبرانية، بما يتوافق مع مستهدفات رؤية المملكة العربية السعودية 2030.

1.3. أهمية الدراسة

1.3.1. على المستوى النظري:

تنبع الأهمية النظرية لهذه الدراسة من كونها تسهم في إثراء الأدبيات العلمية العربية والأجنبية المتعلقة بالذكاء الاصطناعي والأمن السيبراني، من خلال تقديم إطار علمي يوضح العلاقة بين تطبيقات الذكاء الاصطناعي ومستوى تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات. كما تعمل الدراسة على دمج المفاهيم الحديثة في الذكاء الاصطناعي، مثل التعلم الآلي، والتعلم العميق، والتحليلات التنبؤية، مع مفاهيم الأمن السيبراني، بما يتيح بناء نموذج نظري متكامل يفسر تأثير هذه التقنيات في حماية الأنظمة الرقمية وإدارة المخاطر الإلكترونية. وإضافة إلى ذلك، تسهم الدراسة في سد جانب من الفجوة البحثية المتعلقة بالبيئة السعودية، وتوفر مرجعاً علمياً يمكن للباحثين الاستناد إليه في إجراء دراسات مستقبلية تتناول تطبيقات الذكاء الاصطناعي في مجالات الأمن الرقمي والتحول التقني وإدارة المخاطر.

1.3.2. على المستوى التطبيقي:

تكتسب الدراسة أهمية تطبيقية كبيرة لما يمكن أن تقدمه من نتائج وتوصيات عملية تساعد شركات تقنية المعلومات في المملكة العربية السعودية على تطوير استراتيجيات الأمن السيبراني بالاعتماد على تطبيقات الذكاء الاصطناعي، ورفع مستوى قدرتها على اكتشاف التهديدات الإلكترونية، وتحليل المخاطر، والاستجابة السريعة للحوادث السيبرانية، وتقليل الخسائر الناتجة

عن الهجمات الرقمية. كما يمكن أن تستفيد الجهات الحكومية، والهيئات التنظيمية، وصناع القرار، ومراكز الأمن السيبراني، ومطورو الحلول التقنية من نتائج الدراسة عند وضع السياسات والخطط الوطنية الرامية إلى تعزيز الحماية الرقمية، وتطوير الكفاءات البشرية، وتشجيع الاستثمار في التقنيات الذكية. كذلك، تسهم الدراسة في دعم تحقيق مستهدفات رؤية المملكة العربية السعودية 2030 من خلال تعزيز التحول الرقمي الأمن، وزيادة موثوقية المشاريع الرقمية، وبناء بيئة تقنية أكثر مرونة وقدرة على مواجهة التهديدات السيبرانية المتزايدة، بما يعزز التنافسية والابتكار والاستدامة في قطاع تقنية المعلومات.

المراجع:

- المراجع العربية

1. الهيئة الوطنية للأمن السيبراني. (2023). *الضوابط الأساسية للأمن السيبراني*. (ECC-2:2023) الرياض، المملكة العربية السعودية.
2. الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2023). *الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي*. الرياض، المملكة العربية السعودية.
3. الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2024). *تقرير الذكاء الاصطناعي في المملكة العربية السعودية*. الرياض، المملكة العربية السعودية.

- المراجع الأجنبية

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
2. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
3. National Institute of Standards and Technology. (2024). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce.
4. Northouse, P. G. (2022). *Leadership: Theory and practice* (9th ed.). Sage Publications.
5. Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
6. ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. International Organization for Standardization.