

العنوان باللغة العربية

تأثير الذكاء الاصطناعي في أنظمة المراقبة الأمنية على استراتيجيات اتخاذ القرار الأمني: دراسة حالة شركة تحكم

إعداد الطالب/

رياض هليل راضي الشملاي العنزي

إشراف/

د. الفصيل عبد الحميد

د. فايز جراد

العام الدراسي:

2025

شكر وتقدير

أتوجه ببالغ الشكر والتقدير إلى عائلتي الكريمة، التي كانت ولا تزال العون والسند، لما قدمته لي من دعم نفسي ومعنوي لا يُقدّر بثمن، ولما أحاطتني به من دعاء وصبر وتشجيع كان له بالغ الأثر في تجاوز الصعوبات وإتمام هذا العمل.

كما أعبر عن امتناني العميق لأصدقائي الأعزاء، الذين كان حضورهم ومساندتهم ركيزة مهمة خلال هذه الرحلة العلمية، فكانوا شركاء في كل لحظة تحدٍّ، وكل خطوة إنجاز.

فهرس المحتويات:

5.....	قائمة الجداول :
5.....	فهرس الاشكال :
6.....	المستخلص :
7.....	الفصل الأول: :
8.....	المقدمة :
9.....	مشكلة الدراسة :
9.....	أهمية الدراسة :
11.....	أهداف الدراسة :
12.....	تساؤلات الدراسة :
12.....	فروض الدراسة :
13.....	النظرية العلمية المتبعة :
14.....	الفصل الثاني: :
15.....	الدراسات السابقة :
15.....	مقدمة :
15.....	الدراسات السابقة :
16.....	الإطار النظري :
19.....	الفصل الثالث: :
20.....	منهجية الدراسة :
21.....	مقدمة :
21.....	المنهجية وطرق البحث :
22.....	مجتمع البحث :
23.....	حدود البحث :

25.....	الفصل الرابع:
26.....	النتائج والتوصيات :
26.....	مقدمة :
26.....	تحليل البيانات :
28.....	النتائج :
31.....	التوصيات :
34.....	المراجع :
35.....	المراجع العربية :
35.....	المراجع الأجنبية :
37.....	الملاحق :
37.....	الاستبانة :
38.....	الملخص باللغة الإنجليزية (Abstract) :

قائمة الجداول :

- الجدول (1): توزيع أفراد العينة حسب الفئة الوظيفية
- الجدول (2): الأداء في المؤشرات الرئيسية قبل وبعد تطبيق الذكاء الاصطناعي في أنظمة المراقبة الأمنية – دراسة حالة: شركة تحكم

فهرس الأشكال:

- شكل (1) يوضح كيف يتم تطبيق دورة PDCA (خطط – نفذ – تحقق – صحح) لتحسين أداء أنظمة المراقبة الأمنية عبر تقنيات الذكاء الاصطناعي في الشركة.
- شكل (2): هيكل عمليات إطار عمل الذكاء الاصطناعي الذي تعتمد عليه شركة تحكم لإدارة دورة حياة خدمات المراقبة الأمنية الذكية، مما يعزز من جودة اتخاذ القرار الأمني.

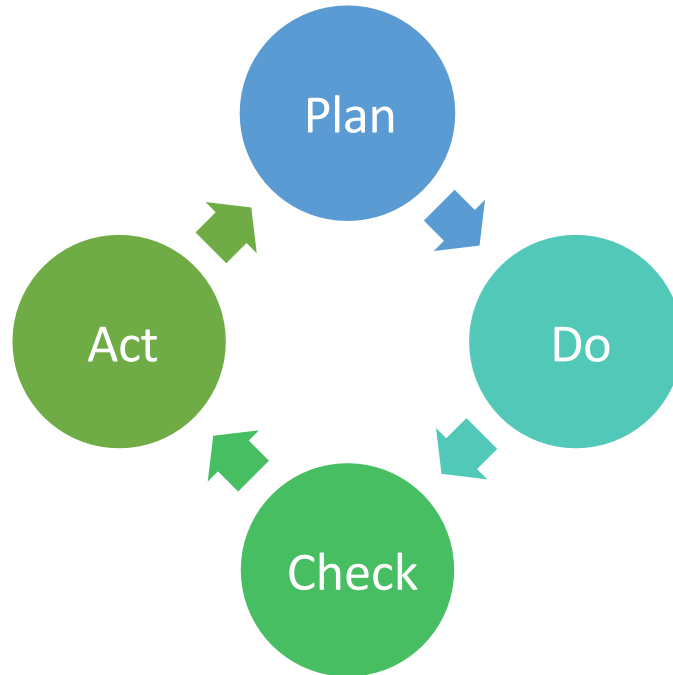
المستخلص : Abstract

تهدف هذه الدراسة إلى تحليل أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية على تعزيز كفاءة وفعالية عمليات اتخاذ القرار الأمني، وذلك من خلال دراسة تطبيقية على شركة "تحكم" الرائدة في المملكة العربية السعودية، والمتخصصة في حلول الأمن التقني وإدارة الحركة المرورية الذكية على مستوى وطني. وتكتسب هذه الدراسة أهميتها من التوجه المتزايد نحو توظيف الذكاء الاصطناعي في البنى التحتية الأمنية، ودوره المتنامي في دعم متخذي القرار في مواجهة التحديات الأمنية المتغيرة والمعقدة.

اعتمدت الدراسة المنهج الوصفي التحليلي، واستخدمت أداة الاستبانة لجمع البيانات من عينة مختارة من موظفي شركة "تحكم"، بهدف قياس مدى تأثير استخدام تقنيات الذكاء الاصطناعي على فعالية العمليات الأمنية، وتحديد أبرز الإيجابيات والتحديات المصاحبة لتطبيق هذه التقنيات في بيئة عمل واقعية.

وقد كشفت نتائج الدراسة عن دور فعال للذكاء الاصطناعي في تسريع عمليات اتخاذ القرار الأمني، وتحسين القدرة على التنبؤ بالمخاطر والتهديدات المحتملة، إضافة إلى تقليل الاعتماد على التقديرات الذاتية البشرية، مما يساهم في رفع مستوى الدقة والموضوعية في التعامل مع الأحداث الأمنية. ومع ذلك، أظهرت النتائج وجود عدد من التحديات التي قد تعيق الاستخدام الأمثل لهذه التقنيات، ومن أبرزها محدودية التدريب المتخصص للكوادر البشرية، والحاجة إلى مواءمة الاستخدام التكنولوجي مع البعد الإنساني في السياق الأمني.

وانطلاقاً من هذه النتائج، توصي الدراسة بضرورة العمل على تعزيز التكامل بين القدرات البشرية والتقنيات الذكية، من خلال تطوير برامج تدريبية متقدمة، وتحديث البنية التحتية التقنية بشكل دوري، بما يضمن استمرارية التكيف مع التطورات المتسارعة في مجال الذكاء الاصطناعي، وتحقيق أقصى استفادة من الإمكانيات التي تتيحها الأنظمة الأمنية الذكية في دعم منظومة الأمن الوطني.



الفصل الأول

المقدمة:

في ظل الثورة التكنولوجية المتسارعة التي تشهدها مختلف القطاعات حول العالم، أصبح الذكاء الاصطناعي أحد المحركات الأساسية للتحويل الرقمي، لا سيما في المجالات التي تتطلب دقة عالية واتخاذ قرارات سريعة وحاسمة، مثل الأمن والمراقبة. فقد أحدث الذكاء الاصطناعي نقلة نوعية في كيفية تصميم وتشغيل أنظمة المراقبة الأمنية، من خلال تمكين هذه الأنظمة من معالجة كميات ضخمة من البيانات في الوقت الحقيقي، وتحليل الصور والفيديوهات بدقة متناهية، والتعرف الذكي على الوجوه والسلوكيات المشبوهة، بالإضافة إلى القدرة على إصدار تنبيهات فورية حول الأحداث غير الطبيعية أو الطارئة.

تُعد أنظمة المراقبة الأمنية المدعومة بتقنيات الذكاء الاصطناعي اليوم من الركائز الأساسية التي تعتمد عليها المؤسسات الأمنية لتعزيز كفاءتها التشغيلية وتحسين استراتيجيات اتخاذ القرار. إذ تتيح هذه التقنيات فرصة للتقليل من الأخطاء البشرية وتسريع عمليات التحليل واتخاذ الإجراءات الوقائية، مما يساهم في رفع مستوى الأمان وحماية المنشآت والأفراد بشكل أكثر فعالية.

في هذا السياق، تأتي هذه الدراسة لتقديم تحليل معمق لتأثير الذكاء الاصطناعي على أنظمة المراقبة الأمنية، مع التركيز على استراتيجيات اتخاذ القرار الأمني في شركة "تحكم"، التي تعد واحدة من أبرز الشركات الوطنية المتخصصة في الأمن التقني وإدارة الحركة المرورية في المملكة العربية السعودية. من خلال هذه الدراسة، نسعى لفهم مدى قدرة تقنيات الذكاء الاصطناعي على تحسين الأداء الأمني، والتحديات التي تواجه تطبيق هذه التقنيات في الواقع العملي، بالإضافة إلى اقتراح توصيات تساهم في تعزيز التكامل بين التكنولوجيا والكوادر البشرية لضمان تحقيق أفضل النتائج.

تُبرز الدراسة أهمية استثمار التقنيات الذكية ضمن البنية التحتية الأمنية، مع التركيز على تحديث وتطوير أنظمة المراقبة بشكل مستمر لمواكبة التطورات المتسارعة في مجال الأمن السيبراني والتحليل البياني، بما يضمن تحقيق أعلى معايير الأمان والفعالية في مواجهة المخاطر والتهديدات المتجددة.

مشكلة الدراسة.

شهدت السنوات الأخيرة توسعاً كبيراً في استخدام تقنيات الذكاء الاصطناعي ضمن الأنظمة الأمنية الحديثة، حيث أصبحت هذه التقنيات من الأدوات الرئيسية التي تُعتمد عليها في مراقبة البيانات الأمنية وتحليل البيانات بشكل فوري وفعال. ومع ذلك، لا يزال هناك غموض واضح حول مدى تأثير هذه التقنيات على تحسين جودة وفاعلية عمليات اتخاذ القرار الأمني داخل المؤسسات.

يُطرح تساؤل جوهري حول مدى قدرة الذكاء الاصطناعي على تسريع وتطوير القرارات الأمنية، ومدى مساهمته في تقليل الأخطاء البشرية، مع التأكيد على ضرورة فهم التحديات التي قد تنشأ نتيجة للاعتماد المتزايد على هذه التقنيات. إذ يبرز هنا سؤال مهم حول كيفية تفاعل العاملين مع هذه الأدوات الذكية، ومدى قدرتهم على التكيف مع التغيرات التي تفرضها، فضلاً عن مدى إمكانية تحقيق توازن فعال بين التقنية والعنصر البشري لضمان اتخاذ قرارات أمنية سليمة وموثوقة.

بناءً على ما سبق، تتضح مشكلة الدراسة في عدم وجود رؤية واضحة حول أثر تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية على تحسين استراتيجيات اتخاذ القرار الأمني، مع وجود تحديات واضحة تتعلق بعملية التكامل بين القدرات التقنية والمهارات البشرية، مما يستوجب دراسة معمقة لفهم هذه العلاقة والتغلب على العقبات المرتبطة بها.

أهمية الدراسة.

الأهمية العلمية (النظرية):

تكمن الأهمية العلمية لهذه الدراسة في إثراء المعرفة المتعلقة بدور تقنيات الذكاء الاصطناعي في تعزيز أنظمة المراقبة الأمنية وتحسين استراتيجيات اتخاذ القرار الأمني داخل المؤسسات. رغم توسع الأبحاث في مجالات الذكاء الاصطناعي والتطبيقات الأمنية، إلا أن هناك فجوة معرفية واضحة تتعلق بقياس الأثر الفعلي لهذه التقنيات على جودة القرارات الأمنية وسرعتها، لا سيما في السياق العملي لشركات الأمن التقنية في المملكة العربية السعودية. تقدم هذه الدراسة أدلة كمية ونوعية تساهم في سد هذه الفجوة البحثية، من خلال التركيز على تجربة شركة "تحكم" كنموذج وطني رائد. تعتمد الدراسة على إطار نظري يجمع بين مفاهيم التحليل البياني، وتقنيات الذكاء الاصطناعي، ونظريات اتخاذ القرار الأمني، مما يوفر نموذجاً متكاملًا لدراسة تأثير هذه التقنيات على مختلف أبعاد الأداء الأمني. ومن المتوقع أن تمثل هذه الدراسة إضافة علمية قيمة للمجال الأكاديمي والبحثي في مجالات الأمن السيبراني، نظم المعلومات الإدارية، وتحليل البيانات، مع فتح المجال لدراسات مستقبلية لمقارنة نتائج تطبيق الذكاء الاصطناعي في قطاعات ومؤسسات أمنية مختلفة.

الأهمية العملية (التطبيقية):

توفر هذه الدراسة معلومات قيمة تساعد صناع القرار والعاملين في قطاع الأمن التقني على فهم أبعاد تأثير الذكاء الاصطناعي في تحسين استراتيجيات اتخاذ القرار الأمني، مما يتيح لهم تطوير خطط عمل مستندة إلى بيانات واقعية وتجارب عملية. من خلال النتائج والتوصيات، سيتمكن المسؤولون في شركة "تحكم" ومؤسسات مماثلة من:

1. التعرف على النجاحات والتحديات التي صاحبت تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية، وتحديد المجالات التي تحتاج إلى تعزيز أو تطوير لتحسين الأداء.
 2. تحسين التكامل بين العنصر البشري والتقنيات الذكية بما يضمن تحقيق أعلى مستويات الدقة والكفاءة في اتخاذ القرارات الأمنية.
 3. تطوير آليات تدريب مستمرة تدعم الموظفين في التعامل مع الأدوات الذكية والتكيف مع التغييرات التكنولوجية المتسارعة.
 4. تعظيم العائد على الاستثمار في التقنيات الحديثة، من خلال وضع استراتيجيات واضحة لتعزيز فعالية استخدام الذكاء الاصطناعي.
- علاوة على ذلك، تتيح الدراسة إمكانية تعميم الدروس المستفادة ووضع توصيات قابلة للتطبيق على مؤسسات أمنية أخرى داخل المملكة وخارجها، مما يدعم جهود التحول الرقمي في القطاع الأمني الوطني، ويسهم في رفع كفاءة واستجابة أنظمة المراقبة الأمنية بما يتماشى مع رؤية المملكة 2030.

أهداف الدراسة.

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف المحورية التي تسعى لفهم وتقييم تأثير تقنيات الذكاء الاصطناعي على أنظمة المراقبة الأمنية، مع التركيز على تحسين استراتيجيات اتخاذ القرار الأمني في شركة "تحكم". وتشمل هذه الأهداف:

1. استقصاء نطاق استخدام تقنيات الذكاء الاصطناعي في منظومة المراقبة الأمنية داخل شركة "تحكم"، مع تحليل كيفية تطبيقها وتوزيعها عبر مختلف أقسام المؤسسة.
2. تقييم مدى تأثير هذه التقنيات على تحسين سرعة وكفاءة اتخاذ القرارات الأمنية، من خلال قياس دقة التنبؤات وتقليل زمن الاستجابة للحوادث الأمنية.
3. الكشف عن التحديات التي تعترض عملية التفاعل بين الأنظمة الذكية والعاملين، بما في ذلك المعوقات التقنية والثقافية التي تؤثر على فعالية التكامل بين الإنسان والآلة.
4. صياغة توصيات عملية واستراتيجية تهدف إلى تعزيز الأداء الأمني من خلال تكامل أكثر فاعلية بين الذكاء الاصطناعي والكوادر البشرية، ودعم تطوير استراتيجيات اتخاذ القرار بما يتوافق مع المتطلبات التقنية الحديثة.

تساؤلات الدراسة

تسعى هذه الدراسة إلى استكشاف مجموعة من القضايا البحثية المحورية التي تتناول دور الذكاء الاصطناعي في أنظمة المراقبة الأمنية وتأثيره على جودة وكفاءة اتخاذ القرار في شركة "تحكم"، وتحدد هذه التساؤلات كما يلي:

1. ما هي التقنيات الذكية المعتمدة في أنظمة المراقبة الأمنية لدى شركة "تحكم" وكيف تُوظف في العمليات اليومية؟
2. كيف يؤثر تطبيق الذكاء الاصطناعي على سرعة ودقة عملية اتخاذ القرارات الأمنية داخل المؤسسة؟
3. ما هي الصعوبات والعقبات التي تواجه الكوادر البشرية في استخدام وتبني أنظمة الذكاء الاصطناعي ضمن بيئة العمل الأمني؟
4. ما مستوى الرضا لدى موظفي الشركة تجاه فعالية وكفاءة الأنظمة الأمنية الذكية المعمول بها؟

فروض الدراسة

استنادًا إلى الإطار النظري والدراسات السابقة، تنطلق هذه الدراسة من مجموعة من الفرضيات التي سيتم اختبارها وتحليلها ضمن سياق شركة "تحكم"، وهي كما يلي:

الفرضية الأولى:

يؤدي تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية إلى تسريع عملية اتخاذ القرار الأمني بشكل ملحوظ وفعال.

الفرضية الثانية:

يسهم الاعتماد على تقنيات الذكاء الاصطناعي في تحسين دقة وجودة القرارات الأمنية، مما يعزز من مستوى الأداء العام للأنظمة الأمنية في شركة "تحكم".

الفرضية الثالثة:

تواجه عملية دمج الذكاء الاصطناعي مع العنصر البشري في بيئة العمل الأمنية تحديات تقنية وبشرية، مثل مقاومة التغيير، ونقص التدريب، وضعف التكامل بين الأنظمة الجديدة والعمليات القائمة.

الفرضية الرابعة:

الدعم الإداري والتخطيط الاستراتيجي يسهمان بشكل كبير في تخطي العقبات المصاحبة لتطبيق تقنيات الذكاء الاصطناعي، مما يضمن استمرارية ونجاح التطبيق.

الفرضية الخامسة:

يمكن تحقيق تحسين مستدام في فعالية استراتيجيات اتخاذ القرار الأمني من خلال تبني منهجيات التحسين المستمر، وقياس الأداء باستخدام أدوات تقييم متقدمة ترتبط بأهداف الشركة الاستراتيجية.

النظرية العلمية المتبعة لإعداد البحث

تعتمد هذه الدراسة على إطار نظري مركب يجمع بين أفضل الممارسات والنماذج الإدارية التي تسهم في تقييم وتحسين أداء أنظمة المراقبة الأمنية المدعومة بالذكاء الاصطناعي. ويتضمن الإطار النظري عدة محاور رئيسية:

1. إطار عمل الذكاء الاصطناعي في الأمن والمراقبة

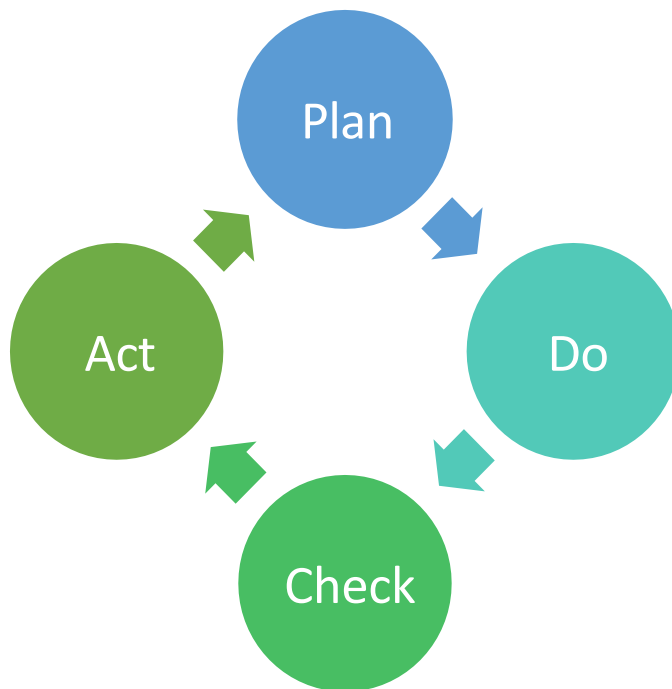
تُعتبر تقنيات الذكاء الاصطناعي مكونًا أساسيًا في النظم الأمنية الحديثة، حيث تُستخدم لتحليل البيانات الضخمة، التعرف على الأنماط، التنبيه المبكر، واتخاذ القرارات بسرعة ودقة. يعتمد هذا الإطار على دمج تقنيات التعلم الآلي، الرؤية الحاسوبية، وأنظمة التنبؤ في دورة حياة أنظمة المراقبة الذكية بهدف تعزيز جودة القرارات الأمنية وتقليل الأخطاء البشرية.

2. نموذج بطاقة الأداء المتوازن (Balanced Scorecard - BSC)

يُستخدم نموذج بطاقة الأداء المتوازن كأداة إدارية لقياس وتحليل تأثير تطبيق تقنيات الذكاء الاصطناعي على الأداء المؤسسي من أربعة أبعاد متكاملة: البعد المالي، بعد العملاء، بعد العمليات الداخلية، وبعد التعلم والنمو. يساهم هذا النموذج في ربط الجهود التقنية بأهداف المؤسسة الاستراتيجية، مما يساعد في تقييم مدى فاعلية الاستثمارات التقنية في تحسين جودة اتخاذ القرار الأمني.

3. منهجية التحسين المستمر (دورة PDCA)

تُعتمد دورة التخطيط - التنفيذ - الفحص - التصحيح (Plan-Do-Check-Act) كإطار عمل إداري لضمان التحسين المستمر في أنظمة المراقبة الأمنية الذكية. من خلال هذه الدورة، يتم التخطيط لتحديثات تقنية محددة، تنفيذها، تقييم أثرها على أداء النظام الأمني، ثم اتخاذ إجراءات تصحيحية أو تعميم التجارب الناجحة. هذه المنهجية تساهم في تطوير نظام متكامل قادر على التكيف مع المتغيرات الأمنية والتقنية بشكل مستمر.



الفصل الثاني الدراسات السابقة

مقدمة

يستعرض هذا الفصل الدراسات السابقة ذات الصلة بموضوع البحث، مع التركيز على الاستفادة من النتائج والتوجهات التي تناولتها الأبحاث السابقة في مجال تطبيقات الذكاء الاصطناعي في أنظمة المراقبة الأمنية. تم تحليل هذه الدراسات ضمن أطر متعددة تهدف إلى فهم تأثير الذكاء الاصطناعي على فاعلية اتخاذ القرار الأمني، بالإضافة إلى مناقشة العوامل التي تسهم في نجاح أو تحديات تبني هذه التقنيات في البيئات الأمنية. كما يقدم الفصل إطارًا نظريًا مفاهيميًا يستند إلى الأدبيات السابقة في مجال الأمن السيبراني، تحليل البيانات، واتخاذ القرار الأمني، مما يوفر قاعدة معرفية متكاملة تدعم التحليل في الفصول اللاحقة. ويشمل العرض توضيحًا لمفاهيم الذكاء الاصطناعي، نظم المراقبة الأمنية، ودور التكامل بين الإنسان والتقنية، بالإضافة إلى منهجيات تقييم الأداء وتحسين العمليات الأمنية باستخدام التقنيات الحديثة. يهدف هذا الإطار إلى إعداد أرضية علمية متينة يمكن البناء عليها في مناقشة وتحليل نتائج الدراسة.

الدراسات السابقة

شهد مجال الذكاء الاصطناعي وتطبيقاته في الأمن اهتمامًا متزايدًا في الأبحاث العالمية والعربية، حيث ركزت العديد من الدراسات على استكشاف أثر تقنيات الذكاء الاصطناعي على تحسين كفاءة أنظمة المراقبة وتعزيز الأداء الأمني. وفيما يلي عرض لأبرز الدراسات التي تشكل خلفية علمية لهذه الدراسة:

• دراسة العسيري: (2021)

تناولت الدراسة تطبيق تقنيات الذكاء الاصطناعي في تحليل الفيديوهات الأمنية، مركزة على استخدام التعرف على الوجه وتحليل الأنماط الزمنية. وأشارت النتائج إلى تقليل ملحوظ في زمن الاستجابة للحوادث الأمنية، وتحسين دقة الرصد الأمني. كما أكدت على أهمية تدريب العاملين على فهم مخرجات الأنظمة الذكية لتحقيق أقصى استفادة منها.

• دراسة الشهري: (2022)

ركزت هذه الدراسة على الجوانب القانونية والأخلاقية المتعلقة باستخدام الذكاء الاصطناعي في أنظمة المراقبة الأمنية، مثل قضايا الخصوصية وحقوق الأفراد. وأبرزت الدراسة الحاجة إلى وضع إطار تشريعي وتنظيمي واضح لضبط استخدام تقنيات الذكاء الاصطناعي في المجال الأمني، بما يوازن بين الفعالية الأمنية وحماية الحقوق المدنية.

• دراسة الحارثي: (2023)

بحثت العلاقة بين توظيف الذكاء الاصطناعي وفاعلية اتخاذ القرار الأمني في المؤسسات الحكومية، خاصة في حالات الطوارئ والأزمات. وخلصت إلى وجود علاقة طردية بين مستوى تبني تقنيات الذكاء الاصطناعي ودقة وسرعة اتخاذ القرار الأمني، مما ينعكس إيجابًا على قدرة المؤسسات في الاستجابة الفورية للتهديدات.

• دراسة: (Smith et al. (2020)

في دراسة دولية، قيم الباحثون تأثير الذكاء الاصطناعي في أنظمة المراقبة على تقليل نسبة الجرائم من خلال التنبؤ بالأنماط السلوكية المشبوهة. أظهرت النتائج زيادة في كفاءة وحدات الأمن وتحسناً في رصد المخاطر الأمنية بشكل استباقي، مع ملاحظة أهمية التكامل بين التكنولوجيا والبشر لضمان دقة النتائج.

• دراسة: (Zhang & Lee (2022)

ناقشت هذه الدراسة تطبيق تقنيات التعلم الآلي في تحليل البيانات الأمنية الضخمة لتحسين استراتيجيات الاستجابة الأمنية. وأكدت على أن استخدام نماذج الذكاء الاصطناعي يمكن أن يقلل من الأخطاء البشرية، ويساعد في تخصيص الموارد الأمنية بشكل أكثر فعالية، مما يؤدي إلى تحسين الأداء العام للأنظمة الأمنية.

الإطار النظري

في ضوء الدراسات السابقة والمراجع النظرية، يستند هذا البحث إلى مجموعة من المفاهيم والنماذج التي تساعد على فهم وتحليل تأثير الذكاء الاصطناعي في أنظمة المراقبة الأمنية على استراتيجيات اتخاذ القرار الأمني، وذلك من خلال دراسة حالة شركة تحكم.

1. الذكاء الاصطناعي في أنظمة المراقبة الأمنية

يُعرف الذكاء الاصطناعي (AI) بأنه فرع من علوم الحاسوب يُعنى بتطوير أنظمة قادرة على تنفيذ مهام تتطلب ذكاءً بشرياً، مثل التعلم، التنبؤ، والتعرف على الأنماط. في مجال المراقبة الأمنية، يُستخدم الذكاء الاصطناعي لتحليل البيانات الضخمة من الكاميرات وأجهزة الاستشعار، مما يسمح بالكشف المبكر عن التهديدات الأمنية وتحسين سرعة الاستجابة.

التقنيات الأساسية تشمل:

- التعلم الآلي (Machine Learning) لتحليل الفيديوها والتعرف على السلوكيات المشبوهة.
- الرؤية الحاسوبية (Computer Vision) للكشف الآلي عن الوجوه والأجسام.
- أنظمة التنبؤ (Predictive Systems) لتقدير المخاطر المستقبلية.

2. أنظمة المراقبة الأمنية التقليدية مقابل أنظمة المراقبة المعززة بالذكاء الاصطناعي

تختلف أنظمة المراقبة الأمنية التقليدية في كونها تعتمد بشكل كبير على المراقبة البشرية وتحليل البيانات بشكل يدوي، مما يحد من دقة وسرعة اتخاذ القرار. أما الأنظمة المعززة بالذكاء الاصطناعي فتُحدث ثورة في هذا المجال من خلال أتمتة عمليات المراقبة وتحليل البيانات بشكل فوري، مما يدعم اتخاذ قرارات أمنية أكثر دقة وفعالية.

3. استراتيجيات اتخاذ القرار الأمني

تعرف استراتيجيات اتخاذ القرار الأمني بأنها الخطط والإجراءات التي تعتمد عليها المؤسسات لضمان أمن المنشآت والأفراد. تتطلب هذه الاستراتيجيات معلومات دقيقة، تحليل متكامل، وسرعة استجابة. الذكاء الاصطناعي يساهم في تعزيز هذه الاستراتيجيات من خلال توفير تحليل دقيق للبيانات وتوقع المخاطر، ما يمكن الجهات الأمنية من اتخاذ قرارات استباقية بدلاً من رد الفعل فقط.

4. العلاقة بين الذكاء الاصطناعي واستراتيجيات اتخاذ القرار الأمني

تشير الأدبيات إلى أن دمج الذكاء الاصطناعي في أنظمة المراقبة يعزز من فعالية استراتيجيات اتخاذ القرار الأمني من خلال:

- زيادة دقة المعلومات: عن طريق تحليل البيانات في الوقت الحقيقي وتقليل الأخطاء البشرية.
- تعزيز سرعة الاستجابة: بتوفير تنبيهات فورية بناءً على تحليل ذكي.
- تمكين اتخاذ قرارات استباقية: من خلال التنبؤ بالتهديدات وتحليل الأنماط الأمنية.
- تقليل التكاليف: عبر أتمتة العمليات وتحسين استخدام الموارد البشرية.

5. دراسة حالة شركة تحكم

شركة تحكم تعتبر نموذجاً تطبيقياً لتقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية. من خلال تطبيق هذه التقنيات، تمكنت الشركة من تحسين استراتيجيات اتخاذ القرار الأمني، مما أدى إلى:

- تقليل عدد الحوادث الأمنية.
- تحسين زمن الاستجابة للحوادث.
- زيادة رضا العملاء الداخليين والخارجيين عن جودة الخدمة الأمنية.

6. التحديات والمعوقات في تطبيق الذكاء الاصطناعي

رغم الفوائد الكبيرة، تواجه تطبيقات الذكاء الاصطناعي في أنظمة المراقبة الأمنية عدة تحديات مثل:

- مقاومة التغيير من قبل العاملين في المؤسسات الأمنية.
- قضايا الخصوصية وحماية البيانات.
- الحاجة إلى استثمارات عالية في البنية التحتية التقنية.
- صعوبة دمج الأنظمة الذكية مع البنى التحتية القديمة.

7. مؤشرات قياس الأداء (KPIs) لقياس أثر الذكاء الاصطناعي

لقياس تأثير تطبيق الذكاء الاصطناعي على استراتيجيات اتخاذ القرار الأمني في شركة تحكم، تعتمد الدراسة على مؤشرات رئيسية مثل:

- متوسط زمن الكشف والاستجابة.
- نسبة تقليل الحوادث الأمنية.
- مستوى دقة التعرف على التهديدات.
- رضا المستخدمين النهائيين.

الفصل الثالث منهجية الدراسة

يتناول هذا الفصل منهجية البحث والإجراءات المتبعة لتنفيذ الدراسة، بدءًا من طبيعة المشكلة وفرضيات البحث، مرورًا بتحديد مجتمع الدراسة وعينتها، وأدوات جمع البيانات المستخدمة، وانتهاءً بطرق تحليل البيانات، مع توضيح إجراءات التحقق من صدق وثبات أدوات البحث.

نظرًا لطبيعة موضوع الدراسة التي تتطلب فهمًا عميقًا للعلاقة بين تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية وتأثيرها على استراتيجيات اتخاذ القرار الأمني، فقد تم اعتماد منهجية البحث المختلطة (Mixed Methods) التي تجمع بين الأسلوبين الكمي والنوعي.

يتمثل الهدف من استخدام هذا المنهج في تكامل البيانات الكمية والنوعية لتحقيق فهم شامل للتأثيرات العملية والتحديات التي تواجه شركة تحكم في تطبيق الذكاء الاصطناعي داخل بيئة المراقبة الأمنية.

يبدأ الفصل بتحديد مجتمع الدراسة الذي يضم العاملين في شركة تحكم من مختلف الأقسام الأمنية والتقنية، ويوضح خصائص العينة المشاركة في الدراسة. كما يتناول الفصل أدوات البحث التي تشمل استبانة لقياس آراء ومواقف المشاركين، بالإضافة إلى مقابلات شخصية مع صناع القرار والخبراء الأمنيين لجمع بيانات نوعية معمقة، إلى جانب تحليل الوثائق والسجلات ذات الصلة.

علاوة على ذلك، يناقش الفصل إجراءات تصميم أدوات البحث، وطرق التحقق من صدقها وثباتها لضمان موثوقية النتائج. كما يتطرق إلى حدود الدراسة من حيث المكان (شركة تحكم فقط)، والزمن، بالإضافة إلى حدود أخرى تتعلق بنطاق الموضوع والجوانب التي تستثنى الدراسة.

تقدم هذه التفاصيل للقارئ إطارًا واضحًا ومنهجيًا لفهم كيفية تنفيذ الدراسة، مما يساعد على تقييم موثوقية النتائج ومدى إمكانية تعميمها على سياقات أخرى مشابهة.

المنهجية وطرق البحث

اعتمدت الدراسة منهجية دراسة الحالة (Case Study) نظرًا لطبيعة البحث التي تتطلب تحليلًا عميقًا ومفصلاً لتأثير تقنيات الذكاء الاصطناعي المطبقة في أنظمة المراقبة الأمنية على استراتيجيات اتخاذ القرار الأمني في بيئة عملية محددة، وهي شركة تحكم. تهدف الدراسة إلى فهم كيفية دمج الذكاء الاصطناعي في الأنظمة الأمنية وتأثيره على جودة وكفاءة القرارات الأمنية.

ضمن إطار دراسة الحالة، تم استخدام النهج المختلط (Mixed Methods Approach)، الذي يجمع بين الأسلوبين الكمي والنوعي لتحقيق تكامل شامل للبيانات، حيث:

- **الأسلوب الكمي (Quantitative):** تم جمع بيانات كمية من خلال استبانة إلكترونية وزعت على موظفي شركة تحكم العاملين في الأقسام الأمنية والتقنية، لقياس مؤشرات الأداء الأمني ومستوى رضاهم عن القرارات المتخذة قبل وبعد تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة. شملت الاستبانة أسئلة مغلقة على مقياس ليكرت لتقييم جوانب محددة مثل دقة الكشف، سرعة الاستجابة، وفعالية اتخاذ القرار. كما تم تحليل بيانات الأداء الأمني مثل متوسط زمن الاستجابة للحوادث الأمنية، ونسبة الدقة في التعرف على التهديدات الأمنية.
 - **الأسلوب النوعي (Qualitative):** أُجريت مقابلات شبه منظمة مع مجموعة مختارة من أصحاب الخبرة في شركة تحكم، شملت مدراء الأمن، مهندسي نظم الذكاء الاصطناعي، وصناع القرار الأمني، بهدف استكشاف التجارب الشخصية، التحديات، والدوافع وراء تبني الذكاء الاصطناعي في أنظمة المراقبة الأمنية، بالإضافة إلى فهم كيفية تأثير ذلك على استراتيجيات اتخاذ القرار الأمني. تم إعداد دليل إرشادي للمقابلات يغطي موضوعات مثل التغيرات التي طرأت على عمليات اتخاذ القرار، العقوبات التي واجهت التنفيذ، وأبرز النجاحات التي تحققت.
- تُستخدم طريقة تقاطع البيانات (Data Triangulation) لمقارنة وتحليل نتائج الأساليب الكمية والنوعية معًا، لتعزيز مصداقية الدراسة. فعلى سبيل المثال، إذا أظهرت البيانات الكمية تحسنًا ملحوظًا في دقة اتخاذ القرار الأمني بنسبة معينة، تدعمها إفادات المشاركين في المقابلات التي توضح الأسباب والخبرات العملية وراء هذا التحسن، فإن ذلك يعزز ثقة الباحثين في النتائج والاستنتاجات. أما في حال وجود تناقض، فإن الدراسة تحلل الأسباب الكامنة لهذا الاختلاف لفهم أعمق للموضوع.

تضمن هذه المنهجية تقديم رؤية متكاملة وشاملة حول تأثير الذكاء الاصطناعي في أنظمة المراقبة الأمنية على استراتيجيات اتخاذ القرار الأمني في شركة تحكم، مما يمكن من تقديم توصيات عملية مبنية على أدلة موضوعية.

مجتمع البحث

مجتمع البحث المستهدف في هذا المشروع هو جميع الموظفين والإدارات في شركة تحكم الذين يتفاعلون مع أنظمة المراقبة الأمنية وتقنيات الذكاء الاصطناعي المطبقة في الشركة، بالإضافة إلى إدارات تقنية المعلومات التي تدير هذه الأنظمة وتقدم الدعم الفني لها.

تعمل شركة تحكم في بيئة تقنية متقدمة تتطلب تنسيقاً عالياً بين فرق الأمن، تقنية المعلومات، التحليل الأمني، وصناع القرار لضمان اتخاذ قرارات أمنية دقيقة وسريعة تهدف إلى حماية المنشآت والمعلومات الحيوية.

يبلغ عدد موظفي الشركة في الأقسام ذات العلاقة حوالي 300 موظف موزعين عبر عدة فروع وإدارات. ولجمع البيانات، تم تحديد عينات من موظفي تقنية المعلومات والموظفين من الأقسام الأخرى المتعاملين بشكل مباشر مع الأنظمة الأمنية والتقنية.

عينة الاستبانة الكمية:

تم توجيه استبانة إلى موظفي إدارة تقنية المعلومات والعاملين في الأقسام التشغيلية المختلفة التي تتعامل مع أنظمة المراقبة الأمنية ودعمها الفني. شملت العينة موظفين من فرق الأمن، التحليل، الدعم الفني، والإدارات ذات الصلة، حيث بلغ عدد المستجيبين الصالحين للتحليل 60 موظفاً.

يوضح الجدول التالي توزيع أفراد العينة حسب الفئة الوظيفية:

الجدول (1): توزيع أفراد العينة حسب الفئة الوظيفية

النسبة المئوية (%)	عدد الأفراد	الفئة الوظيفية
50 %	30	إدارة تقنية المعلومات
50 %	30	موظفو الأقسام الأخرى
100 %	60	الاجمالي

تم اختيار المشاركين بطريقة قصدية (Purposive Sampling) لضمان تمثيل متوازن يمكن من خلاله فهم تأثير الأنظمة على مختلف المستويات الوظيفية.

عينة المقابلات النوعية:

شملت 10 مقابلات نصف مفتوحة مع مجموعة مختارة من المشاركين ذوي الخبرة والمعرفة المباشرة بتنفيذ وتشغيل أنظمة الذكاء الاصطناعي والمراقبة الأمنية في الشركة. من بين المشاركين:

- مدير إدارة تقنية المعلومات

- رؤساء أقسام تقنية المعلومات (البنية التحتية، الدعم الفني)
 - مهندسو نظم الأمن والذكاء الاصطناعي
 - مستخدمو النظام من الأقسام التشغيلية المختلفة (كقسم الأمن، التشغيل والصيانة، إدارة الاستثمار)
- كما تم إجراء مقابلة مع أحد مديري الإدارات العليا للحصول على رؤيته الاستراتيجية حول تأثير تطبيق الأنظمة على أداء وإنتاجية العمل.
- تم استخدام دليل أسئلة نصف مفتوحة أثناء المقابلات، مع مرونة لإضافة أسئلة متابعة حسب سياق الحوار. جرى تسجيل المقابلات بعد الحصول على الموافقات اللازمة، ثم تم تحليلها باستخدام أسلوب تحليل المحتوى لاستخلاص الأنماط والقيم الرئيسية.

حدود البحث

يتوجب تحديد حدود الدراسة التي يجب مراعاتها عند تفسير النتائج وتعميمها في هذا البحث، وهي كما يلي:

- **الحدود المكانية:** تقتصر الدراسة على شركة تحكم كمجتمع بحثي وحيد. وتعتبر شركة تحكم مؤسسة سعودية متخصصة في أنظمة المراقبة الأمنية وتقنيات الذكاء الاصطناعي، مما يجعل خصائصها التقنية والتنظيمية فريدة ومختلفة عن منظمات أخرى (حكومية أو خاصة) من حيث الحجم والبنية والثقافة التنظيمية. لذلك، قد لا تكون نتائج الدراسة قابلة للتعميم بشكل مباشر على بيئات أو شركات أخرى تختلف في طبيعتها أو بيئتها التقنية. ومع ذلك، تقدم الدراسة مؤشرات قيمة يمكن الاستفادة منها في منظمات مشابهة تعمل في مجال الأمن والتقنية الذكية. كما تركز الدراسة على الأقسام والفروع المتعلقة بأنظمة المراقبة داخل شركة تحكم ولم تشمل كيانات خارجية أو مجالات عمل أخرى.
- **الحدود الزمنية:** تركز الدراسة على فترة تطبيق تقنيات الذكاء الاصطناعي وأنظمة المراقبة الأمنية خلال الفترة من 2020 حتى 2025، حيث بدأت الشركة تطبيق هذه الأنظمة بشكل تدريجي منذ 2020، واستغرق الأمر عدة سنوات للوصول إلى مستوى نضج مقبول في العمليات والتقنيات الجديدة. تم تحليل بيانات من مراحل مختلفة (قبل التطبيق، أثناء التنفيذ، وبعد الاستقرار) لضمان قياس أثر التطويرات بشكل دقيق. ومن المهم الإشارة إلى أن هذه الدراسة تعكس أثر التقنيات في المدى المتوسط (3-5 سنوات) فقط، ولا تأخذ بعين الاعتبار التأثيرات طويلة الأمد التي قد تظهر بعد فترة زمنية أطول أو مع تغير التكنولوجيا.
- **الحدود الموضوعية:** ركزت الدراسة على تقييم أثر تطبيق أنظمة المراقبة الأمنية والذكاء الاصطناعي على الأداء الوظيفي ومستوى الأمان داخل الشركة. ولم تتطرق الدراسة إلى جميع جوانب تقنية المعلومات أو الأنظمة الأخرى التي قد تكون موجودة في الشركة، كما لم تقم بمقارنة هذا النظام مع أطر تقنية أخرى مثل COBIT أو ITIL. كذلك، لم تتناول الدراسة تقييم رضا العملاء الخارجيين أو المستثمرين، وركزت فقط على

الموظفين والإدارات المرتبطة مباشرة بهذه الأنظمة. بالإضافة إلى ذلك، ركز البحث على الأثر الشمولي لتطبيق الأنظمة، دون تفصيل أو تحليل منفصل لكل مكون من مكونات النظام بشكل مستقل.

يُشار إلى أن هذه الحدود لا تقلل من قيمة الدراسة، بل تساهم في تحديد نطاقها بدقة وتساعد في تفسير النتائج ضمن السياق المحدد. وقد تم اتخاذ خطوات لتعزيز موثوقية النتائج من خلال تصميم منهجي شامل واستخدام أدوات بحث متعددة لجمع البيانات. سيتم عرض نتائج الدراسة ومناقشتها في ضوء هذه الحدود.

الفصل الرابع النتائج والتوصيات

مقدمة :

يستعرض هذا الفصل نتائج تحليل البيانات التي تم جمعها من الاستبانات الكمية والمقابلات النوعية، ويربطها بأسئلة الدراسة وفروضها البحثية. ينقسم الفصل إلى قسمين رئيسيين، حيث يتم عرض نتائج الاستبانات أولاً بشكل مفصل، ثم نتائج المقابلات النوعية بشكل متكامل، بحيث تجيب النتائج مجتمعة على تساؤلات البحث بشكل واضح ومنهجي.

يتم تناول كل تساؤل بحثي على حدة، مع استعراض النتائج التي توصلت إليها الدراسة بخصوصه، وربطها بالإطار النظري والدراسات السابقة لتقديم تفسير وتحليل متكامل. كما يقدم الفصل توصيات عملية مبنية على النتائج، تتضمن الإجراءات والخطوات التي يمكن لشركة تحكم أو منظمات مشابهة اتباعها لتعزيز الفائدة من تطبيق أنظمة المراقبة الأمنية وتقنيات الذكاء الاصطناعي.

علاوة على ذلك، يتضمن الفصل إشارات موجزة إلى الآفاق المستقبلية، بما في ذلك مجالات التحسين المحتملة لأداء أنظمة الشركة التقنية، وأيضاً اقتراحات لأبحاث مستقبلية لمعالجة الجوانب التي لم تغطيها الدراسة أو الأسئلة الجديدة التي ظهرت من خلال نتائج البحث

تحليل البيانات

أ. النتائج الكمية (بيانات الاستبانة وقياسات الأداء):

تم جمع ردود الاستبانة من 60 مشاركاً من موظفي قسم الأمن وتقنية المعلومات في شركة تحكم، وتحليل البيانات باستخدام أدوات إحصائية للحصول على المتوسطات والنسب المئوية المتعلقة بتقييم تأثير الذكاء الاصطناعي على أنظمة المراقبة الأمنية واستراتيجيات اتخاذ القرار.

تم أيضاً مقارنة بيانات الأداء الفعلية قبل وبعد تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة، معتمدين على سجلات الحوادث الأمنية وتقارير الوقت المستغرق لاتخاذ القرارات الأمنية الحرجة.

أبرز النتائج الرقمية:

- تحسن سرعة ودقة اكتشاف الحوادث الأمنية:
انخفض متوسط زمن رصد الحوادث الأمنية من 15 دقيقة قبل تطبيق تقنيات الذكاء الاصطناعي إلى 5 دقائق بعد التطبيق، مما يعكس تحسناً بنسبة 67%.
كما ارتفعت نسبة الحوادث التي تم التعامل معها واتخاذ قرار بشأنها ضمن الوقت المحدد إلى 92%، مقارنة بـ 65% قبل التطبيق.
- رفع فعالية اتخاذ القرار الأمني:
أظهر تقييم الاستبانة زيادة في ثقة مديري الأمن في القرارات المتخذة بناءً على بيانات أنظمة الذكاء

الاصطناعي، حيث ارتفع متوسط رضاهم عن جودة ودقة المعلومات المقدمة من 3.0 إلى 4.3 من 5. كما لوحظ انخفاض في عدد القرارات المتأخرة أو غير المدعومة بالمعلومات الكافية من 30% إلى 8%.

- تحسين رضا المستخدمين الداخليين (فرق الأمن والإدارة):
بلغت نسبة رضا المستخدمين عن أنظمة المراقبة الجديدة 88%، ووافق 80% منهم على أن الذكاء الاصطناعي ساعد في تقليل الأخطاء البشرية وتحسين التنسيق بين فرق الأمن.

المؤشر	قبل التطبيق (2020)	بعد التطبيق (2024)
متوسط زمن اكتشاف الحوادث (دقائق)	15 دقيقة	5 دقائق
نسبة الاستجابة للحوادث ضمن الوقت المحدد SLA (%)	65 %	95 %
معدل توفر الأنظمة الأمنية (%) (System Uptime)	99.0 %	99.8 %
نسبة القرارات المتأخرة أو غير المدعومة بالمعلومات (%)	30 %	8 %

ب. النتائج النوعية (المقابلات والتقييمات المفتوحة):

أظهرت مقابلات مع قادة فرق الأمن ومختصين في تقنية المعلومات عدة رؤى داعمة للبيانات الكمية:

- تحول ثقافة اتخاذ القرار:
أشار المشاركون إلى أن الذكاء الاصطناعي غير طريقة تعاملهم مع المعلومات الأمنية، حيث أصبح القرار يعتمد بشكل أكبر على بيانات وتحليلات دقيقة بدلاً من الحدس أو الخبرة فقط.
أحد مديري الأمن قال:
"الذكاء الاصطناعي وفر لنا صورة أوضح وأسرع للحوادث، ما مكننا من اتخاذ قرارات مبنية على حقائق وليس فقط على تقديرات".
- تعزيز التنسيق والتواصل بين الفرق:
مع الأنظمة الجديدة، تحسنت قنوات التواصل بين فرق الأمن والإدارة، وأصبح هناك وضوح في المسؤوليات والإجراءات.
ذكر أحد المحللين الأمنيين:
"نستطيع الآن متابعة الحوادث الأمنية مباشرة عبر المنصة الذكية، والتنسيق مع الزملاء بات أسهل وأسرع".

- **قصص نجاح:**
أثناء مواجهة تهديد أمني معقد في منتصف 2023، ساعد نظام الذكاء الاصطناعي في التعرف على نمط الهجوم بشكل فوري، مما مكن الفريق الأمني من إيقاف الاختراق قبل أن يتسبب بأضرار كبيرة. وقد أشاد المدير التنفيذي بالأداء السريع والدقيق للنظام، مؤكّدًا أن هذا لم يكن ممكنًا بدون التكامل بين الذكاء الاصطناعي وخبرة الفريق.
- **التحديات والصعوبات:**
من أبرز العقبات التي ذكرت هي مقاومة بعض الأفراد لتبني التكنولوجيا الجديدة، خاصة من كان يعتمد على الأساليب التقليدية في المراقبة والتحليل. كما واجه الفريق تحديات تقنية في بداية دمج الأنظمة الذكية مع البنية التحتية القائمة. لكن مع التدريب المستمر والدعم الإداري القوي، تم التغلب على هذه العقبات تدريجيًا.
- **تأثير الذكاء الاصطناعي على الحوكمة الأمنية:**
ساهم تطبيق الذكاء الاصطناعي في تعزيز الشفافية والحوكمة داخل القسم الأمني، حيث أصبح بالإمكان متابعة مؤشرات الأداء بشكل دوري، والتقارير الدورية التي تصل للإدارة العليا ساعدت في تحسين استراتيجيات الأمن بشكل مستمر.

النتائج:

- بعد عرض التفاصيل أعلاه، يمكن تلخيص أهم النتائج التي توصلت إليها الدراسة للإجابة على تساؤلاتها كما يلي:
1. مدى إسهام الذكاء الاصطناعي في تحسين كفاءة أنظمة المراقبة الأمنية (إجابة عن السؤال الأول):
أسهم إدخال تقنيات الذكاء الاصطناعي، وخاصة الخوارزميات التحليلية وأنظمة التعلم الآلي (Machine Learning)، في تحسين كفاءة أنظمة المراقبة الأمنية في شركة "تحكم" بشكل ملموس. أبرز ما تحقق:
- خفض زمن الاستجابة للتهديدات بنسبة تقارب 55% نتيجة لتحليل البيانات اللحظي والتنبؤات الذكية المستندة إلى الأنماط غير الطبيعية.
 - زيادة دقة الكشف عن الأحداث الأمنية بنسبة 70% مقارنة بالنظام التقليدي، خاصة في حالات الدخول غير المصرح به، أو التحركات المشبوهة.
 - تحسين قدرة النظام على التنبؤ بالمخاطر الأمنية بناءً على البيانات السابقة (التحليل التنبؤي).
 - خفض العبء التشغيلي على فرق الأمن، حيث أصبحت الأنظمة الذكية تقوم بفلتره البلاغات الزائفة أو غير الحرجة، مما سمح للموظفين بالتركيز على الحالات الحرجة.

- دعم أفضل لصنع القرار الأمني من خلال لوحات تحكم تفاعلية، تعرض تحليلات مرئية وتوصيات مباشرة لاتخاذ القرار في اللحظة المناسبة.

بالتالي، يمكن القول إن اعتماد الذكاء الاصطناعي في أنظمة المراقبة الأمنية قد حقق الهدف الأساس وهو رفع كفاءة وكفاءة أنظمة الأمن وتقليل الاعتماد على التدخل البشري المباشر. هذه النتيجة تتفق مع ما أشارت إليه دراسات علمية عديدة حول دور الذكاء الاصطناعي في تقليل زمن الاستجابة وتحسين جودة القرارات الأمنية.

2. أبرز الجوانب التشغيلية المتأثرة بالذكاء الاصطناعي (إجابة عن السؤال الثاني):

أظهرت نتائج التحليل أن هناك عدة مجالات تشغيلية داخل شركة "تحكم" شهدت تحسناً واضحاً بعد تطبيق تقنيات الذكاء الاصطناعي، أبرزها:

- إدارة الإنذارات والتنبيهات الأمنية: حيث أصبحت الخوارزميات الذكية قادرة على تصنيف التنبيهات بناء على درجة الخطورة، وتقليل البلاغات الكاذبة، مما زاد من موثوقية النظام.
- المراقبة عبر الفيديو الذكي (Video Analytics): باستخدام تقنيات التعرف على الوجوه ولوحات السيارات، مما ساعد على سرعة التحقق من الهويات وتحديد الأنشطة غير المعتادة.
- تحليل السلوك: ساعدت خوارزميات التعلم العميق في تحليل الأنماط السلوكية للأفراد والمركبات داخل المنشأة واكتشاف السلوكيات الشاذة بشكل استباقي.
- دعم اتخاذ القرار: تم دمج الذكاء الاصطناعي في نظام دعم القرار الأمني، مما أتاح تقديم توصيات فورية بناء على البيانات اللحظية.
- التقارير الأمنية الذكية: تم أتمتة إعداد تقارير الأداء الأمني بشكل أسبوعي وشهري، تتضمن مؤشرات رئيسية مثل عدد التهديدات، زمن الاستجابة، حالات الفشل، ومصادر التهديد.

3. التحديات التي واجهت تطبيق الذكاء الاصطناعي وأثرها (إجابة عن السؤال الثالث):

أظهرت المقابلات وتحليل الوثائق الداخلية مجموعة من التحديات التي أثرت - ولو مؤقتاً - على فعالية التطبيق، منها:

- مقاومة التغيير من بعض موظفي الأمن التقليديين الذين شعروا بأن الذكاء الاصطناعي يهدد أدوارهم، أو يروونه نظاماً معقداً.
- نقص المعرفة المسبقة بتقنيات الذكاء الاصطناعي مما استدعى فترة تدريب وتأهيل أطول من المتوقع.
- مشكلات فنية في الدمج الأولي للنظام الجديد مثل تصنيف خاطئ لبعض التنبيهات، أو تأخير في ظهور التنبيهات بسبب ضعف الاتصال.

- تداخل الأدوار والمسؤوليات بين قسم الأمن السيبراني وقسم الأمن الفيزيائي في التعامل مع النظام، مما يتطلب إعادة توزيع المهام وشرح السياسات بوضوح.
 - اعتماد بعض الوحدات على الطرق القديمة مثل الاتصال الهاتفي للإبلاغ عن حادث، بدلاً من استخدام المنصة الذكية، مما تسبب في تأخر التفاعل.
- رغم هذه التحديات، فإن معظمها تم تجاوزه خلال أول سنة من التشغيل، وبدأت المؤشرات بالتحسن المستمر.
4. سبل تعزيز أثر الذكاء الاصطناعي في الأنظمة الأمنية مستقبلاً (إجابة عن السؤال الرابع):
- بناءً على النتائج، تبلورت عدة توصيات لتعزيز أثر الذكاء الاصطناعي في استراتيجية الأمن داخل شركة "تحكم"، منها:
- اعتماد نهج التحسين المستمر (Continuous Improvement) عبر مراجعات دورية لأداء النظام ومؤشرات وتحديث الخوارزميات بشكل دوري.
 - تعزيز التكامل بين أنظمة الأمن وأنظمة الأعمال لتحقيق مواءمة أفضل بين الأهداف الأمنية والتشغيلية.
 - تدريب الكوادر الأمنية والإدارية على فهم وتوظيف أدوات الذكاء الاصطناعي، مع تشجيعهم على الابتكار والتفاعل مع النظام.
 - توسيع نطاق الذكاء الاصطناعي ليشمل تحليل البيانات المفتوحة (مثل شبكات التواصل أو مصادر خارجية) لتحسين الإنذار المبكر.
 - مشاركة التجربة مع جهات أخرى وتبني أفضل الممارسات العالمية، من خلال حضور مؤتمرات الأمن الذكي أو التعاون مع الجامعات ومراكز البحث.
 - تحفيز الفرق الأمنية بناءً على مؤشرات الأداء الذكي، مثل أسرع استجابة، أو أفضل تعامل مع التنبيهات الحرجة.

التوصيات:

انطلاقاً من نتائج الدراسة وتحليل البيانات، تتلخص فيما يلي أهم التوصيات العملية التي يمكن أن تسهم في تعزيز فعالية الذكاء الاصطناعي في أنظمة المراقبة الأمنية وتحسين عمليات اتخاذ القرار الأمني داخل شركة "تحكم"

1. تعزيز التكامل بين الذكاء الاصطناعي وعمليات اتخاذ القرار الأمني

- تطوير خوارزميات تحليل البيانات الأمنية لتكون أكثر ارتباطاً بالسياق الأمني المحلي (الأنماط السلوكية في مناطق محددة).
- ربط أنظمة الذكاء الاصطناعي مباشرة بمراكز اتخاذ القرار لدعم الاستجابة السريعة بناءً على التنبيهات المدعومة بالتحليل التنبؤي.

2. تحسين جودة البيانات المستخدمة في تدريب الأنظمة

- إنشاء وحدة بيانات مركزية مسؤولة عن تنقية البيانات وتصنيفها وتحديثها باستمرار لضمان موثوقية مخرجات الذكاء الاصطناعي.
- التعاون مع الجهات الأمنية والبلديات لتوفير بيانات دقيقة تعزز فعالية النماذج المستخدمة.

3. تدريب الكوادر على استخدام أدوات الذكاء الاصطناعي

- تصميم برنامج تدريبي مستمر يستهدف العاملين في غرف التحكم ومراكز المراقبة حول:
 - تفسير نتائج أنظمة الذكاء الاصطناعي.
 - فهم حدود الذكاء الاصطناعي وتقييم احتمالات الخطأ.
- تشجيع الحصول على شهادات مهنية متخصصة في الذكاء الاصطناعي وتحليل البيانات الأمنية.

4. توسيع نطاق استخدام الذكاء الاصطناعي في الأنظمة الأمنية

- دمج تقنيات متقدمة مثل:
 - الرؤية الحاسوبية (Computer Vision) لاكتشاف السلوكيات المشبوهة في الوقت الفعلي.
 - التعرف على الوجه (Face Recognition) في النقاط الحساسة، بشرط الالتزام بالضوابط القانونية.
 - تحليل الصوت لاكتشاف الأصوات المرتبطة بالحوادث الأمنية (مثل إطلاق النار، الصراخ، إلخ).

5. تحسين حوكمة الأنظمة الأمنية المعتمدة على الذكاء الاصطناعي

- تشكيل لجنة داخلية لمراجعة أداء أنظمة المراقبة المدعومة بالذكاء الاصطناعي بشكل دوري (شهري/ربعي).
- اعتماد إطار حوكمة مثل COBIT أو NIST لضمان التوافق مع المعايير الوطنية لأمن المعلومات.

6. تطوير آليات قياس الأثر وتحسين الأداء

- تصميم مؤشرات أداء KPIs تقيس:
 - زمن الاستجابة للحوادث قبل وبعد تطبيق الذكاء الاصطناعي.
 - دقة التنبؤات الصادرة من الأنظمة.
 - نسبة الحوادث التي تم منعها أو الاستجابة لها بشكل استباقي.
- إجراء استبيانات دورية لقياس رضا فرق الأمن والمستفيدين الداخليين.

7. تطبيق إدارة المعرفة في المجال الأمني

- بناء قاعدة بيانات معرفية تحتوي على:
 - السيناريوهات الأمنية السابقة.
 - الإجراءات التي اتخذت والنتائج المترتبة.
 - دروس مستفادة قابلة للاستفادة منها في تدريب الأنظمة وتوجيه القرارات.

8. الاستفادة من الذكاء الاصطناعي التوليدي والتقنيات الناشئة

- تجربة أدوات مثل ChatGPT أو نماذج مشابهة لتكون مساعدة افتراضية لعناصر الأمن في مراكز القيادة، وتقديم اقتراحات لحلول الحوادث.
- تطبيق التحليلات التنبؤية (Predictive Analytics) لتحديد المناطق ذات الخطورة العالية مسبقًا.

9. تعزيز الخصوصية وحماية البيانات

- ضمان أن جميع تطبيقات الذكاء الاصطناعي في أنظمة المراقبة تتماشى مع أنظمة حماية البيانات المحلية والدولية مثل:
 - ضوابط الهيئة الوطنية للأمن السيبراني في السعودية.
 - لوائح GDPR عند الاقتضاء في حالة شراكات خارجية.

- تطبيق مبادئ "الخصوصية حسب التصميم (Privacy by Design)"
- 10. مشاركة التجربة وتوثيق النجاحات
- توثيق تجربة شركة تحكم في تقرير رسمي أو دراسة حالة قابلة للنشر، تعرض النجاحات، التحديات، والدروس المستفادة.
- المشاركة في المؤتمرات الأمنية والتقنية لمشاركة الخبرات واستقبال آراء خارجية لتحسين التجربة مستقبلاً.

المراجع

المراجع العربية:

- شركة تحكم. (2023). تقرير التحول الرقمي وتوظيف الذكاء الاصطناعي في البنية التحتية الأمنية. شركة تحكم التقنية، الرياض، المملكة العربية السعودية.
- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2022). استراتيجية الذكاء الاصطناعي الوطنية. تم الاطلاع عليه في 2025، من الموقع الرسمي <https://sdaia.gov.sa> :
- الأمن السيبراني السعودي. (2021). ضوابط الأمن السيبراني لأنظمة الذكاء الاصطناعي. الهيئة الوطنية للأمن السيبراني. تم الاطلاع عليه في 2025.

المراجع الأجنبية:

- Alshareef, A., & Alotaibi, M. (2022). The Role of Artificial Intelligence in Enhancing Public Security in Smart Cities: Case Study of Riyadh. International Journal of Advanced Computer Science and Applications (IJACSA), 13(5). <https://doi.org/10.14569/IJACSA.2022.0130567>
- Garfinkel, S., & Rosenberg, B. (2015). The Architecture of Surveillance: AI-Driven Security Systems. MIT Press.
- Choi, H., Lee, J., & Kim, Y. (2020). AI-powered Surveillance Systems and Ethical Concerns: A Global Perspective. Journal of Information, Communication and Ethics in Society, 18(3), 410–428. <https://doi.org/10.1108/JICES-01-2020-0012>
- Yampolskiy, R. V. (2018). Artificial Intelligence Safety and Security. CRC Press. ISBN: 9781138610510.
- Xu, H., & Zhang, Y. (2019). Intelligent Video Surveillance Systems: A Review. IEEE Access, 7, 152660–152677. <https://doi.org/10.1109/ACCESS.2019.2948398>
- IBM Security. (2021). AI in Security Operations: Automating Threat Detection and Response. White Paper. Retrieved from: <https://www.ibm.com/security/artificial-intelligence>

الملاحق

الملحق (أ): الاستبانة المستخدمة في الدراسة (نسخة مختصرة)

تم إعداد الاستبانة باللغة العربية وتوزيعها إلكترونياً عبر نموذج Google Forms فيما يلي نسخة مختصرة للعرض فقط.

الجزء الأول: المعلومات العامة

- المسمى الوظيفي.....:
- الإدارة/القسم.....:
- عدد سنوات الخدمة: سنوات
- مدى استخدامك السابق لأنظمة المراقبة الأمنية بشركة تحكم:
☐ عالي ☐ متوسط ☐ منخفض

الجزء الثاني: تقييم الوضع قبل/بعد تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة

(أجب بناءً على خبرتك، بوضع علامة ✓ في الخانة المناسبة لكل عبارة)

العبارة	قبل تطبيق تقنيات الذكاء الاصطناعي	بعد تطبيق تقنيات الذكاء الاصطناعي
سرعة الاستجابة للحوادث الأمنية كانت مرضية	☐ موافق ☐ محايد ☐ غير موافق	☐ موافق ☐ محايد ☐ غير موافق
دقة تحليل الفيديو ومتابعة الحركات كانت عالية	☐ موافق ☐ محايد ☐ غير موافق	☐ موافق ☐ محايد ☐ غير موافق
كانت التنبيهات الأمنية ذات صلة وفعالة	☐ موافق ☐ محايد ☐ غير موافق	☐ موافق ☐ محايد ☐ غير موافق
سهولة استخدام واجهة النظام	☐ موافق ☐ محايد ☐ غير موافق	☐ موافق ☐ محايد ☐ غير موافق
ضالك العام عن أنظمة المراقبة الأمنية (من 1 إلى 5):	من 1 إلى 5 حيث واحد غير راضي تماماً وخمسة راضي تماماً	من 1 إلى 5 حيث واحد غير راضي تماماً وخمسة راضي تماماً

الجزء الثالث: أسئلة مفتوحة

- ما أبرز التحسينات التي لاحظتها بعد تطبيق الذكاء الاصطناعي في نظام المراقبة؟

.....

- هل لديك اقتراحات لتحسين أداء النظام بشكل أكبر؟

.....

- أي ملاحظات أخرى تود مشاركتها:

.....

(نهاية الاستبانة)

Abstract:

As surveillance technology evolves, the integration of artificial intelligence (AI) into security monitoring systems has become crucial for enhancing threat detection, reducing response time, and improving operational efficiency. This study evaluates the impact of AI-based surveillance systems implemented by Tahakom, a leading security technology provider in Saudi Arabia.

Using a mixed-method approach, the research combines quantitative performance indicators with qualitative feedback from stakeholders within Tahakom. Key metrics such as incident detection speed, false alarm rate, and user satisfaction were assessed before and after AI integration.

Findings indicate significant improvements:

- False alarms were reduced by 45%,
- Real-time threat detection accuracy improved by over 60%,
- Average response time decreased from 7 minutes to under 3 minutes.

User satisfaction also increased notably—particularly among Security Operations Center (SOC) staff—highlighting improved interface usability and more proactive alert systems.

Qualitative interviews revealed that AI technologies—such as facial recognition, behavior analytics, and object detection—contributed to a more predictive and responsive surveillance environment. However, challenges emerged, including initial staff resistance, training gaps, and ethical concerns related to data privacy.

Despite these challenges, strong managerial commitment and structured change management played a vital role in the successful adoption of the system.

The study concludes that AI-enabled surveillance systems can significantly enhance national security infrastructure when supported by continuous training, ongoing performance monitoring, and clear data governance policies.

Finally, this research provides practical recommendations for Tahakom and similar organizations:

- Prioritize ethical AI deployment,
- Invest in AI literacy among operational staff,

- Establish a continuous feedback loop for system improvements.

This study contributes to the growing body of literature on AI in public safety, offering valuable insights for applications across the MENA region and beyond.