

عنوان الرسالة:

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

اسم الطالبة/

روان فايز الشهري

الرقم الجامعي

232000926

مشروع تخرج - 2

كلية الإدارة - جامعة ميدأوشن

إشراف

د. عبد الرحيم 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:	9
1.3.	أهمية الدراسة	10
1.3.1.	على المستوى النظري:	10
1.3.2.	على المستوى التطبيقي:	10
1.4.	أسئلة الدراسة:	11
1.5.	أهداف الدراسة:	11
1.6.	فرضيات الدراسة	12
1.7.	نموذج الدراسة	14
1.8.	منهجية الدراسة	14
1.9.	الدراسة الميدانية	18
1.10.	مخطط المشروع المقترح	20
2.	الفصل الثاني: الدراسات السابقة	22
2.1.	المقدمة:	23
2.2.	المتغيرات المستقلة:	24
2.3.	المتغير التابع:	26
2.4.	العلاقة بين المتغير المستقل والمتغير التابع:	27
2.5.	الخاتمة:	27
	المراجع	29
4.	الملاحق:	32
4.1.	ملحق (أ): الاستبيان	33

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 (Shao، 2025).

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 (Bhatele، 2019).

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 (Sharma، 2024).

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 سيرياني 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 سيرياني 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 السيرياني داخل شركات تقنية المعلومات، بما يساهم في تعزيز قدرتها على حماية أصولها الرقمية وضمان استمرارية خدماتها بكفاءة وأمان (Jerab، 2024).

وقد أولت المملكة العربية السعودية اهتماماً بالغاً بتطوير منظومة الأمن السيرياني، 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 السيرياني، ووضع الاستراتيجيات الوطنية، وإصدار الأطر التنظيمية والمعايير التي تهدف إلى رفع مستوى الجاهزية السيريانية، 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 السيرياني، بما يعزز من مكانتها الإقليمية والعالمية في مجالات الأمن الرقمي والابتكار التقني (Elbehairy، 2025).

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 تسهم 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 (Steiti، 2024).

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 (Folorunso، 2024).

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 (Cadet، 2024).

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 يساهم 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 (Jada، 2024).

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 (Abaker، 2026).

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 تتمثل 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 صناع القرار على تطوير استراتيجيات الحماية الرقمية، وتعزيز جاهزية المؤسسات لمواجهة التهديدات السيبرانية المتنامية (Geaiger، 2026).

1.2.1. فجوات على المستوى النظري:

تشير مراجعة الأدبيات العلمية إلى وجود اهتمام متزايد بدراسة الذكاء الاصطناعي والأمن السيبراني كل 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 طُبقت في بيئات اقتصادية وتقنية تختلف عن البيئة السعودية، الأمر الذي يحد من إمكانية تعميم نتائجها على قطاع تقنية المعلومات في المملكة (AL-Khassawneh، 2022).

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 (Khadka, 2025).

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 (Mufleh, 2026).

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 (Almaqtari, 2026).

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 (Kaur، 2023).

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 للأمن، وزيادة موثوقية المشاريع الرقمية، وبناء بيئة تقنية أكثر مرونة وقدرة على مواجهة التهديدات السيبرانية المتزايدة، بما يعزز التنافسية والابتكار والاستدامة في قطاع تقنية المعلومات (Abudaqqa، 2025).

1.4. أسئلة الدراسة:

التساؤل الرئيسي للدراسة

ما دور الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات في المملكة العربية السعودية؟

الأسئلة الفرعية

1. ما أثر استخدام تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية على تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية؟
2. ما أثر الاستجابة الذكية والآلية للحوادث السيبرانية باستخدام تطبيقات الذكاء الاصطناعي على تعزيز الأمن السيبراني للمشاريع الرقمية؟
3. ما أثر تحليل البيانات الأمنية والتنبؤ بالمخاطر السيبرانية باستخدام الذكاء الاصطناعي على تعزيز الأمن السيبراني للمشاريع الرقمية؟
4. ما أثر أتمتة العمليات الأمنية باستخدام تطبيقات الذكاء الاصطناعي على رفع كفاءة الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات؟
5. ما أثر دعم اتخاذ القرارات الأمنية باستخدام تقنيات الذكاء الاصطناعي على تعزيز الأمن السيبراني للمشاريع الرقمية في المملكة العربية السعودية؟

1.5. أهداف الدراسة:

الهدف الرئيسي للدراسة

التعرف على دور الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات في المملكة العربية السعودية.

الأهداف الفرعية

1. قياس أثر استخدام تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية على تعزيز الأمن السيبراني للمشاريع الرقمية.
2. التعرف على أثر الاستجابة الذكية والآلية للحوادث السيبرانية باستخدام الذكاء الاصطناعي على مستوى الأمن السيبراني للمشاريع الرقمية.
3. تحليل أثر تحليل البيانات الأمنية والتنبؤ بالمخاطر السيبرانية باستخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية.
4. قياس أثر أتمتة العمليات الأمنية باستخدام تطبيقات الذكاء الاصطناعي على كفاءة الأمن السيبراني للمشاريع الرقمية.
5. تحديد أثر دعم اتخاذ القرارات الأمنية باستخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية.

1.6. فرضيات الدراسة

الفرضية الرئيسية للدراسة

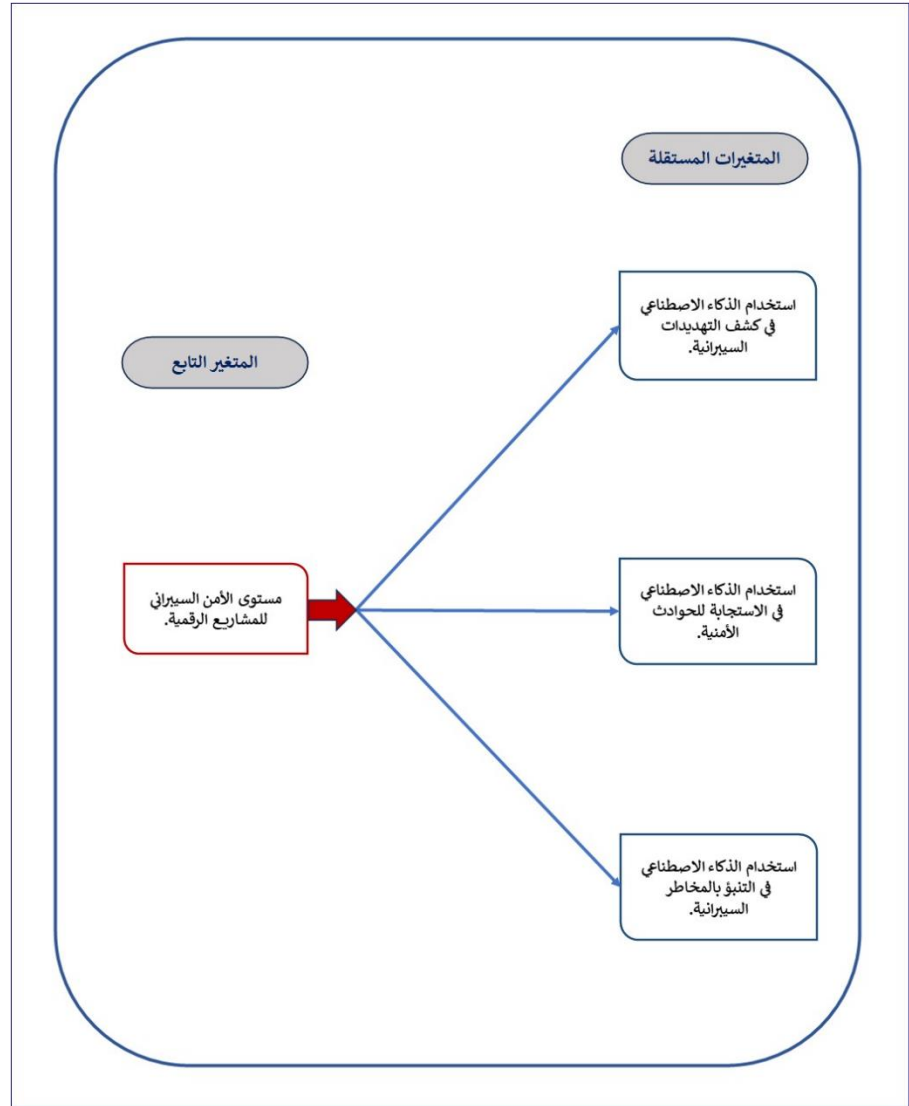
توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين تطبيقات الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية.

الفرضيات الفرعية

1. توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين استخدام تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية وتعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية.

2. توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستجابة الذكية والآلية للحوادث السيبرانية باستخدام الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية.
3. توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين تحليل البيانات الأمنية والتنبيه بالمخاطر السيبرانية باستخدام الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية.
4. توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين أتمتة العمليات الأمنية باستخدام تطبيقات الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية.
5. توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين دعم اتخاذ القرارات الأمنية باستخدام تقنيات الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية.

1.7. نموذج الدارسة



المصدر: إعداد الباحث

1.8. منهجية الدارسة

تعتمد هذه الدارسة على المنهجية الكمية (Quantitative Research Methodology) باعتبارها المنهجية الأكثر ملاءمة لتحقيق أهداف الدارسة والإجابة عن تساؤلاتها واختبار فرضياتها، وذلك لكونها تستهدف قياس أثر تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة

العربية السعودية من خلال بيانات رقمية قابلة للتحليل الإحصائي. وتقوم المنهجية الكمية على جمع البيانات بصورة منظمة باستخدام أدوات قياس مقننة، ثم تحليلها باستخدام الأساليب الإحصائية المناسبة لاستخلاص النتائج العلمية المتعلقة بالعلاقات بين المتغيرات، وهو ما يحقق مستوى مرتفعاً من الموضوعية والدقة في تفسير الظواهر الإدارية والتقنية. كما تُعد هذه المنهجية من أكثر المناهج استخداماً في الدراسات الإدارية والتقنية الحديثة، لما توفره من إمكانية اختبار النماذج البحثية وقياس قوة التأثير بين المتغيرات بصورة علمية يمكن تعميم نتائجها على مجتمع الدراسة.

وتنسجم المنهجية الكمية مع طبيعة الدراسة الحالية التي تعتمد على نموذج يتضمن متغيراً تابعاً وثلاثة متغيرات مستقلة، حيث تهدف الدراسة إلى قياس مستوى تبني تطبيقات الذكاء الاصطناعي داخل شركات تقنية المعلومات، وتحليل مدى تأثيرها في تعزيز الأمن السيبراني للمشاريع الرقمية. ولذلك تعتمد الدراسة على استبانة علمية يتم تصميمها وفق مقياس ليكرت الخماسي، بحيث تتيح قياس اتجاهات أفراد العينة نحو متغيرات الدراسة وتحويلها إلى بيانات رقمية قابلة للتحليل باستخدام البرامج الإحصائية المتخصصة مثل SPSS، بما يسمح باستخراج نتائج دقيقة تدعم اختبار الفرضيات وتقديم توصيات علمية قائمة على الأدلة.

- المنهج الكمي (Quantitative Research)

يعتمد البحث على المنهج الكمي بوصفه منهجاً علمياً يقوم على القياس والتحليل الإحصائي للبيانات، ويهدف إلى اختبار الفرضيات وتحديد طبيعة العلاقات بين المتغيرات بصورة موضوعية. ويتميز هذا المنهج بالاعتماد على البيانات الرقمية التي يتم جمعها من عدد كبير من أفراد مجتمع الدراسة باستخدام أدوات قياس موحدة، الأمر الذي يساهم في تقليل التحيز الشخصي وزيادة دقة النتائج. كما يسمح المنهج الكمي بقياس درجة تأثير كل متغير مستقل في المتغير التابع، وتحديد مستوى الدلالة الإحصائية لهذه العلاقات، وهو ما يجعله مناسباً للدراسات التطبيقية التي تتناول موضوعات الأمن السيبراني والذكاء الاصطناعي.

وفي الدراسة الحالية، يوفر المنهج الكمي إطاراً علمياً مناسباً لقياس مدى إسهام تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية داخل شركات تقنية المعلومات في المملكة العربية السعودية، من خلال جمع البيانات من أصحاب القرار والمتخصصين والعاملين في المجال التقني وتحليلها بصورة كمية. كما يساعد

هذا المنهج في بناء استنتاجات دقيقة يمكن تعميمها على مجتمع الدراسة في ضوء الأساليب العلمية المستخدمة في اختيار العينة وتحليل البيانات، مما يعزز من القيمة العلمية للدراسة ويزيد من موثوقية نتائجها.

- التصميم البحثي

تعتمد الدراسة التصميم الوصفي التحليلي في إطار المنهجية الكمية، حيث يجمع هذا التصميم بين وصف الظاهرة المدروسة وتحليل العلاقات القائمة بين متغيراتها. ويهدف الجانب الوصفي إلى التعرف على مستوى استخدام تطبيقات الذكاء الاصطناعي في شركات تقنية المعلومات، ومستوى الأمن السيبراني للمشاريع الرقمية، بينما يركز الجانب التحليلي على قياس أثر تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني، واختبار الفرضيات التي بنيت عليها الدراسة.

ويُعد هذا التصميم مناسباً لطبيعة الدراسة، لأنه لا يقتصر على وصف واقع استخدام تقنيات الذكاء الاصطناعي، وإنما يتجاوز ذلك إلى تحليل تأثيرها في الأمن السيبراني، وتفسير النتائج في ضوء الأدبيات العلمية والنظريات ذات العلاقة. كما يساعد التصميم الوصفي التحليلي في بناء نموذج علمي يوضح طبيعة العلاقة بين المتغيرات، ويقدم أدلة كمية تدعم الاستنتاجات والتوصيات التي ستتوصل إليها الدراسة.

- أداة جمع البيانات

تعتمد الدراسة على الاستبانة (Questionnaire) باعتبارها الأداة الرئيسة لجمع البيانات، لما تتميز به من قدرة على الوصول إلى عدد كبير من أفراد العينة خلال فترة زمنية مناسبة، وسهولة تحليل بياناتها باستخدام البرامج الإحصائية. وقد تم تصميم الاستبانة في ضوء الأدبيات العلمية والدراسات السابقة ذات الصلة، بحيث تتضمن مجموعة من العبارات التي تقيس أبعاد تطبيقات الذكاء الاصطناعي، إلى جانب مجموعة أخرى تقيس مستوى تعزيز الأمن السيبراني للمشاريع الرقمية.

وقد صيغت جميع فقرات الاستبانة باستخدام مقياس ليكرت الخماسي، الذي يتيح للمشاركين التعبير عن درجة موافقتهم على العبارات المطروحة، بدءاً من (أوافق بشدة) وحتى (لا أوافق بشدة). ويساعد هذا المقياس في تحويل الاتجاهات والآراء إلى بيانات كمية دقيقة يمكن تحليلها إحصائياً. كما سيتم عرض الاستبانة على

مجموعة من المحكمين المتخصصين للتأكد من صدقها الظاهري، بالإضافة إلى اختبار ثباتها باستخدام معامل ألفا كرونباخ لضمان الاتساق الداخلي لفقراتها.

- أسلوب تحليل البيانات

بعد الانتهاء من جمع البيانات، سيتم مراجعتها وترميزها وإدخالها إلى برنامج SPSS لإجراء عمليات التحليل الإحصائي. وسيتم استخدام الإحصاء الوصفي لاستخراج التكرارات، والنسب المئوية، والمتوسطات الحسابية، والانحرافات المعيارية، بهدف وصف خصائص أفراد العينة ومستويات استجاباتهم تجاه متغيرات الدراسة. كما ستستخدم مجموعة من الأساليب الإحصائية الاستدلالية لاختبار فرضيات الدراسة، من أبرزها معامل ارتباط بيرسون لقياس قوة واتجاه العلاقة بين المتغيرات، وتحليل الانحدار الخطي المتعدد لقياس أثر المتغيرات المستقلة في المتغير التابع، إضافة إلى اختبار (T-Test) وتحليل التباين الأحادي (One-Way ANOVA) عند الحاجة لدراسة الفروق بين استجابات أفراد العينة وفقاً للخصائص الديموغرافية. وتوفر هذه التحليلات مؤشرات علمية دقيقة تساعد في تفسير النتائج والوصول إلى استنتاجات موثوقة.

- مبررات اختيار المنهجية الكمية

تم اختيار المنهجية الكمية لأنها تتوافق مع طبيعة الدراسة التي تسعى إلى اختبار فرضيات محددة وقياس العلاقة بين تطبيقات الذكاء الاصطناعي وتعزيز الأمن السيبراني للمشاريع الرقمية باستخدام بيانات رقمية قابلة للتحليل الإحصائي. كما تتميز هذه المنهجية بالموضوعية، والدقة، والقدرة على قياس حجم التأثير بين المتغيرات، وإنتاج نتائج قابلة للتعميم عند اختيار العينة وفق الأساليب العلمية المناسبة.

إضافة إلى ذلك، تسمح المنهجية الكمية بإجراء مقارنات علمية بين نتائج الدراسة الحالية والدراسات السابقة، وتوفير أساساً قوياً لاتخاذ القرارات المبنية على الأدلة، سواء على مستوى شركات تقنية المعلومات أو الجهات التنظيمية وصناع السياسات. ومن ثم، فإن اعتماد هذه المنهجية يساهم في تحقيق أهداف الدراسة بكفاءة، ويعزز من موثوقية نتائجها، ويزيد من إمكانية الاستفادة منها في تطوير استراتيجيات الأمن السيبراني وتوسيع نطاق توظيف الذكاء الاصطناعي داخل المشاريع الرقمية في المملكة العربية السعودية.

1.9. الدراسة الميدانية

تمثل الدراسة الميدانية الجانب التطبيقي للدراسة الحالية، حيث تهدف إلى جمع البيانات الواقعية من أفراد مجتمع الدراسة وتحليلها للتحقق من صحة الفرضيات والإجابة عن تساؤلات البحث، وقياس أثر تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالملكة العربية السعودية. وتُعد الدراسة الميدانية مرحلة أساسية في البحث العلمي، لأنها تتيح اختبار النموذج النظري في بيئة العمل الفعلية، وربط المفاهيم الأكاديمية بالممارسات التطبيقية، مما يساهم في الوصول إلى نتائج دقيقة تعكس واقع استخدام تقنيات الذكاء الاصطناعي في المؤسسات التقنية السعودية، ومدى إسهامها في رفع مستوى الحماية السيبرانية للمشاريع الرقمية.

واعتمدت الدراسة الميدانية على المنهج الكمي باستخدام الاستبانة كأداة رئيسة لجمع البيانات، حيث تم إعدادها في ضوء الأدبيات العلمية والدراسات السابقة، بما يضمن قياس المتغيرات بصورة دقيقة وشاملة. وتضمنت الاستبانة مجموعة من الفقرات التي تقيس أبعاد تطبيقات الذكاء الاصطناعي، وهي: الكشف المبكر عن التهديدات السيبرانية، والاستجابة الذكية وإدارة الحوادث السيبرانية، وتحليل البيانات الأمنية ودعم اتخاذ القرار، بالإضافة إلى مجموعة من الفقرات التي تقيس مستوى تعزيز الأمن السيبراني للمشاريع الرقمية. وتم استخدام مقياس ليكرت الخماسي لقياس اتجاهات أفراد العينة، لما يتمتع به من دقة ومرونة في تحويل الآراء إلى بيانات كمية قابلة للتحليل الإحصائي.

ويستهدف مجتمع الدراسة العاملين في شركات تقنية المعلومات بالملكة العربية السعودية، وبصفة خاصة المديرين التنفيذيين، ومديري الأمن السيبراني، ومديري تقنية المعلومات، ومهندسي الأمن السيبراني، ومطوري الأنظمة، والمختصين في تطبيقات الذكاء الاصطناعي، باعتبارهم الأكثر ارتباطاً بموضوع الدراسة والأقدر على تقييم مستوى استخدام تقنيات الذكاء الاصطناعي ودورها في تعزيز الأمن السيبراني للمشاريع الرقمية. ويساهم تنوع أفراد العينة في توفير بيانات أكثر شمولاً، تعكس واقع الممارسات الأمنية والتقنية داخل الشركات، وتدعم دقة النتائج وإمكانية تعميمها.

وروعي في تنفيذ الدراسة الميدانية الالتزام بالمعايير الأخلاقية للبحث العلمي، حيث تم توضيح أهداف الدراسة للمشاركين، والتأكيد على أن المعلومات التي يتم جمعها ستستخدم لأغراض البحث العلمي فقط، مع ضمان سرية البيانات وعدم الإفصاح عن هوية المشاركين أو شركاتهم. كما اعتمدت الدراسة على مبدأ المشاركة الطوعية، بما يعزز من صدق الاستجابات ويزيد من موثوقية البيانات التي سيتم تحليلها.

وبعد الانتهاء من جمع الاستبانات، سيتم فحصها للتأكد من اكتمالها وصلاحيتها للتحليل، واستبعاد أي استبانات غير مكتملة أو غير صالحة. ثم تُرمز البيانات وتُدخل إلى برنامج SPSS لإجراء التحليلات الإحصائية اللازمة، حيث تستخدم الإحصاءات الوصفية لعرض خصائص العينة ومستويات استجاباتها، بينما تستخدم الاختبارات الاستدلالية، مثل معامل ارتباط بيرسون وتحليل الانحدار الخطي المتعدد، لاختبار الفرضيات وقياس أثر المتغيرات المستقلة في المتغير التابع، إلى جانب اختبار (T-Test) وتحليل التباين الأحادي عند الحاجة.

كما تتضمن الدراسة الميدانية التحقق من جودة أداة القياس من خلال اختبار الصدق والثبات، إذ تُعرض الاستبانة على عدد من المحكمين المتخصصين في الذكاء الاصطناعي والأمن السيبراني والإدارة وتقنية المعلومات للتأكد من ملاءمة الفقرات وارتباطها بمتغيرات الدراسة، كما يُحسب معامل ألفا كرونباخ (Cronbach's Alpha) للتحقق من الاتساق الداخلي لفقرات الاستبانة وضمان ثباتها. وتسهم هذه الإجراءات في تعزيز جودة البيانات وزيادة الثقة في النتائج النهائية.

وتمثل نتائج الدراسة الميدانية الأساس الذي تُبنى عليه مناقشة النتائج واستخلاص الاستنتاجات والتوصيات، حيث ستوضح مدى تأثير تطبيقات الذكاء الاصطناعي في رفع مستوى الأمن السيبراني للمشاريع الرقمية، وتحدد أكثر التطبيقات فاعلية في تعزيز الحماية الإلكترونية داخل شركات تقنية المعلومات. كما ستوفر النتائج مؤشرات علمية وعملية يمكن أن تستفيد منها الشركات التقنية، والهيئة الوطنية للأمن السيبراني، وصناع القرار، ومطورو الحلول الذكية عند تصميم استراتيجيات الأمن الرقمي، وتطوير الأنظمة الذكية، ورفع جاهزية المؤسسات لمواجهة التهديدات السيبرانية، بما يدعم مستهدفات رؤية المملكة العربية السعودية 2030 في بناء اقتصاد رقمي آمن، وتعزيز الابتكار، وتحقيق الاستفادة في قطاع تقنية المعلومات.

1.10. مخطط المشروع المقترح

المرحلة	الأنشطة الرئيسية	الأهداف	المدة الزمنية	المخرجات المتوقعة
التحضير والتخطيط	مراجعة الأدبيات والمراجع العلمية	وضع خطة واضحة ومنهجية للدراسة	0.5 شهر	خطة بحثية مفصلة مع جدول زمني
	تحديد أدوات جمع البيانات	تصميم الاستبانة وأدوات القياس		أدوات جمع بيانات جاهزة للاستخدام
	التنسيق مع الجهات المشاركة	الحصول على الموافقات اللازمة		موافقات رسمية من المؤسسات المشاركة
جمع البيانات	توزيع الاستبانة على المشاركين	جمع بيانات ميدانية دقيقة وموثوقة	1 شهر	مجموعة بيانات مكتملة وصحيحة
	إجراء مقابلات مع خبراء مختارين	تعميق الفهم حول التحديات والفرص		ملاحظات ومعلومات نوعية داعمة
تحليل البيانات	تنظيف وترتيب البيانات	التأكد من جودة البيانات ودقتها	1 شهر	بيانات جاهزة للتحليل

استخدام البرامج الإحصائية (SPSS) وغيرها	اختبار الفرضيات وتحليل العلاقات بين المتغيرات		نتائج إحصائية تدعم أو ترفض الفرضيات
إعداد الرسوم البيانية والتقارير التحليلية	توضيح النتائج وتفسيرها		جداول ورسوم بيانية وتفسيرية مفصلة
إعداد التقرير النهائي	صياغة نتائج الدراسة والتوصيات	تقديم بحث متكامل وموثق	تقرير نهائي متكامل يشمل كافة أجزاء الدراسة
مراجعة التقرير وتنقيحه	ضمان دقة وسلاسة المحتوى		تقرير معد للنشر أو العرض
عرض النتائج	تقديم العرض في مؤتمرات أو ورش عمل	نشر المعرفة والاستفادة العملية	عرض تقديمي شامل + ملاحظات وردود فعل من الجمهور
مناقشة نتائج الدراسة مع الجهات المعنية	الحصول على تقييمات وملاحظات لتحسين البحث		مخرجات نقاشية تعزز من جودة البحث وتطبيقه المستقبلي

2. الفصل الثاني: الدراسات السابقة

2.1. المقدمة:

يشكل الفصل الثاني من الدراسة الإطار النظري الذي تستند إليه جميع المراحل اللاحقة للبحث، إذ يمثل الركيزة العلمية التي تُبنى عليها مشكلة الدراسة، وتسؤلاتها، وفرضياتها، ونموذجها البحثي. وتنبع أهمية هذا الفصل من كونه يقدم معالجة علمية منهجية للمفاهيم والنظريات والأدبيات الحديثة المرتبطة بموضوع الدراسة، بما يساهم في تكوين قاعدة معرفية راسخة تساعد على فهم الظاهرة محل البحث بصورة شاملة ومتعمقة. كما يهدف هذا الفصل إلى توضيح الأسس الفكرية التي تناولتها المدارس الإدارية والتقنية الحديثة في تفسير موضوع الدراسة، مع الاستفادة من نتائج البحوث والدراسات السابقة التي تناولت الموضوع من زوايا متعددة، بما يعزز من قوة البناء النظري للدراسة ويمنحها بعداً علمياً ينسجم مع التطورات المتسارعة في مجالات الذكاء الاصطناعي والأمن السيبراني والتحول الرقمي.

ويتناول هذا الفصل عرضاً تفصيلياً لمتغيرات الدراسة من خلال استعراض مفاهيمها، وأبعادها، وخصائصها، وأهم النظريات والنماذج التي تناولتها الأدبيات العلمية، مع تحليلها بصورة نقدية تربط بين الجوانب النظرية والتطبيقية. كما يركز الفصل على توضيح طبيعة العلاقة التي تربط بين متغيرات الدراسة في ضوء ما قدمته الدراسات السابقة من نتائج ونماذج تفسيرية، وذلك بهدف بناء إطار نظري متكامل يفسر هذه العلاقة ويبرر صياغة الفرضيات التي تقوم عليها الدراسة. ويأتي هذا الطرح دون الاقتصار على عرض المفاهيم بصورة وصفية، وإنما من خلال تحليلها وربطها بالسياق المؤسسي والتقني الذي تعمل فيه شركات تقنية المعلومات في المملكة العربية السعودية، بما يتيح فهماً أعمق للعوامل المؤثرة في البيئة الرقمية الحديثة.

كما يهدف الفصل إلى إبراز التطورات الفكرية والتقنية التي شهدها مجال الدراسة خلال السنوات الأخيرة، واستعراض الاتجاهات الحديثة في الأدبيات العلمية التي تناولت توظيف التقنيات الذكية في دعم كفاءة الأنظمة الرقمية وتعزيز قدرتها على مواجهة التحديات الأمنية المتزايدة. ويساعد هذا العرض في توضيح الخلفية العلمية التي تستند إليها الدراسة الحالية، والكشف عن أوجه الاتفاق والاختلاف بين الدراسات السابقة، وتحديد

الفجوات البحثية التي تسعى الدراسة إلى معالجتها، الأمر الذي يسهم في تعزيز القيمة العلمية للبحث وإبراز إسهامه في تطوير المعرفة المتعلقة بموضوع الدراسة.

وتبرز أهمية هذا الفصل أيضاً في كونه يمثل حلقة الوصل بين الجانب النظري والجانب الميداني للدراسة، حيث يوفر الأساس العلمي اللازم لتطوير أداة الدراسة، وتحديد أبعاد القياس، وصياغة الفرضيات، واختيار الأساليب الإحصائية المناسبة لاختبارها. كما يسهم في بناء نموذج بحثي متكامل يستند إلى منطق علمي واضح، ويضمن أن تكون النتائج التي سيتم التوصل إليها لاحقاً قابلة للتفسير في ضوء الأدبيات والنظريات ذات العلاقة. ومن ثم، فإن هذا الفصل لا يقتصر على عرض المعلومات، وإنما يؤدي دوراً محورياً في تعزيز جودة الدراسة، وزيادة موثوقية نتائجها، وإبراز أهميتها العلمية والتطبيقية في دعم التحول الرقمي الأمن وتعزيز الابتكار داخل شركات تقنية المعلومات في المملكة العربية السعودية.

2.2. المتغيرات المستقلة:

- المتغير المستقل الأول: الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية

يشكل الكشف المبكر عن التهديدات السيبرانية باستخدام الذكاء الاصطناعي من أهم التطبيقات الحديثة التي أحدثت تحولاً كبيراً في مجال الأمن السيبراني، حيث تعتمد الأنظمة الذكية على خوارزميات التعلم الآلي والتعلم العميق لتحليل كميات ضخمة من البيانات الأمنية بصورة مستمرة، والتعرف على الأنماط غير الطبيعية التي قد تشير إلى وجود محاولات اختراق أو هجمات إلكترونية قبل أن تتسبب في أضرار فعلية. وتتميز هذه الأنظمة بقدرتها على التعلم المستمر من البيانات الجديدة، مما يجعلها أكثر كفاءة في اكتشاف التهديدات المستجدة مقارنة بالأنظمة التقليدية التي تعتمد على قواعد بيانات ثابتة.

كما يسهم هذا التطبيق في تقليل زمن اكتشاف الحوادث الأمنية، ورفع مستوى دقة التحليلات، وتقليل الإنذارات الخاطئة، مما يساعد فرق الأمن السيبراني على التركيز على التهديدات الحقيقية واتخاذ الإجراءات الوقائية في الوقت المناسب. وفي شركات تقنية المعلومات التي تعتمد على بيئات تشغيل رقمية معقدة، يمثل

الكشف المبكر أحد أهم عناصر بناء منظومة أمنية استباقية قادرة على الحد من المخاطر الإلكترونية قبل تطورها إلى أزمات تؤثر في استمرارية الأعمال أو سلامة البيانات.

- المتغير المستقل الثاني: الذكاء الاصطناعي في الاستجابة الذكية وإدارة الحوادث السيبرانية

يشير هذا المتغير إلى قدرة تطبيقات الذكاء الاصطناعي على أتمتة عمليات الاستجابة للحوادث السيبرانية وإدارة الهجمات الإلكترونية بصورة سريعة وفعالة، من خلال تحليل الحدث الأمني فور اكتشافه، وتحديد مستوى الخطورة، واقتراح أو تنفيذ إجراءات الاستجابة المناسبة بصورة آلية أو شبه آلية. وتساعد هذه التقنيات في تقليل زمن الاستجابة للحوادث، والحد من انتشار الهجمات، وتقليل حجم الأضرار التي قد تلحق بالأنظمة الرقمية.

وتكتسب هذه الخاصية أهمية كبيرة في المشاريع الرقمية التي تتعامل مع كميات ضخمة من البيانات والخدمات الإلكترونية، حيث يصعب على فرق الأمن التقليدية التعامل مع جميع الحوادث الأمنية بالسرعة المطلوبة. ويسهم الذكاء الاصطناعي في دعم فرق الأمن من خلال توفير تحليلات فورية، وتحديد أولويات التعامل مع التهديدات، وتنفيذ بعض إجراءات الاحتواء والعزل بشكل تلقائي، مما يعزز كفاءة إدارة الحوادث، ويرفع مستوى جاهزية المؤسسة في مواجهة التهديدات السيبرانية المتطورة.

- المتغير المستقل الثالث: الذكاء الاصطناعي في تحليل البيانات الأمنية ودعم اتخاذ القرار

يمثل تحليل البيانات الأمنية ودعم اتخاذ القرار باستخدام الذكاء الاصطناعي أحد أهم التطبيقات التي تعتمد عليها المؤسسات الحديثة في تطوير الأمن السيبراني، حيث تقوم تقنيات الذكاء الاصطناعي بتحليل كميات هائلة من البيانات المستخرجة من الشبكات والأجهزة والتطبيقات، واكتشاف العلاقات والأنماط الخفية التي يصعب ملاحظتها بالطرق التقليدية. كما تستخدم النماذج الذكية التحليلات التنبؤية لتوقع الهجمات المستقبلية، وتقييم مستويات المخاطر، وتقديم توصيات تساعد متخذي القرار على اختيار أفضل الإجراءات الأمنية.

وتسهم هذه التقنيات في رفع جودة القرارات الأمنية من خلال توفير معلومات دقيقة ومحدثة بصورة مستمرة، الأمر الذي يساعد الإدارات التقنية على تخصيص الموارد بكفاءة، وتطوير استراتيجيات الحماية، وتحديد أولويات الاستثمار في الأمن السيبراني. كما أن الاعتماد على التحليلات الذكية يقلل من احتمالية الخطأ البشري، ويزيد من سرعة اتخاذ القرار، ويعزز قدرة المؤسسة على التكيف مع التهديدات الرقمية المتغيرة، مما يدعم استدامة المشاريع الرقمية ويزيد من موثوقيتها.

2.3. المتغير التابع:

- تعزيز الأمن السيبراني للمشاريع الرقمية

يمثل تعزيز الأمن السيبراني للمشاريع الرقمية المتغير التابع في هذه الدراسة، ويُقصد به قدرة المشاريع الرقمية على حماية أنظمتها وشبكاتنا وقواعد بياناتها وأصولها الرقمية من التهديدات والهجمات الإلكترونية، مع المحافظة على سرية المعلومات وسلامتها وتوافرها، وضمان استمرارية العمليات التشغيلية دون انقطاع. كما يشمل هذا المفهوم قدرة المؤسسة على اكتشاف المخاطر السيبرانية، والاستجابة السريعة للحوادث الأمنية، وتقليل الآثار الناتجة عنها، والالتزام بالسياسات والمعايير الوطنية والدولية المتعلقة بالأمن السيبراني.

ويشكل الأمن السيبراني في المشاريع الرقمية من أهم العوامل التي تؤثر في نجاح المؤسسات التقنية واستدامتها، نظراً لاعتمادها الكامل على الأنظمة الرقمية والبنية التحتية التقنية. فكلما ارتفع مستوى الحماية الإلكترونية، ازدادت ثقة العملاء والشركاء، وتحسنت موثوقية الخدمات الرقمية، وانخفضت احتمالات التعرض للخسائر المالية أو التشغيلية الناتجة عن الاختراقات الإلكترونية. كما أن الأمن السيبراني الفعال يدعم استمرارية الأعمال، ويعزز الامتثال للأنظمة والتشريعات، ويرفع جاهزية المؤسسات لمواجهة التهديدات المتجددة في بيئة الأعمال الرقمية.

2.4. العلاقة بين المتغير المستقل والمتغير التابع:

يقوم النموذج المقترح للدراسة على افتراض وجود علاقة تأثير إيجابية مباشرة بين تطبيقات الذكاء الاصطناعي، ممثلة في الكشف المبكر عن التهديدات السيبرانية، والاستجابة الذكية وإدارة الحوادث السيبرانية، وتحليل البيانات الأمنية ودعم اتخاذ القرار، وبين تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية. ويستند هذا الافتراض إلى أن تطبيقات الذكاء الاصطناعي توفر قدرات تحليلية واستباقية لا تستطيع الأنظمة التقليدية تحقيقها بنفس الكفاءة، الأمر الذي يؤدي إلى تحسين مستوى الحماية الإلكترونية، ورفع سرعة اكتشاف الهجمات، وتقليل زمن الاستجابة، وتعزيز دقة تقييم المخاطر.

كما يفترض النموذج أن المتغيرات المستقلة لا تعمل بصورة منفصلة، وإنما تتكامل فيما بينها لتشكيل منظومة أمن سيبراني ذكية؛ إذ يبدأ التكامل بالكشف المبكر عن التهديدات، يليه الاستجابة السريعة وإدارة الحوادث، ثم تحليل البيانات الأمنية واستخدام نتائجها في دعم القرارات المستقبلية وتحسين الاستراتيجيات الأمنية بصورة مستمرة. ويؤدي هذا التكامل إلى بناء بيئة رقمية أكثر أمنًا ومرونة، ويعزز قدرة المشاريع الرقمية على حماية أصولها المعلوماتية، والمحافظة على استمرارية أعمالها، والحد من المخاطر السيبرانية، بما ينسجم مع مستهدفات رؤية المملكة العربية السعودية 2030 في بناء اقتصاد رقمي آمن ومستدام.

2.5. الخاتمة:

تناول هذا الفصل الإطار النظري للدراسة بصورة متكاملة، من خلال استعراض وتحليل الأدبيات العلمية والنظريات الحديثة التي تناولت موضوع الدراسة، بما أسهم في بناء قاعدة معرفية متينة توضح الأسس الفكرية التي تستند إليها الدراسة الحالية. كما تضمن الفصل عرضاً علمياً لمتغيرات الدراسة، وبيان مفاهيمها وأبعادها وخصائصها، مع تحليلها في ضوء ما توصلت إليه الدراسات السابقة، الأمر الذي وفر فهماً متكاملًا لطبيعة هذه المتغيرات ودورها في تفسير الظاهرة محل البحث. وإلى جانب ذلك، تناول الفصل العلاقة العلمية التي تربط بين

متغيرات الدراسة استناداً إلى النماذج والنظريات ذات الصلة، مما أتاح بناء إطار نظري متماسك يدعم صياغة الفرضيات وبوجه الدراسة نحو اختبارها في الجانب الميداني.

وقد أسهم ما تضمنه الفصل من عرض وتحليل في توضيح الكيفية التي تتفاعل بها متغيرات الدراسة ضمن منظومة واحدة، وأبرز أهمية النظر إليها باعتبارها عناصر مترابطة تؤثر في تحقيق النتائج المستهدفة، بدلاً من التعامل معها بصورة منفصلة. كما ساعد هذا التحليل في بناء تصور علمي واضح حول طبيعة العلاقات التي ستخضع للاختبار الإحصائي في الدراسة التطبيقية، وهو ما يعزز من سلامة النموذج البحثي ويمنح الدراسة أساساً علمياً راسخاً لتفسير النتائج في ضوء الأدبيات العلمية الحديثة.

كما أظهر الفصل أهمية الإطار النظري في دعم جودة البحث العلمي، من خلال إسهامه في اختيار أدوات القياس المناسبة، وتحديد الأبعاد الرئيسة لمتغيرات الدراسة، وصياغة الفرضيات وفق أسس علمية ومنهجية دقيقة. وأسهم كذلك في الكشف عن الفجوات المعرفية التي لا تزال قائمة في الأدبيات، والتي شكلت منطلقاً لإجراء الدراسة الحالية، بما يعزز من قيمتها العلمية، ويميز إسهامها في تطوير المعرفة المتعلقة بالذكاء الاصطناعي والأمن السيبراني في بيئة الأعمال السعودية.

وفي ضوء ما سبق، يمكن التأكيد على أن الفصل الثاني أدى دوراً محورياً في تأسيس البناء العلمي للدراسة، حيث وفر الخلفية النظرية اللازمة لفهم موضوع البحث، ومهد للانتقال إلى الجانب الميداني من خلال تقديم إطار معرفي متكامل يفسر طبيعة المتغيرات والعلاقة فيما بينها.

- Adebola Folorunso. (2024). Impact of AI on cybersecurity and security compliance. تم الاسترداد من https://www.researchgate.net/publication/385558741_Impact_of_AI_on_cybersecurity_and_security_compliance
- Ahmad Subhi Salem Mufleh. (2026). Social aspects of artificial intelligence (AI)-driven sustainability in Saudi Arabia: A systematic review with insights on labor market transformations. تم الاسترداد من <https://www.sciencedirect.com/science/article/pii/S2590291126001762>
- Ahmed Abaker. (2026). Emerging Technologies as Enablers of Sustainable Management: A Comprehensive Framework—The Role of Saudi Arabia's Vision 2030. تم الاسترداد من <https://www.mdpi.com/2071-1050/18/7/3168>
- Amani Steiti. (2024). Artificial Intelligence Predictions in Cyber Security: Analysis and Early Detection of Cyber Attacks. تم الاسترداد من https://www.researchgate.net/publication/380459183_Artificial_Intelligence_Predictions_in_Cyber_Security_Analysis_and_Early_Detection_of_Cyber_Attacks
- Anay Sharma. (2024). THE IMPACT OF CYBERSECURITY BREACHES ON BIG BUSINESSES. تم الاسترداد من https://www.researchgate.net/publication/385421361_THE_IMPACT_OF_CYBERSECURITY_BREACHES_ON_BIG_BUSINESSES
- Daoud Abdellatif Jerab. (2024). The Impact of Digital Transformation on Public Services. تم الاسترداد من https://www.researchgate.net/publication/383836540_The_Impact_of_Digital_Transformation_on_Public_Services
- Emmanuel Cadet. (2024). Applying artificial intelligence in Cybersecurity to enhance threat detection, response, and risk management. تم الاسترداد من https://www.researchgate.net/publication/385236454_Applying_artificial_intelligence_in_Cybersecurity_to_enhance_threat_detection_response_and_risk_management
- Faozi A. Almaqtari. (2026). The impact of AI technologies and cybersecurity threats readiness on ERP accounting systems: The role of Cybersecurity Governance. تم الاسترداد من <https://www.sciencedirect.com/science/article/pii/S2199853126000831>

- Fatma Abudaqqa. (2025). Artificial Intelligence for IT Governance in Saudi Arabia: Opportunities, Challenges, and Future Directions within COBIT and ISO/IEC 38500 Frameworks 2019
 تــــم الــــاســــترــــداد مــــن
https://www.researchgate.net/publication/396009885_Artificial_Intelligence_for_IT_Governance_in_Saudi_Arabia_Opportunities_Challenges_and_Future_Directions_within_COBIT_2019_and_ISOIEC_38500_Frameworks
- Irshaad Jada. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review
 تــــم الــــاســــترــــداد مــــن
<https://www.sciencedirect.com/science/article/pii/S2543925123000372>
- Kalam Khadka. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal
 تــــم الــــاســــترــــداد مــــن
https://www.researchgate.net/publication/391277059_Human_factors_in_cybersecurity_an_interdisciplinary_review_and_framework_proposal
- Kirti Raj Bhatele. (2019). The Role of Artificial Intelligence in Cyber Security
 تــــم الــــاســــترــــداد مــــن
https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security
- Mohamed Yagoub Geaiger. (2026). A Systematic Survey of AI-Enhanced Cybersecurity in Saudi Arabia: Strategic Trends and Future Directions
 تــــم الــــاســــترــــداد مــــن
http://researchgate.net/publication/405390954_A_Systematic_Survey_of_AI-Enhanced_Cybersecurity_in_Saudi_Arabia_Strategic_Trends_and_Future_Directions
- Moustafa Elbehairy. (2025). Data Sovereignty and Digital Health Transformation in Saudi Arabia: A Review with Policy Implications for Vision 2030
 تــــم الــــاســــترــــداد مــــن
https://www.researchgate.net/publication/396270843_Data_Sovereignty_and_Digital_Health_Transformation_in_Saudi_Arabia_A_Review_with_Policy_Implications_for_Vision_2030
- Ramanpreet Kaur. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions
 تــــم الــــاســــترــــداد مــــن
<https://www.sciencedirect.com/science/article/pii/S1566253523001136>

- Weiqian Shao. (2025). The Role of Digital Transformation in Enhancing Organizational Agility and Competitive Advantages: A Strategic Perspective
ن_____م_____الاس_____ترداد م_____ن
https://www.researchgate.net/publication/387806349_The_Role_of_Digital_Transformation_in_Enhancing_Organizational_Agility_and_Competitive_Advantages_A_Strategic_Perspective
- Yazan AL-Khassawneh. (2022). A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges
ن_____م_____الاس_____ترداد م_____ن
https://www.researchgate.net/publication/366622747_A_Review_of_Artificial_Intelligence_in_Security_and_Privacy_Research_Advances_Applications_Opportunities_and_Challenges

3. الملاحق:

3.1. ملحق (أ): الاستبيان

عنوان الدراسة:

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

المملكة العربية السعودية

السادة المشاركون/المشاركات،

يهدف هذا الاستبيان إلى جمع البيانات اللازمة لدراسة دور الذكاء الاصطناعي في تعزيز الأمن السيبراني للمشاريع الرقمية في شركات تقنية المعلومات بالمملكة العربية السعودية. وتستخدم البيانات لأغراض البحث العلمي فقط، مع الحفاظ على سرية المعلومات وعدم استخدامها إلا لأغراض الدراسة.

يرجى قراءة كل عبارة بعناية، ثم اختيار الإجابة التي تعبر عن درجة موافقتكم عليها.

مقياس الإجابة:

- أوافق بشدة
- أوافق
- محايد
- لا أوافق
- لا أوافق بشدة

❖ أولاً: البيانات الديموغرافية

1. العمر:

- 20-30 سنة

- 30-40 سنة

- 40-50 سنة

- 50-60 سنة

- 60 سنة فأكثر

2. الجنس:

- ذكر

- أنثى

3. الدرجة العلمية:

- ثانوي

- بكالوريوس

- ماجستير

- دكتوراه

- مؤهل أعلى

ثانيًا: محاور الاستبيان

❖ المحور الأول: استخدام الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية

1. يسهم استخدام تقنيات الذكاء الاصطناعي في اكتشاف التهديدات السيبرانية في المشاريع الرقمية بسرعة.

2. تساعد تقنيات الذكاء الاصطناعي في التعرف على الأنشطة غير الطبيعية داخل الأنظمة الرقمية.

3. يسهم الذكاء الاصطناعي في تحسين دقة اكتشاف الهجمات السيبرانية مقارنة بالأساليب التقليدية.
4. يساعد الذكاء الاصطناعي في تحليل كميات كبيرة من البيانات للكشف عن التهديدات الأمنية.

❖ المحور الثاني: الاستجابة الذكية للحوادث والهجمات السيبرانية

1. يسهم استخدام الذكاء الاصطناعي في الاستجابة السريعة للحوادث والهجمات السيبرانية.
2. تساعد أنظمة الذكاء الاصطناعي في اتخاذ الإجراءات المناسبة عند اكتشاف حادث أمني.
3. يقلل استخدام الذكاء الاصطناعي من الوقت اللازم لاحتواء الحوادث السيبرانية.
4. يساعد الذكاء الاصطناعي في الحد من الآثار السلبية الناتجة عن الحوادث الأمنية على المشاريع الرقمية.

❖ المحور الثالث: تحليل البيانات الأمنية والتنبيه بالمخاطر السيبرانية

1. تساعد تقنيات الذكاء الاصطناعي في التنبيه بالمخاطر والتهديدات السيبرانية المحتملة.
2. يسهم الذكاء الاصطناعي في تحديد نقاط الضعف الأمنية قبل استغلالها من قبل المهاجمين.
3. تساعد التحليلات المعتمدة على الذكاء الاصطناعي في تحسين قدرة الشركة على تقييم المخاطر السيبرانية.

4. يسهم استخدام الذكاء الاصطناعي في تطوير إجراءات استباقية للحد من المخاطر الأمنية.

❖ المحور الرابع: تعزيز الأمن السيبراني للمشاريع الرقمية

1. يسهم استخدام الذكاء الاصطناعي في رفع مستوى حماية البيانات والأنظمة في المشاريع الرقمية.
2. يساعد الذكاء الاصطناعي في تقليل احتمالية تعرض المشاريع الرقمية للاختراقات السيبرانية.

3. يسهم الذكاء الاصطناعي في تعزيز قدرة الشركة على المحافظة على سرية المعلومات وسلامتها وتوافرها.
4. يؤدي توظيف الذكاء الاصطناعي إلى تحسين مستوى الأمن السيبراني العام للمشاريع الرقمية.
5. يسهم استخدام الذكاء الاصطناعي في تعزيز قدرة المشاريع الرقمية على مواجهة التهديدات السيبرانية المتطورة.