

## مشروع خطة أطروحة للتسجيل لدرجة الدكتوراه

### العنوان باللغة العربية/

تقييم كفاءة أنظمة المراقبة الذكية في الأمن الصناعي: دراسة ميدانية حول تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات

### العنوان باللغة الإنجليزية/

Evaluation of the Efficiency of Intelligent Monitoring Systems in Industrial Security: A Field Study on Artificial Intelligence Applications in Threat Detection

|                 |                        |
|-----------------|------------------------|
| اسم الباحث      | سلطان سعد محمد ال حميد |
| الرقم الأكاديمي | ٢٢٢٠٠١٢٧٥              |
| الكلية          | الادارة                |

٢٠٢٥ م

## قائمة المحتويات:

|    |                                     |
|----|-------------------------------------|
| ٣  | مقدمة الدراسة:                      |
| ٤  | مشكلة الدراسة:                      |
| ٥  | أهمية الدراسة:                      |
| ٧  | أهداف الدراسة:                      |
| ٨  | تساؤلات الدراسة:                    |
| ٩  | فروض الدراسة:                       |
| ١٠ | الإطار النظري للدراسة:              |
| ١٢ | الدراسات السابقة:                   |
| ١٦ | التعليق على الدراسات السابقة:       |
| ١٩ | أوجه الاستفادة من الدراسات السابقة: |
| ٢١ | مفاهيم الدراسة:                     |
| ٢٣ | الإجراءات المنهجية للدراسة:         |
| ٢٥ | أدوات جمع بيانات الدراسة:           |
| ٢٧ | التبويب المقترح لفصول الدراسة:      |
| ٣٠ | المراجع:                            |

## مقدمة الدراسة:

في ظل التطورات التكنولوجية المتسارعة، أصبح الأمن الصناعي من المجالات التي تشهد تحولات جوهرية نتيجة إدماج التقنيات الذكية في أنظمة الحماية والمراقبة. فمع تزايد المخاطر الأمنية التي تهدد المنشآت الصناعية، لم يعد الاعتماد على الأساليب التقليدية في الحماية كافياً لضمان بيئة عمل آمنة ومستدامة. ومع ظهور الذكاء الاصطناعي، برزت أنظمة المراقبة الذكية كحلول متطورة قادرة على تحسين قدرة المنشآت الصناعية على الكشف عن التهديدات والتعامل معها بشكل أكثر كفاءة ودقة (George، ٢٠٢٤).

تُعد أنظمة المراقبة الذكية امتداداً للتطور الطبيعي لوسائل الحماية التي بدأت بالكاميرات التقليدية وأجهزة الإنذار البسيطة، لكنها اليوم تعتمد على تقنيات متقدمة مثل التعلم العميق، وتحليل البيانات، ومعالجة الصور والفيديو. هذه التقنيات تتيح لأنظمة الأمن الصناعي التمييز بين الأنشطة الطبيعية وغير الطبيعية داخل المنشآت، مما يساهم في تقليل نسبة الإنذارات الكاذبة وزيادة الاستجابة السريعة للحوادث الأمنية. كما أن قدرة هذه الأنظمة على تحليل السلوكيات غير الاعتيادية وتوقع الأخطار قبل وقوعها يمنح المؤسسات فرصة لاتخاذ التدابير الاستباقية اللازمة لتجنب وقوع الأضرار (Al-Hashemi، ٢٠٢٤).

من ناحية أخرى، فإن الاعتماد على الذكاء الاصطناعي في المراقبة الصناعية لا يقتصر على تحديد التهديدات الأمنية فقط، بل يمتد ليشمل تقييم المخاطر التشغيلية مثل الأعطال الفنية والتسربات الغازية أو الحرائق. فمن خلال تقنيات الاستشعار وتحليل البيانات الضخمة، يمكن لأنظمة المراقبة الذكية رصد المؤشرات المبكرة للأعطال الميكانيكية أو البيئية، مما يساعد على تقليل فترات التوقف عن العمل وتحسين كفاءة التشغيل. وبالتالي، فإن تأثير الذكاء الاصطناعي على الأمن الصناعي لا يقتصر فقط على الحماية الأمنية، بل يتجاوزها إلى تحسين استمرارية الأعمال وتقليل الخسائر المادية والبشرية (Yazdi، ٢٠٢٤).

لكن رغم الفوائد العديدة لأنظمة المراقبة الذكية، فإن تطبيقها يواجه بعض التحديات التي قد تؤثر على فعاليتها. من بين هذه التحديات، مسألة التكلفة العالية لتطوير وتطبيق الأنظمة المتقدمة، فضلاً عن الحاجة إلى بنية تحتية قوية لمعالجة البيانات بكفاءة. كما أن خصوصية البيانات وحماية المعلومات تعد من الجوانب الحساسة التي تحتاج إلى حلول متقدمة لضمان عدم

اختراق الأنظمة أو إساءة استخدامها. بالإضافة إلى ذلك، فإن دمج هذه الأنظمة يتطلب تدريباً مكثفاً للعاملين على كيفية التعامل معها وتحليل مخرجاتها بالشكل الصحيح لضمان تحقيق أقصى استفادة منها (Renukappa، ٢٠٢٢).

تهدف هذه الدراسة إلى تقييم كفاءة أنظمة المراقبة الذكية في الأمن الصناعي، وذلك من خلال دراسة ميدانية تستعرض تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات، ومدى فعاليتها في تحسين مستوى الأمان داخل المنشآت الصناعية. كما ستسعى الدراسة إلى تحديد أهم العوامل المؤثرة في نجاح هذه الأنظمة، وتسلط الضوء على التحديات التي تواجهها المؤسسات عند تطبيقها. من خلال ذلك، يمكن الوصول إلى رؤية واضحة حول كيفية توظيف الذكاء الاصطناعي في تعزيز الأمن الصناعي بشكل أكثر كفاءة واستدامة.

### مشكلة الدراسة:

يعد الأمن الصناعي من القضايا الحيوية التي تؤثر بشكل مباشر على سلامة الأفراد والمنشآت واستمرارية العمليات الإنتاجية في مختلف القطاعات. فمع تزايد حجم المنشآت الصناعية وتعقيد أنظمتها التشغيلية، برزت الحاجة الملحة لاعتماد تقنيات حديثة تضمن حماية متكاملة من المخاطر الأمنية المتنوعة، مثل التسلل غير المشروع، السرقات، الحوادث الناجمة عن الأعطال الميكانيكية، والتسريبات الخطرة. في هذا السياق، لعبت أنظمة المراقبة الذكية دوراً محورياً في تعزيز تدابير الأمن الصناعي، حيث تعتمد هذه الأنظمة على تقنيات الذكاء الاصطناعي مثل التعلم العميق، تحليل البيانات، والتعرف على الأنماط السلوكية، مما يمكنها من كشف التهديدات بسرعة وكفاءة تفوق الأساليب التقليدية.

ورغم التقدم الذي أحرزته أنظمة المراقبة الذكية، إلا أن فعاليتها الفعلية في البيئات الصناعية لا تزال موضع تساؤل. فمن ناحية، توفر هذه الأنظمة قدرات متقدمة في تحليل الفيديو والتنبؤ بالمخاطر، ولكن من ناحية أخرى، تواجه تحديات تتعلق بدقة الكشف، تكاليف التطبيق، ومدى تكيفها مع البيئات الصناعية المختلفة. علاوة على ذلك، فإن هذه الأنظمة تعتمد على كميات هائلة من البيانات، مما يطرح إشكاليات تتعلق بحماية الخصوصية وأمن المعلومات، لا سيما في ظل التهديدات السيبرانية

المتزايدة. وبالتالي، هناك حاجة ملحة إلى تقييم مدى كفاءة هذه الأنظمة، ليس فقط من حيث قدرتها على اكتشاف التهديدات، بل أيضًا من حيث موثوقيتها، تكلفتها، وإمكانية تكاملها مع الأنظمة الأمنية التقليدية (Rodríguez-Espíndola، ٢٠٢٢).

وتتجلى المشكلة البحثية لهذه الدراسة في الفجوة المعرفية المتعلقة بمدى فعالية أنظمة المراقبة الذكية في البيئات الصناعية المختلفة، حيث إن معظم الدراسات السابقة تركز على تطبيقات هذه الأنظمة في المجالات المدنية والتجارية، بينما تفتقر الأدبيات العلمية إلى تقييم شامل لمدى نجاحها في البيئات الصناعية التي تتطلب استجابة أكثر تعقيدًا وفعالية. كما أن التطورات المستمرة في الذكاء الاصطناعي تفرض ضرورة مراجعة كفاءة هذه الأنظمة بانتظام، خاصة مع ظهور تحديات جديدة تتعلق بالتكيف مع الظروف البيئية القاسية، دقة التحليل، وقدرة الأنظمة على العمل في الوقت الفعلي دون تأخير أو أخطاء تؤثر على قرارات الأمن والسلامة.

وانطلاقًا من هذا الأساس النظري، فإن الدراسة تستند إلى مفهوم الأمن الصناعي باعتباره مزيجًا من الإجراءات التقنية والإدارية التي تهدف إلى تقليل المخاطر والحفاظ على استمرارية الأعمال. كما تعتمد على نظرية "الإدارة القائمة على البيانات" التي تؤكد أهمية التحليل المستند إلى الذكاء الاصطناعي في اتخاذ قرارات أمنية أكثر دقة وفعالية. ويأتي ذلك في إطار التحول الرقمي الذي تشهده القطاعات الصناعية، والذي يتطلب تكامل الحلول الذكية مع الأنظمة التشغيلية لضمان تحقيق أقصى درجات الأمان والاستدامة.

وبناءً على ما سبق، تتمحور مشكلة الدراسة حول السؤال الرئيسي التالي: إلى أي مدى تُعد أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي فعالة في الكشف عن التهديدات الأمنية في المنشآت الصناعية، وما العوامل التي تؤثر على كفاءتها؟

### أهمية الدراسة:

يشكل الأمن الصناعي أحد الركائز الأساسية التي تعتمد عليها المنشآت الصناعية لضمان استمرارية عملياتها التشغيلية وحماية الأفراد والممتلكات من المخاطر المحتملة. في ظل التحولات الرقمية المتسارعة، أصبح من الضروري دمج التقنيات الحديثة، وعلى رأسها أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي، لتعزيز مستويات الحماية والكشف المبكر عن التهديدات

الأمنية. ومع ذلك، فإن نجاح هذه الأنظمة في تحقيق أهدافها يتطلب تقييمًا دقيقًا لكفاءتها ومدى فعاليتها في مختلف البيئات الصناعية. ومن هنا، تبرز أهمية هذه الدراسة من حيث الجوانب النظرية والتطبيقية التي تسعى إلى تقديمها.

### - الأهمية النظرية

تتبع الأهمية النظرية لهذه الدراسة من مساهمتها في إثراء المعرفة العلمية حول تطبيقات الذكاء الاصطناعي في مجال الأمن الصناعي. فعلى الرغم من التطور الكبير في مجال تقنيات المراقبة الذكية، إلا أن الأبحاث الأكاديمية حول كفاءتها الفعلية في الكشف عن التهديدات في البيئات الصناعية لا تزال محدودة. تركز معظم الدراسات الحالية على استخدام الذكاء الاصطناعي في المجالات المدنية والتجارية، مثل أنظمة التعرف على الوجوه في الأماكن العامة أو تحليل سلوك العملاء في المتاجر، بينما تنقر الأدبيات العلمية إلى تقييم معمق لتطبيقات هذه الأنظمة في البيئات الصناعية التي تتطلب معايير أمنية أكثر تعقيدًا.

كما أن الدراسة تستند إلى عدة نظريات علمية حديثة، مثل نظرية "الإدارة القائمة على البيانات"، التي توضح أهمية تحليل البيانات الضخمة لاتخاذ قرارات أمنية أكثر دقة، ونظرية "التعلم العميق" التي تعزز قدرة أنظمة المراقبة على التكيف مع أنماط التهديدات الجديدة. ومن خلال تحليل هذه المفاهيم وتطبيقها على الأمن الصناعي، تسهم الدراسة في بناء إطار معرفي متكامل يساعد الباحثين والممارسين في تطوير استراتيجيات أكثر فاعلية لمواجهة المخاطر الأمنية في المنشآت الصناعية.

فإن هذه الدراسة تفتح المجال لمناقشة القضايا الأخلاقية والقانونية المتعلقة باستخدام الذكاء الاصطناعي في المراقبة الأمنية، مثل حماية الخصوصية والحد من الاستخدامات غير المشروعة لهذه التقنيات. ومن خلال تقديم تحليل متوازن لهذه الجوانب، يمكن أن تسهم الدراسة في توجيه السياسات والإجراءات التنظيمية التي تحكم استخدام أنظمة المراقبة الذكية في البيئات الصناعية (Qin، ٢٠٢٣).

### - الأهمية التطبيقية

أما من الناحية التطبيقية، فإن هذه الدراسة توفر تقييمًا عمليًا لكفاءة أنظمة المراقبة الذكية في المنشآت الصناعية، مما يساعد على تحسين مستوى الأمان وتعزيز الاستجابة السريعة للتهديدات الأمنية. تعتمد الكثير من المنشآت الصناعية حاليًا على أنظمة تقليدية للمراقبة، مثل كاميرات الدوائر التلفزيونية المغلقة (CCTV) وأجهزة الاستشعار البسيطة، التي غالبًا ما تكون غير

قادرة على تحليل البيانات بشكل متقدم أو التنبؤ بالمخاطر قبل وقوعها. ومن خلال تحليل الأداء الفعلي لأنظمة الذكاء الاصطناعي في الكشف عن التهديدات المختلفة، يمكن لهذه الدراسة أن توفر رؤى عملية تساعد المؤسسات الصناعية في اتخاذ قرارات مستنيرة حول كيفية تحسين أنظمتها الأمنية.

كما تساعد نتائج الدراسة الشركات والمصانع على تقليل الخسائر البشرية والمادية من خلال توفير حلول وقائية تعتمد على البيانات والتحليل الفوري. على سبيل المثال، يمكن لأنظمة المراقبة الذكية المجهزة بتقنيات الذكاء الاصطناعي تحليل تسجيلات الفيديو الحية للكشف عن أي سلوك غير طبيعي، مثل دخول غير مصرح به إلى مناطق حساسة أو حدوث اشتعال في أماكن العمل، ومن ثم إرسال تنبيهات فورية إلى المسؤولين لاتخاذ الإجراءات اللازمة. هذا النوع من التكنولوجيا يمكن أن يسهم في تقليل زمن الاستجابة للحوادث، مما يقلل من مخاطر الأضرار الجسيمة.

كما أن الدراسة تسهم في توجيه السياسات الأمنية داخل المنشآت الصناعية، حيث يمكن أن توفر توصيات عملية حول كيفية تحسين تكامل أنظمة المراقبة الذكية مع بقية أنظمة الأمن والسلامة، مثل أنظمة مكافحة الحرائق وأجهزة الاستشعار البيئية. وبذلك، تساعد نتائج الدراسة في تطوير بيئة صناعية أكثر ذكاءً وأمانًا، خاصة في ظل تزايد التحديات الأمنية التي تواجه المنشآت الصناعية الحديثة (Myagmar-Ochir، ٢٠٢٣).

## أهداف الدراسة:

في ظل التقدم التكنولوجي المتسارع وتزايد الحاجة إلى تعزيز معايير الأمن الصناعي، تأتي هذه الدراسة لتقييم كفاءة أنظمة المراقبة الذكية التي تعتمد على الذكاء الاصطناعي في الكشف عن التهديدات المحتملة داخل البيئات الصناعية. يهدف البحث إلى تقديم تحليل شامل لكيفية توظيف هذه التقنيات في رفع مستوى الأمان وتحسين سرعة ودقة الاستجابة للمخاطر.

### - الهدف الرئيسي

✓ تقييم كفاءة أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي في تحسين الأمن الصناعي من خلال الكشف المبكر عن التهديدات وتحليل مدى فعاليتها مقارنة بالأنظمة التقليدية.

## - الأهداف الفرعية

١. تحليل مدى دقة وفعالية أنظمة المراقبة الذكية في التعرف على التهديدات الأمنية المختلفة في البيئات الصناعية.
٢. تقييم مدى سرعة استجابة أنظمة المراقبة الذكية للحوادث الأمنية بالمقارنة مع الأساليب التقليدية.
٣. دراسة تأثير استخدام الذكاء الاصطناعي في تقليل الأخطاء البشرية وتحسين كفاءة إدارة المخاطر الأمنية.
٤. تحليل مدى تكامل أنظمة المراقبة الذكية مع بقية أنظمة الأمن الصناعي (مثل أنظمة مكافحة الحرائق، والتحكم في الدخول، وأجهزة الاستشعار البيئية).
٥. تقديم توصيات علمية وعملية حول أفضل الممارسات لاستخدام أنظمة المراقبة الذكية في المنشآت الصناعية، مع اقتراح معايير لتطوير وتحسين هذه الأنظمة.

## تساؤلات الدراسة:

في ظل التطورات التكنولوجية المتسارعة وتزايد الحاجة إلى تعزيز معايير الأمن الصناعي، تبرز أهمية تقييم كفاءة أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي في الكشف عن التهديدات. لذلك، تسعى هذه الدراسة إلى الإجابة على التساؤل الرئيسي التالي:

## - السؤال الرئيسي

- ✓ إلى أي مدى تُعد أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي فعالة في الكشف عن التهديدات وتحسين مستوى الأمن الصناعي مقارنة بالأنظمة التقليدية؟

## - التساؤلات الفرعية

١. ما مدى دقة وفعالية أنظمة المراقبة الذكية في التعرف على التهديدات الأمنية المختلفة داخل البيئات الصناعية؟
٢. كيف تؤثر سرعة استجابة أنظمة المراقبة الذكية في تقليل المخاطر الأمنية مقارنة بالأساليب التقليدية؟
٣. ما الدور الذي يلعبه الذكاء الاصطناعي في تقليل الأخطاء البشرية وتعزيز كفاءة إدارة المخاطر في الأمن الصناعي؟

٤. إلى أي مدى يمكن تحقيق تكامل بين أنظمة المراقبة الذكية وبقية أنظمة الأمن الصناعي، مثل أنظمة مكافحة الحرائق والتحكم في الدخول؟

٥. ما التحديات التقنية والاقتصادية التي تواجه تطبيق أنظمة المراقبة الذكية في المنشآت الصناعية، وما الحلول المقترحة لتطويرها؟

### فروض الدراسة:

تعتمد هذه الدراسة على اختبار مجموعة من الفرضيات التي تهدف إلى تقييم كفاءة أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي في الكشف عن التهديدات وتعزيز الأمن الصناعي. وتقوم الفرضيات على أساس العلاقة بين الذكاء الاصطناعي وكفاءة أنظمة المراقبة من حيث الدقة، والسرعة، وتقليل الأخطاء البشرية، ومدى التكامل مع الأنظمة الأمنية الأخرى، والتحديات المرتبطة بتطبيقها.

#### - الفرضية الرئيسية

✓ تُساهم أنظمة المراقبة الذكية المعتمدة على الذكاء الاصطناعي بشكل فعال في تحسين مستوى الأمن الصناعي من خلال الكشف الدقيق عن التهديدات وتقليل المخاطر مقارنة بالأنظمة التقليدية.

#### - الفروض الفرعية

١. تتميز أنظمة المراقبة الذكية بدقة وكفاءة أعلى في التعرف على التهديدات الأمنية مقارنة بالأنظمة التقليدية المستخدمة في الأمن الصناعي.

٢. تساهم تقنيات الذكاء الاصطناعي في تقليل زمن الاستجابة للحوادث الأمنية، مما يؤدي إلى تحسين قدرة المنشآت الصناعية على التعامل مع المخاطر في الوقت الفعلي.

٣. يؤدي الاعتماد على الذكاء الاصطناعي في أنظمة المراقبة الذكية إلى تقليل الأخطاء البشرية في تقدير التهديدات واتخاذ القرارات الأمنية.

٤. يمكن لأنظمة المراقبة الذكية أن تعمل بفعالية أكبر عند تكاملها مع أنظمة الأمن الصناعي الأخرى، مثل أنظمة مكافحة الحرائق والتحكم في الدخول والاستشعار البيئي.

٥. توجد تحديات تقنية واقتصادية تحدّ من تبني أنظمة المراقبة الذكية في المنشآت الصناعية، إلا أنه يمكن التغلب عليها من خلال تبني استراتيجيات متقدمة لتطوير وتحسين هذه الأنظمة.

### الإطار النظري للدراسة:

يعتبر الأمن الصناعي من الركائز الأساسية التي تعتمد عليها المنشآت الصناعية لضمان حماية الموارد البشرية والمادية من المخاطر المحتملة. ومع تطور التكنولوجيا، أصبحت أنظمة المراقبة تلعب دورًا أساسيًا في تحقيق هذا الهدف، حيث انتقلت من الاعتماد على الوسائل التقليدية، مثل كاميرات المراقبة وأفراد الأمن، إلى تقنيات أكثر تطورًا تعتمد على الذكاء الاصطناعي. ويعد هذا التحول نتيجة مباشرة لتزايد التهديدات الأمنية وتنامي الحاجة إلى أنظمة قادرة على الاستجابة بسرعة وكفاءة عالية. تتناول هذه الدراسة تقييم كفاءة أنظمة المراقبة الذكية في الأمن الصناعي، مع التركيز على تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات وتحليل مدى فاعلية هذه التقنيات مقارنة بالأساليب التقليدية.

### - مفهوم الأمن الصناعي وأنظمة المراقبة الذكية

يرتبط الأمن الصناعي بمجموعة من التدابير والأنظمة المصممة لحماية المنشآت الصناعية والعاملين فيها من المخاطر التي قد تنتج عن الأعطال الفنية، الحرائق، الحوادث، أو التهديدات الأمنية المختلفة. مع تقدم التكنولوجيا، أصبح من الضروري تطوير أنظمة مراقبة أكثر تطورًا، قادرة على التفاعل في الوقت الفعلي مع التهديدات المحتملة. ظهرت أنظمة المراقبة الذكية كأحد الحلول الرائدة في هذا المجال، حيث تعتمد على تقنيات مثل الذكاء الاصطناعي، التعلم الآلي، وإنترنت الأشياء لتحليل البيانات واستشعار الأخطار المحتملة. تتميز هذه الأنظمة بقدرتها على التعرف على الأنماط غير الطبيعية والتنبؤ بالحوادث قبل وقوعها، مما يساعد في تقليل الخسائر وتعزيز كفاءة التدخل السريع (Ganeshan، ٢٠١٨).

## - الأساس النظري للدراسة: نظرية النظم الذكية

تعتمد هذه الدراسة على نظرية النظم الذكية التي تفسر كيفية عمل الأنظمة الذكية في بيئات معقدة تتطلب تفاعلاً سريعاً واتخاذ قرارات آنية. تفترض هذه النظرية أن الأنظمة القائمة على الذكاء الاصطناعي يمكنها معالجة المعلومات وتحليلها بشكل مستقل، مما يسمح لها بالتعلم من البيانات السابقة والتكيف مع التغيرات الجديدة. في سياق الأمن الصناعي، تعني هذه النظرية أن أنظمة المراقبة الذكية لا تقتصر على تسجيل الأحداث فقط، بل تعمل على تحليل الأنماط السلوكية، وتصنيف التهديدات وفقاً لدرجة خطورتها، وتقديم توصيات لاتخاذ إجراءات وقائية أو تصحيحية. يساعد هذا النهج في تحسين دقة التنبؤ بالمخاطر وتقليل التكاليف التشغيلية المرتبطة بالأخطاء البشرية (Phillips-Wren، ٢٠١٧).

## - دور الذكاء الاصطناعي في تعزيز الأمن الصناعي

يلعب الذكاء الاصطناعي دوراً حيوياً في تطوير أنظمة المراقبة الذكية، حيث يوفر أدوات تحليل متقدمة قادرة على التمييز بين التهديدات الحقيقية والإنذارات الكاذبة. من خلال تحليل البيانات الكبيرة، تستطيع الأنظمة الذكية تحديد الأفراد المشبوهين، التعرف على السلوكيات غير المعتادة، وتقديم إنذارات فورية عند اكتشاف أي نشاط غير طبيعي. كما يساهم الذكاء الاصطناعي في تحسين سرعة الاستجابة للحوادث الأمنية، حيث يمكنه إرسال تنبيهات تلقائية وتوجيه فرق التدخل إلى المواقع التي تحتاج إلى دعم فوري. علاوة على ذلك، فإن هذه الأنظمة قادرة على التكامل مع أنظمة أخرى مثل التحكم في الوصول وأجهزة الاستشعار البيئية، مما يخلق بيئة صناعية أكثر أماناً واستجابة للتحديات الأمنية (Paul، ٢٠٢٤).

## - التحديات المرتبطة بتطبيق أنظمة المراقبة الذكية

على الرغم من المزايا العديدة التي توفرها أنظمة المراقبة الذكية، إلا أن هناك بعض التحديات التي قد تواجه تطبيقها في القطاع الصناعي. من بين هذه التحديات التكلفة العالية لتطوير وتركيب هذه الأنظمة، والتي قد تشكل عبئاً مالياً على بعض المنشآت الصناعية. بالإضافة إلى ذلك، فإن نجاح هذه الأنظمة يعتمد بشكل كبير على دقة الخوارزميات المستخدمة، والتي قد تواجه صعوبة في التمييز بين الحالات العادية والمواقف التي تتطلب تدخلاً أمنياً، مما قد يؤدي إلى حدوث إنذارات كاذبة أو تجاهل تهديدات حقيقية. كما أن قضايا الخصوصية وحماية البيانات تعتبر من العوامل المهمة التي يجب مراعاتها عند تنفيذ هذه

الأنظمة، حيث تتطلب عمليات تحليل البيانات جمع معلومات حساسة تتعلق بالموظفين والزوار، مما قد يثير مخاوف قانونية وأخلاقية (Anagnostopoulos، ٢٠٢١).

#### - التوجهات المستقبلية لأنظمة المراقبة الذكية في الأمن الصناعي

مع استمرار التطورات في تقنيات الذكاء الاصطناعي، من المتوقع أن تتحسن كفاءة أنظمة المراقبة الذكية في الكشف عن التهديدات الأمنية والتعامل معها بشكل أكثر دقة. من المتوقع أن تشهد هذه الأنظمة مزيداً من التكامل مع تقنيات مثل الحوسبة السحابية، التي تتيح تخزين كميات هائلة من البيانات وتحليلها في الوقت الفعلي، مما يسهل عملية اتخاذ القرارات الأمنية بشكل أسرع وأكثر دقة. كما أن استخدام تقنيات البلوك تشين يمكن أن يساهم في تحسين أمن البيانات المخزنة، مما يقلل من مخاطر الاختراقات السيبرانية. بالإضافة إلى ذلك، فإن تطوير أنظمة ذكاء اصطناعي أكثر تطوراً يعتمد على التعلم العميق سيعزز قدرة هذه الأنظمة على التكيف مع التغيرات المستمرة في بيئة العمل الصناعية، مما يزيد من فاعليتها في تعزيز الأمن والاستجابة للتهديدات (Olawade، ٢٠٢٤).

#### الدراسات السابقة:

أفضت التطورات المتلاحقة المصاحبة للعصر الرقمي إلى ظهور أنماط جديدة من الجرائم تتسم باستعمال الذكاء وتسخير الآلة في ارتكابها وعلى مستوى نوع الجريمة وأساليب ارتكابها أسفرت تلك التطورات عن تعقد عمليات الكشف عن الجرائم الجديدة، واستتبع ذلك البحث عن سبل ملائمة للكشف عنها تمهيداً لملاحقتها، فظهرت بعض الوسائل المستحدثة كاللتصت على الهواتف وضبط المراسلات، تسجيل المكالمات الهاتفية والاستعانة بالأجهزة الإلكترونية كالهواتف المحمولة وأجهزة الكمبيوتر والانترنت وكاميرات المراقبة وغيرها. وقد بدأ البعض يطرح وجهات نظر جديدة وتساؤلات ذات قيمة، مفادها: ما مدى إمكانية الكشف عن الجريمة من خلال استخدام تطبيقات الذكاء الاصطناعي والمراقبة الذكية وعمليات تحليل البيانات لاسيما ما يسمى بالبيانات الضخمة أو الكبيرة BIG DATA؟؟ وهل يمكن لأجهزة البحث الجنائي والشرطة وسلطات التحقيق أن تستعين بهذه الوسائل الحديثة في الكشف عن الجرائم التي وقعت بالفعل؟؟ وهل يمكن لتلك السلطات المسؤولة عن الحد من الجريمة والوقاية منها

وملاحظتها أن تستخدم آلية تحليل البيانات المخزنة لدى الأجهزة الحكومية أو غيرها في التنبؤ بوقوع الجريمة؟. ويشير استخدام هذه التقنيات الحديثة في مجال الكشف عن الجرائم والتنبؤ بها العديد من الإشكاليات منها ما يتعلق بحماية حق الأفراد في الخصوصية وحماية الحياة الخاصة ومنها أيضاً ما يتعلق بالحماية القانونية المقررة للبيانات الشخصية للأفراد. فضلاً عن إشكاليات عملية تتعلق بالأدلة المستخلصة بواسطة تقنيات الذكاء الاصطناعي وتحليل البيانات (على، ٢٠٢٣).

تواجه الأجهزة الأمنية تحديات جمة ومتعددة، وأهمها الاتجاه إلى العولمة والانفتاح التقني ودخول مسرعات مستقبلية، مثل مشاريع الطابعات ثلاثية الأبعاد والروبوت الصناعي والسيارات ذاتية القيادة، وظهور مفاهيم جرائم المستقبل، لذا كثر الحديث عن الذكاء الاصطناعي ومدى إحلاله محل العقل البشري في بعض المهام ودوره في مجال مكافحة الجريمة من خلال تحليل قواعد البيانات الخاصة بالبلاغات بشكل آلي، وذلك لحسن توجيه الدوريات الأمنية إلى المناطق المراد تغطيتها أمنياً، أو التنبؤ بالمناطق الجغرافية المتوقع ارتفاع معدل الجريمة بها، فضلاً عن المساهمة في تقليل زمن الاستجابة لمركز القيادة في اتخاذ القرارات بناء على معلومات دقيقة في كل ما يخص الجريمة. وتثير تقنيات الذكاء الاصطناعي وتكنولوجيا المعلومات إشكاليات عديدة في مجال القانون ومكافحة الجريمة، ففي مجال القانون الجنائي تثار إشكاليات المسؤولية الجنائية الناشئة عن استخدام تقنيات الذكاء الاصطناعي، وفي القانون المدني التساؤلات المتصلة بالمسؤولية التقصيرية الناشئة عن استخدام تلك التقنيات، وفي مجال القانون الإجرائي ما يتعلق بالعدالة الإلكترونية والتقاضي عن بعد، وما يتعلق بالذكاء الاصطناعي ومدى الاستفادة به في مكافحة الجريمة منعا وكشفاً كإحدى أدوات استشراف المستقبل، فضلاً عن استعانة الأجهزة الأمنية بالروبوتات وتقنيات الذكاء الاصطناعي في أداء مهام حفظ الأمن ومكافحة الجرائم، والتنبؤ بأماكن حدوثها بناءً على بيانات لأماكن تجمع المجرمين وتتبعهم، وهو ما يندرج تحت استراتيجيه المدن الذكية التي من أهم أهدافها استخدام التقنيات المتطورة مثل الذكاء الاصطناعي، لضمان سلامة وأمن الناس لتحسين أحوال المجتمعات وتسريع أهداف التنمية المستدامة. تهدف الدراسة إلقاء الضوء حول ماهية الذكاء الاصطناعي وسماته، والعلاقة بينه وبين العقل البشري والأنظمة الخبيرة، والذكاء ومجالات استخداماته كإحدى أدوات استشراف المستقبل في مكافحة الجريمة منعا وكشفاً، وفي إيجاد منظومة أمن ذكية قادرة على توقع الأحداث قبل وقوعها، مع تصور رؤية استشراف الأعمال الشرطة والأمن في الدول العربية، مع تحديد المسؤولية الجنائية عن جرائم الذكاء الاصطناعي وعقوباتها (عوضين، ٢٠٢٢).

تتبع أنظمة التحكم الصناعي (ICS)، والتي تشمل أنظمة التحكم الإشرافي واكتساب البيانات (SCADA)، وأنظمة التحكم الموزعة (DCS)، ووحدات التحكم المنطقية القابلة للبرمجة (PLC)، دورًا حاسمًا في إدارة وتنظيم العمليات الصناعية. ومع ذلك، فإن ضمان أمن هذه الأنظمة له أهمية قصوى بسبب العواقب الوخيمة المحتملة للهجمات الإلكترونية. تقدم هذه المقالة نظرة عامة على أمن أنظمة التحكم الصناعي، وتغطي مكوناتها وبروتوكولاتها وتطبيقاتها الصناعية وجوانب الأداء. كما تسلط الضوء على التهديدات والثغرات النموذجية التي تواجهها هذه الأنظمة. علاوة على ذلك، تحدد المقالة العوامل الرئيسية التي تؤثر على قرارات التصميم المتعلقة بخصائص التحكم والاتصالات والموثوقية والتكرار لأنظمة التحكم الصناعي، حيث أنها بالغة الأهمية في تحديد الاحتياجات الأمنية للنظام. تحدد المقالة التدابير الأمنية الحالية، بما في ذلك تقسيم الشبكة والتحكم في الوصول وإدارة التصحيحات ومراقبة الأمان. علاوة على ذلك، تستكشف المقالة تكامل تقنيات التعلم الآلي لتعزيز الأمن السيبراني لأنظمة التحكم الصناعي. يوفر التعلم الآلي العديد من المزايا، مثل اكتشاف الشذوذ وتحليل استخبارات التهديدات والصيانة التنبؤية. ومع ذلك، فإن الجمع بين التعلم الآلي وتدابير الأمن الأخرى أمر ضروري لإنشاء استراتيجية دفاع شاملة لأنظمة التحكم الصناعي (Nankya, 2023).

تهدف دراسة (اشتية، ٢٠٢٤) إلى التعرف على تقنيات الذكاء الاصطناعي وانعكاس استخدامها على التحقيق الجنائي وتحقيق العدالة. وتكمن أهمية الدراسة في تعاظم استخدام تقنيات الذكاء الاصطناعي في مواجهة الجريمة والحد منها من خلال استخدام تقنيات الذكاء الاصطناعي في تحليل كميات ضخمة من البيانات بأسرع وقت ممكن وبدقة وحرفية عاليتين. وتتمثل مشكلة الدراسة في الإجابة على السؤال: ما دور الذكاء الاصطناعي في الحد من الجرائم؟ وقد استخدم الباحثان المنهج الوصفي التحليلي. وتوصل الباحثان إلى عدد من النتائج يمكن سرد أهمها: يعزز الذكاء الاصطناعي من قدرة مأموري الضبط القضائي من القيام بالدور الوقائي لمنع وقوع الجرائم من خلال امكانية التنبؤ بها واتخاذ تدابير اللازمة لمنعها بشكل الذكاء الاصطناعي وسيلة لتعزيز الأدلة المقدمة من مأموري الضبط القضائي في مرحلة التحري والاستدلال مما ينعكس على قوة الإثبات الجنائي ويحقق العدالة. وتعزز تقنيات الذكاء الاصطناعي من استقرار النظام العام. ويوصي الباحثان بدعوة المؤسسات الحكومية والأهلية في المجتمع الفلسطيني إلى توعية المواطنين بفوائد تقنيات الذكاء الاصطناعي وأهميتها في مكافحة الجريمة. دعوة المشرع الفلسطيني إلى سن قانون ينظم إنتاج وتطوير واستخدام تقنيات الذكاء الاصطناعي، وبما يراعي الخصوصية وحقوق الإنسان دعوة أجهزة إنفاذ القانون في فلسطين إلى زيادة مستوى تدريب كوادرها على استخدام تقنيات الذكاء الاصطناعي في ظل التطور

المستمر. دعوة المشرع الفلسطيني إلى فتح آفاق التعاون الدولي في مجال استخدام تقنيات الذكاء الاصطناعي في مجال مكافحة الجريمة وتبادل المعلومات، خاصة الجريمة الإلكترونية والعابرة للحدود الوطنية.

نظرًا لارتفاع وتيرة الهجمات الإلكترونية بشكل مستمر، أصبح اعتماد أساليب الذكاء الاصطناعي، وخاصة التعلم الآلي والتعلم العميق والتعلم المعزز، أمرًا ضروريًا في مجال الأمن السيبراني. وقد أثبتت هذه التقنيات فعاليتها في الكشف عن الهجمات الإلكترونية والتخفيف منها، والتي يمكن أن تسبب ضررًا كبيرًا للأفراد والمؤسسات وحتى البلدان. تستخدم خوارزميات التعلم الآلي أساليب إحصائية لتحديد الأنماط والشذوذ في مجموعات البيانات الكبيرة، مما يمكن محلي الأمن من اكتشاف التهديدات غير المعروفة سابقًا. أظهر التعلم العميق، وهو مجال فرعي من التعلم الآلي، إمكانات كبيرة في تحسين دقة وكفاءة أنظمة الأمن السيبراني، وخاصة في التعرف على الصور والكلام. من ناحية أخرى، يعد التعلم المعزز مرة أخرى مجالًا فرعيًا من التعلم الآلي يدرّب الخوارزميات على التعلم من خلال التجربة والخطأ، مما يجعله فعالًا بشكل خاص في البيئات الديناميكية. كما قمنا بتقييم استخدام أدوات الذكاء الاصطناعي الشبيهة بـ ChatGPT في مجالات المشكلات المتعلقة بالإنترنت على كلا الجانبين، الإيجابي والسلبي. تقدم هذه المقالة نظرة عامة حول كيفية تطبيق التعلم الآلي والتعلم العميق والتعلم التعزيزي في مجال الأمن السيبراني، بما في ذلك استخدامها في الكشف عن البرامج الضارة واكتشاف الاختراق وتقييم نقاط الضعف وغيرها من المجالات. يتم تقييم الدراسات الحديثة باستخدام نماذج التعلم الآلي والتعلم العميق والتعلم التعزيزي في كل قسم بناءً على الفكرة الرئيسية والتقنيات والنتائج المهمة. كما تناقش تحديات وقيود هذه التقنيات، بما في ذلك جودة البيانات وقابلية التفسير والهجمات المعادية. بشكل عام، يحمل استخدام التعلم الآلي والتعلم العميق والتعلم التعزيزي في مجال الأمن السيبراني وعدًا كبيرًا لتحسين فعالية أنظمة الأمان وتعزيز قدرتنا على الحماية من الهجمات السيبرانية. ومع ذلك، من الضروري الاستمرار في تطوير وتحسين هذه التقنيات لمعالجة الطبيعة المتطورة باستمرار للتهديدات السيبرانية. علاوة على ذلك، فإن بعض الحلول الواعدة التي تعتمد على التعلم الآلي والتعلم العميق والتعلم التعزيزي معرضة للهجمات المعادية، مما يؤكد على أهمية وضع هذه الثغرة في الاعتبار عند ابتكار تدابير مضادة ضد التهديدات السيبرانية المعقدة. وخلصنا أيضًا إلى أن ChatGPT يمكن أن يكون أداة قيمة للأمن السيبراني، ولكن تجدر الإشارة إلى أن الأدوات المشابهة لـ ChatGPT يمكن أيضًا التلاعب بها لتهديد سلامة البيانات وسريتها وتوافرها (Ozkan، ٢٠٢٤).

في ظل تزايد وتيرة وتعقيد الهجمات الإلكترونية، أصبحت طرق الكشف عن التهديدات الأمنية السيبرانية التقليدية صعبة في التعامل مع أنواع جديدة من التهديدات. أصبحت تقنية الذكاء الاصطناعي، مع قدراتها القوية في معالجة البيانات والتعرف على الأنماط، تدريباً أداة مهمة لتعزيز الأمن السيبراني. تهدف هذه الورقة إلى استكشاف تطبيق الذكاء الاصطناعي في الكشف عن تهديدات الأمن السيبراني، أولاً تحديد الوضع الحالي لتطوير تقنية الذكاء الاصطناعي في مجال الأمن السيبراني، ثم التركيز على تحليل تطبيق الأساليب الأساسية مثل التعلم الآلي والتعلم العميق في الكشف عن التهديدات، ومناقشة مزايا التعلم المتكامل والأساليب المتعددة الوسائط. أخيراً، تلخص هذه الورقة التحديات الحالية التي تواجهها تقنية الذكاء الاصطناعي في مجال الأمن السيبراني وتتطلع إلى اتجاه التطوير المستقبلي. من خلال البحث في هذه الورقة، من المتوقع أن توفر مرجعاً لتحسين دقة وكفاءة الكشف عن تهديدات الأمن السيبراني (Wang، ٢٠٢٤).

### التعليق على الدراسات السابقة:

يعد استعراض الدراسات السابقة وتحليلها عنصراً جوهرياً في دعم الدراسة الحالية حول تقييم كفاءة أنظمة المراقبة الذكية في الأمن الصناعي. فقد تم تناول الذكاء الاصطناعي وتطبيقاته الأمنية في العديد من الدراسات السابقة، سواء من منظور الكشف عن الجرائم، أو تحسين الأمن السيبراني، أو إدارة المخاطر الصناعية. وفيما يلي تحليل نقدي لهذه الدراسات، مع توضيح أوجه التشابه والاختلاف بينها وبين الدراسة الحالية، ومدى إمكانية الاستفادة منها.

#### - أوجه الاتفاق مع الدراسات السابقة

- أكدت معظم الدراسات، مثل (عوضين، ٢٠٢٢) و(Nankya, 2023)، على أهمية الذكاء الاصطناعي في تعزيز الأمن، سواء في الكشف عن الجرائم أو التنبؤ بالمخاطر. وهذا يتوافق مع فرضيات الدراسة الحالية التي تؤكد أن أنظمة المراقبة الذكية قادرة على اكتشاف التهديدات بسرعة ودقة أكبر من الأنظمة التقليدية.

- أظهرت دراسات مثل (Ozkan ، ٢٠٢٤ (Wang)، ٢٠٢٤) (أن تقنيات التعلم العميق والتعلم الآلي تعزز من قدرة أنظمة الأمن الصناعي على التعرف على الأنماط المشبوهة وتقليل الإنذارات الكاذبة، وهو ما يتماشى مع أهداف البحث الحالي.
- ركزت بعض الدراسات مثل (اشتية، ٢٠٢٤) على استخدام الذكاء الاصطناعي في التحقيقات الجنائية ومكافحة الجريمة، مؤكدة على أهمية تحليل البيانات الضخمة في تحسين فعالية التحقيقات، وهذا يعزز أهمية تطبيق نفس المفاهيم في البيئة الصناعية.

#### - أوجه الاختلاف عن الدراسات السابقة

- ركزت معظم الدراسات السابقة على استخدام الذكاء الاصطناعي في الأمن السيبراني ومكافحة الجرائم التقليدية، في حين أن الدراسة الحالية تهتم بالأمن الصناعي، مما يجعلها أكثر تخصصًا في مجال لم يحظَ بتغطية كافية في الأدبيات السابقة.
- لم تتناول بعض الدراسات، مثل (عوضين، ٢٠٢٢)، بعمق التحديات الاقتصادية والتقنية التي تواجه تطبيق أنظمة المراقبة الذكية، بينما تسعى الدراسة الحالية إلى تحليل هذه العوامل وتقديم حلول مقترحة لتحسين كفاءة الأنظمة.
- في حين ركزت دراسات مثل (Nankya, 2023) على أمن أنظمة التحكم الصناعي (ICS) وتكاملها مع الأمن السيبراني، فإن الدراسة الحالية تتناول الذكاء الاصطناعي في المراقبة الأمنية المادية داخل المنشآت الصناعية، مما يفتح آفاقًا جديدة للبحث.

#### - نقاط القوة في الدراسات السابقة

- توفر الدراسات السابقة أساسًا نظريًا قويًا حول تطبيقات الذكاء الاصطناعي في الأمن، وهو ما يدعم الإطار النظري للدراسة الحالية.
- أثبتت الأبحاث مثل (Wang) ، ٢٠٢٤ (Ozkan)، ٢٠٢٤ (فاعلية التعلم العميق في تحليل البيانات الأمنية، مما يشير إلى إمكانية تطبيق هذه التقنيات في مجال الأمن الصناعي.
- توفر بعض الدراسات، مثل (اشتية، ٢٠٢٤)، رؤى حول التأثير القانوني لاستخدام الذكاء الاصطناعي في المراقبة، وهو جانب يمكن الاستفادة منه عند تقييم أخلاقيات أنظمة المراقبة الذكية في المنشآت الصناعية.

#### - الفجوات البحثية التي تسعى الدراسة إلى سدها

- لم تتناول الدراسات السابقة بعمق مدى تكامل أنظمة المراقبة الذكية مع الأنظمة الأمنية التقليدية، وهو ما تسعى الدراسة الحالية إلى تحليله.
- هناك نقص في الدراسات التي تقيم أداء أنظمة الذكاء الاصطناعي في البيئات الصناعية، مما يبرز أهمية البحث الحالي في سد هذه الفجوة.
- لا تزال هناك حاجة لمزيد من الدراسات حول تأثير الذكاء الاصطناعي على إدارة المخاطر الصناعية، وهو ما تسعى الدراسة إلى تسليط الضوء عليه من خلال تحليل العوامل التي تؤثر على نجاح هذه الأنظمة.

## أوجه الاستفادة من الدراسات السابقة:

يعد استعراض الدراسات السابقة وتحليلها عنصرًا حيويًا لدعم الدراسة الحالية التي تبحث في "تقييم كفاءة أنظمة المراقبة الذكية في الأمن الصناعي"، حيث يتيح فهمًا أعمق للتطورات البحثية السابقة في هذا المجال، ويساعد في تحديد الفجوات البحثية التي يمكن معالجتها. كما تساهم الدراسات السابقة في توفير مرجع علمي قوي يدعم الإطار النظري للدراسة، ويمكن الاستفادة منها في تطوير منهجية البحث، وتحليل النتائج، واستنباط التوصيات التي تسهم في تحسين أداء أنظمة المراقبة الذكية في البيئات الصناعية.

### - الاستفادة من الأطر النظرية والمفاهيم الأساسية

استفادت الدراسة الحالية من مجموعة من الأطر النظرية التي تم تناولها في الدراسات السابقة، والتي ساهمت في بناء فهم متكامل لموضوع البحث. فعلى سبيل المثال، تناولت دراسة (Nankya, 2023) مفهوم أنظمة التحكم الصناعي (ICS)، وأوضحت كيف يمكن تعزيز الأمن الصناعي من خلال تكامل هذه الأنظمة مع تقنيات الذكاء الاصطناعي، وهو ما يساعد الدراسة الحالية في استكشاف مدى إمكانية تطبيق هذه التقنيات على المراقبة الذكية وتحسين مستوى الحماية في المنشآت الصناعية. كما أن الأبحاث التي تناولت التعلم العميق والتعلم الآلي، مثل دراسة (Ozkan, 2024)، ساعدت في فهم كيف يمكن استخدام هذه التقنيات في تحليل البيانات الأمنية واكتشاف التهديدات المحتملة بدقة أعلى.

إضافة إلى ذلك، قدمت دراسة (اشتية، ٢٠٢٤) منظورًا مهمًا حول تأثير الذكاء الاصطناعي على مجال التحقيقات الجنائية، وهو ما يمكن ربطه بالدراسة الحالية من حيث استخدام نفس التقنيات في تحليل بيانات المراقبة ورصد الأنشطة المشبوهة في البيئات الصناعية. كما ركزت دراسات أخرى مثل (Wang, ٢٠٢٤) على تطبيقات الذكاء الاصطناعي في الأمن السيبراني، مما يتيح للدراسة الحالية استكشاف إمكانية الاستفادة من هذه التطبيقات في تطوير استراتيجيات حماية أكثر تطورًا لأنظمة المراقبة الذكية.

### - الاستفادة من المناهج البحثية والأساليب التحليلية

إحدى أهم الفوائد التي تقدمها الدراسات السابقة هي تقديم نماذج بحثية يمكن الاستفادة منها في تصميم الدراسة الحالية. على سبيل المثال، استخدمت دراسات مثل (عوضين، ٢٠٢٢) و (Ozkan, 2024) منهجيات تحليل البيانات الضخمة لتقييم فاعلية

أنظمة الذكاء الاصطناعي في الأمن الصناعي، مما يتيح إمكانية تبني منهج مشابه في الدراسة الحالية لتحليل بيانات المراقبة الذكية واستخلاص نتائج دقيقة حول أدائها. كما استخدمت بعض الدراسات التحليل الإحصائي والنمذجة التنبؤية، وهو ما يوفر أساسًا لتطبيق أساليب مشابهة في تقييم مدى دقة وكفاءة أنظمة المراقبة الذكية في البيئات الصناعية المختلفة.

علاوة على ذلك، ساعدت الدراسات التي اعتمدت على المنهج الوصفي التحليلي، مثل دراسة (اشتية، ٢٠٢٤)، في توجيه البحث الحالي نحو استخدام أدوات بحثية مثل الاستبيانات والمقابلات لجمع البيانات من الخبراء في مجال الأمن الصناعي، مما يعزز من دقة النتائج ويوفر صورة واضحة حول مدى نجاح هذه الأنظمة في تحقيق أهدافها الأمنية.

#### - الاستفادة من التحليل النقدي للتحديات والفرص

أظهرت العديد من الدراسات السابقة أن تطبيق أنظمة الذكاء الاصطناعي في الأمن الصناعي يواجه تحديات متعددة، مثل التكلفة العالية، وحماية الخصوصية، ودقة الخوارزميات المستخدمة في الكشف عن التهديدات. فعلى سبيل المثال، ناقشت دراسة (Wang، ٢٠٢٤) بعض العوائق التقنية التي تؤثر على أداء أنظمة الذكاء الاصطناعي في مجال الأمن السيبراني، مثل محدودية البيانات المتاحة وصعوبة التمييز بين التهديدات الحقيقية والإنذارات الكاذبة، وهو ما يمكن الاستفادة منه في تقييم مدى تأثير هذه العوامل على أنظمة المراقبة الذكية في المنشآت الصناعية.

كما أن دراسة (Nankya، 2023) قدمت تحليلًا للعوامل المؤثرة في نجاح أنظمة المراقبة الذكية، مثل تكاملها مع الأنظمة التقليدية للأمن الصناعي، ومدى سرعة استجابتها للتهديدات المحتملة، وهو ما يوفر قاعدة معرفية هامة يمكن استخدامها في الدراسة الحالية لتحليل كيفية تحسين أداء هذه الأنظمة وجعلها أكثر كفاءة.

#### - الاستفادة في تطوير استراتيجيات التحسين والتوصيات

ساهمت الدراسات السابقة في تقديم مجموعة من الاستراتيجيات التي يمكن الاستفادة منها في تحسين كفاءة أنظمة المراقبة الذكية. على سبيل المثال، تناولت دراسة (Ozkan، 2024) إمكانية دمج تقنيات الذكاء الاصطناعي مع أنظمة تحليل البيانات الضخمة، مما يسمح بتوفير تنبؤات دقيقة حول الأنشطة المشبوهة وتعزيز قدرات المراقبة الاستباقية، وهو ما يمكن تطبيقه في الدراسة الحالية لتقديم توصيات حول كيفية تحسين أداء أنظمة المراقبة الذكية في البيئات الصناعية.

كما سلطت دراسة (اشتية، ٢٠٢٤) الضوء على أهمية توفير إطار قانوني وتنظيمي يضمن الاستخدام المسؤول للذكاء الاصطناعي في الأمن، وهو ما يساعد في توجيه الدراسة نحو تحليل الجوانب القانونية المرتبطة باستخدام هذه الأنظمة، مثل حماية الخصوصية ومنع الاستخدام غير المشروع للمعلومات الأمنية.

#### - تحديد الفجوات البحثية والتوجهات المستقبلية

رغم الفوائد العديدة التي قدمتها الدراسات السابقة، إلا أن هناك جوانب لم تحظ بتغطية كافية، وهو ما يمكن للدراسة الحالية أن تسهم في معالجته. فعلى سبيل المثال، ركزت معظم الأبحاث السابقة على استخدام الذكاء الاصطناعي في الأمن السيبراني أو التحقيقات الجنائية، بينما لم يتم تناول تطبيقاته في الأمن الصناعي بنفس العمق. كما أن هناك نقصاً في الدراسات التي تحلل التأثير الاقتصادي لأنظمة المراقبة الذكية ومدى جدواها مقارنة بالأنظمة التقليدية، وهو ما تسعى الدراسة الحالية إلى استكشافه. بالإضافة إلى ذلك، لم تتناول العديد من الدراسات السابقة كيفية تكامل أنظمة الذكاء الاصطناعي مع التقنيات الحديثة مثل إنترنت الأشياء (IoT) والحوسبة السحابية لتعزيز الأمن الصناعي، وهو ما يمكن للدراسة الحالية أن تتطرق إليه كجزء من تحليلها المستقبلي.

#### مفاهيم الدراسة:

##### أولاً: المفاهيم الاصطلاحية

- **الأمن الصناعي:** يُعرف الأمن الصناعي بأنه مجموعة من التدابير والإجراءات التنظيمية والتقنية التي تهدف إلى حماية المنشآت الصناعية والعاملين فيها من المخاطر المحتملة، سواء كانت ناتجة عن الحوادث التشغيلية، الأعطال الفنية، الحرائق، أو التهديدات الأمنية. ويشمل الأمن الصناعي أنظمة السلامة، الوقاية من المخاطر، وإدارة الطوارئ (Reniers، ٢٠٢٠).

- **أنظمة المراقبة الذكية:** يشير هذا المصطلح إلى الأنظمة التقنية التي تستخدم تقنيات متقدمة مثل الذكاء الاصطناعي، التعلم الآلي، وإنترنت الأشياء لمراقبة البيانات الصناعية وتحليل البيانات الأمنية في الوقت الفعلي. هذه الأنظمة قادرة

على التعرف على التهديدات الأمنية، مثل التسلل غير المصرح به، والتصرفات غير الطبيعية، وإرسال إنذارات تنبيهية تلقائيًا (Kumar، ٢٠١٩).

- **الذكاء الاصطناعي:** هو فرع من علوم الحاسوب يهدف إلى تطوير أنظمة قادرة على محاكاة الذكاء البشري من خلال التعلم، التحليل، واتخاذ القرارات. ويستخدم الذكاء الاصطناعي في الأمن الصناعي لتعزيز دقة وكفاءة أنظمة المراقبة الذكية، من خلال تحليل الأنماط السلوكية والكشف عن التهديدات بسرعة (Ghosh، ٢٠٢١).
- **الكشف عن التهديدات:** يُعرف بأنه العملية التي يتم من خلالها تحديد المخاطر المحتملة التي قد تؤثر على بيئة العمل الصناعية، وذلك باستخدام تقنيات متقدمة تعتمد على تحليل البيانات الضخمة، الرؤية الحاسوبية، والخوارزميات التنبؤية لتحديد الأخطار قبل وقوعها (Aminu، ٢٠٢٤).
- **الدراسة الميدانية:** تعني البحث الذي يتم تنفيذه في بيئة واقعية لجمع البيانات وتحليلها بشكل مباشر، بهدف الوصول إلى نتائج عملية حول ظاهرة معينة. في هذه الدراسة، يتم تطبيق أدوات البحث الميداني لتقييم كفاءة أنظمة المراقبة الذكية في البيئات الصناعية المختلفة (Saunders، ٢٠٢٣).

#### - ثانيًا: المفاهيم الإجرائية

- **الأمن الصناعي:** يُقصد به في هذه الدراسة جميع الإجراءات والتقنيات التي تعتمد عليها المنشآت الصناعية لتعزيز الأمان والحماية من التهديدات الأمنية المحتملة، وذلك من خلال الاعتماد على أنظمة المراقبة الذكية المدعومة بالذكاء الاصطناعي.
- **أنظمة المراقبة الذكية:** يُقصد بها في هذه الدراسة الأنظمة المستخدمة داخل المنشآت الصناعية التي تعتمد على تقنيات الذكاء الاصطناعي لمعالجة البيانات وتحليل الفيديو والصوت والاستجابة للتهديدات الأمنية بناءً على خوارزميات التعلم الآلي.

- **الذكاء الاصطناعي:** يُعرف في سياق هذه الدراسة بأنه استخدام خوارزميات وتقنيات تحليل البيانات الضخمة والتعلم الآلي لتعزيز قدرات أنظمة المراقبة الذكية في الكشف عن التهديدات الأمنية والتفاعل معها بفعالية.
- **الكشف عن التهديدات:** يُشير إلى العمليات التقنية التي تقوم بها أنظمة المراقبة الذكية داخل المنشآت الصناعية لاكتشاف أي نشاط غير مألوف أو خطر محتمل، بناءً على تحليل البيانات المرئية والصوتية والسلوكية، وإرسال تنبيهات أو اتخاذ إجراءات وقائية.
- **الدراسة الميدانية:** يُقصد بها في هذه الدراسة إجراء بحث تطبيقي داخل بيئات صناعية مختلفة في المملكة العربية السعودية، بهدف تقييم مدى فاعلية أنظمة المراقبة الذكية في الكشف عن التهديدات الأمنية، من خلال جمع البيانات وتحليلها باستخدام أدوات البحث العلمي.

## الإجراءات المنهجية للدراسة:

### - نوع ومنهج الدراسة

تعتمد هذه الدراسة على المنهج الكمي، الذي يُعد من أكثر المناهج البحثية ملاءمة لتحليل البيانات المتعلقة بكفاءة أنظمة المراقبة الذكية في الأمن الصناعي. ويعتمد المنهج الكمي على جمع البيانات الرقمية وتحليلها إحصائيًا من أجل الوصول إلى نتائج دقيقة وقابلة للتعميم. ونظرًا لطبيعة الدراسة التي تهدف إلى تقييم أداء أنظمة المراقبة الذكية المدعومة بالذكاء الاصطناعي، فإن استخدام التحليل الكمي يمكن الباحث من قياس مدى فعالية هذه الأنظمة في الكشف عن التهديدات، ومدى استجابتها للمتغيرات المختلفة في البيئات الصناعية. كما يسمح هذا المنهج بإجراء مقارنات بين منشآت صناعية مختلفة تعتمد على تقنيات مراقبة متنوعة، مما يتيح التحقق من كفاءة هذه الأنظمة بناءً على معايير موضوعية ومحددة.

تعتمد الدراسة أيضًا على المنهج الوصفي التحليلي، حيث يتم وصف الواقع الحالي لأنظمة المراقبة الذكية وتحليل أدائها بناءً على البيانات الميدانية. ويهدف هذا النهج إلى تقديم رؤية متكاملة حول كيفية استخدام الذكاء الاصطناعي في تحسين الأمن الصناعي، من خلال جمع البيانات من مصادر متعددة وتحليلها باستخدام الأدوات الإحصائية المناسبة (Islam, 2024).

## - مجتمع وعينة الدراسة

لتحقيق أهداف الدراسة، تم تحديد مجتمع الدراسة ليشمل المنشآت الصناعية الكبرى في المملكة العربية السعودية التي تعتمد على أنظمة المراقبة الذكية في تعزيز الأمن الصناعي. يشمل المجتمع الصناعات الحيوية مثل المصانع الكبرى، المنشآت البتروكيميائية، محطات الطاقة، والمرافق اللوجستية التي تعتمد على أنظمة الذكاء الاصطناعي لمراقبة أمنها. تم اختيار هذه القطاعات نظرًا لحساسيتها الأمنية واعتمادها المتزايد على تقنيات المراقبة المتقدمة.

أما عينة الدراسة، فقد تم اختيارها وفقًا لأسلوب العينة العشوائية الطبقية، حيث تم تقسيم المنشآت الصناعية إلى فئات وفقًا لحجمها وطبيعة نشاطها ومستوى اعتمادها على أنظمة الذكاء الاصطناعي في المراقبة. ومن ثم، تم اختيار عدد من المنشآت من كل فئة لضمان تمثيل شامل لمختلف القطاعات الصناعية. كما شملت العينة العاملين في إدارات الأمن الصناعي والخبراء التقنيين المسؤولين عن تشغيل وصيانة أنظمة المراقبة الذكية، بالإضافة إلى المسؤولين عن اتخاذ القرارات الأمنية في المنشآت المستهدفة.

## - الإطار المكاني للدراسة

تُجرى الدراسة في المملكة العربية السعودية، نظرًا لما تشهده من تطور في القطاع الصناعي واعتمادها على تقنيات الذكاء الاصطناعي في مختلف المجالات، بما في ذلك الأمن الصناعي. تشمل الدراسة مناطق صناعية رئيسية مثل الجبيل، ينبع، الرياض، جدة، والدمام، حيث تتركز العديد من المنشآت الصناعية الكبرى التي تعتمد على أنظمة مراقبة متطورة لحماية بيئات العمل. اختيار هذه المناطق يعكس التنوع في أنواع الصناعات والتقنيات المستخدمة، مما يعزز من شمولية الدراسة ودقة نتائجها.

## - الإطار الزمني للدراسة

تمتد الدراسة خلال الفترة الزمنية من يناير ٢٠٢٤ إلى ديسمبر ٢٠٢٤، وهي الفترة التي سيتم خلالها جمع البيانات وتحليلها لاستخلاص النتائج النهائية. يشمل الإطار الزمني مراحل متعددة تبدأ بجمع البيانات الأولية، ثم تحليلها باستخدام الأدوات الإحصائية المناسبة، يلي ذلك مناقشة النتائج واستخلاص التوصيات النهائية. يتيح هذا الإطار الزمني متابعة التطورات التقنية في مجال أنظمة المراقبة الذكية، وضمان دقة البيانات التي يتم جمعها.

## - الإطار البشري للدراسة

يشمل الإطار البشري للدراسة المهندسين والمختصين في الأمن الصناعي، مسؤولي المراقبة الأمنية، الفنيين المشرفين على أنظمة الذكاء الاصطناعي، وخبراء تكنولوجيا المعلومات العاملين في المنشآت الصناعية المستهدفة. كما تتضمن الدراسة آراء مديري الأمن والسلامة في هذه المنشآت، نظرًا لدورهم الحيوي في تقييم أداء أنظمة المراقبة الذكية. يتم جمع البيانات من هؤلاء الأفراد باستخدام استبيانات مصممة بعناية، بالإضافة إلى مقابلات محدودة مع الخبراء لفهم التحديات والفرص المرتبطة بتطبيق الذكاء الاصطناعي في الأمن الصناعي.

## أدوات جمع بيانات الدراسة:

تُعد أدوات جمع البيانات من الركائز الأساسية التي تقوم عليها البحوث العلمية، إذ تتيح للباحث الحصول على معلومات دقيقة يمكن تحليلها للوصول إلى استنتاجات موثوقة. وفي هذه الدراسة، تم الاعتماد على الاستبيان المغلق باستخدام مقياس ليكرت كأداة رئيسية لجمع البيانات من المشاركين، وذلك نظرًا لما يوفره من منهجية قياسية لقياس تصورات وآراء العاملين في قطاع الأمن الصناعي حول كفاءة أنظمة المراقبة الذكية المدعومة بالذكاء الاصطناعي.

يعتمد الاستبيان المغلق على تقديم مجموعة من الأسئلة ذات الخيارات المحددة مسبقًا، مما يضمن تجانس الإجابات وسهولة تحليلها إحصائيًا. ويتميز هذا النوع من الاستبيانات بأنه يقلل من التحيزات الذاتية ويوفر بيانات قابلة للقياس، ما يساهم في تقديم نتائج أكثر موضوعية ودقة. كما يساعد في تقليل تأثير الفروقات اللغوية أو التفسيرية بين المشاركين، حيث تكون الإجابات محددة ضمن خيارات واضحة.

تم تصميم مقياس ليكرت في الاستبيان بحيث يتضمن خمس درجات تقييمية تتراوح بين (1) :موافق بشدة، (2) :موافق، (3) محايد، (4) :غير موافق، و (5) :غير موافق بشدة. وقد تم اختيار هذا المقياس نظرًا لقدرته على قياس اتجاهات المشاركين بدقة وتقديم بيانات كمية قابلة للتحليل الإحصائي المتقدم، مما يمكن الباحث من استخلاص استنتاجات دقيقة حول مدى فاعلية أنظمة المراقبة الذكية (Karunarathna، ٢٠٢٤).

## - بناء الاستبيان وهيكلته

تم تصميم الاستبيان ليشمل عدة محاور تغطي الجوانب الأساسية لموضوع الدراسة، حيث تم تقسيمه إلى أربعة أقسام رئيسية لضمان شمولية التقييم:

١. البيانات الديموغرافية؛ يتضمن هذا القسم أسئلة حول خصائص المشاركين مثل العمر، الجنس، المؤهل العلمي، وذلك لفهم تأثير هذه العوامل على آرائهم تجاه أنظمة المراقبة الذكية.

٢. مدى انتشار واستخدام أنظمة المراقبة الذكية؛ يهدف هذا القسم إلى قياس مدى استخدام تقنيات الذكاء الاصطناعي في المراقبة الأمنية داخل المنشآت الصناعية، وأنواع الأنظمة المطبقة، ومستوى الاعتماد عليها في الكشف عن التهديدات الأمنية.

٣. كفاءة أنظمة المراقبة الذكية في الكشف عن التهديدات؛ يركز هذا القسم على تقييم دقة وفعالية هذه الأنظمة في رصد التهديدات الأمنية المحتملة، مثل تسلل الأفراد غير المصرح لهم، أو رصد السلوكيات غير الطبيعية، أو تحليل البيانات الصوتية والبصرية للكشف عن المخاطر.

٤. التحديات والتحسينات المطلوبة؛ يتناول هذا الجزء العقبات التي قد تواجه المنشآت في تبني هذه الأنظمة، ومدى الحاجة إلى تطويرها أو تحسينها لتحقيق نتائج أكثر دقة وكفاءة.

## - اختبار صدق وثبات الاستبيان

لضمان موثوقية الأداة البحثية، تم إجراء اختبار الصدق من خلال عرضه على مجموعة من الخبراء في مجال الأمن الصناعي وتقنيات الذكاء الاصطناعي، للتأكد من وضوح الأسئلة ومدى ملاءمتها لأهداف الدراسة. كما تم حساب معامل الثبات باستخدام اختبار كرونباخ ألفا (Cronbach's Alpha) لضمان استقرار الإجابات واتساقها، مما يعزز دقة النتائج التي سيتم الحصول عليها.

## - آلية توزيع الاستبيان وجمع البيانات

سيتم توزيع الاستبيان على عينة من العاملين في المنشآت الصناعية المختارة باستخدام الوسائل الإلكترونية، وذلك لضمان وصوله إلى أكبر عدد ممكن من المشاركين بسهولة وسرعة. كما تم التنسيق مع إدارات الأمن والسلامة في المنشآت المستهدفة لتشجيع الموظفين على المشاركة، مع التأكيد على سرية الإجابات واستخدامها لأغراض البحث العلمي فقط.

## التبويب المقترح لفصول الدراسة:

تعتمد هذه الدراسة على هيكلية واضحة ومنهجية منظمة تسهم في تحقيق أهدافها البحثية، وذلك من خلال تقسيمها إلى مجموعة من الفصول التي تغطي الجوانب المختلفة لموضوع "تقييم كفاءة أنظمة المراقبة الذكية في الأمن الصناعي: دراسة ميدانية حول تطبيقات الذكاء الاصطناعي في الكشف عن التهديدات". ويتضمن التبويب المقترح لهذه الفصول تناول الإطار النظري للدراسة، وتحليل البيانات، ومناقشة النتائج، واستخلاص التوصيات.

## - الفصل الأول: الإطار العام للدراسة

يُقدم هذا الفصل الخلفية العامة للدراسة، حيث يستعرض مقدمة شاملة توضح أهمية البحث ودوافعه، بالإضافة إلى مشكلة الدراسة التي تحدد الفجوة البحثية التي يسعى الباحث إلى معالجتها. كما يتناول هذا الفصل صياغة أهداف الدراسة وفق منهجية SMART، إلى جانب التساؤلات البحثية التي توجه عملية البحث. كما يتطرق إلى الفرضيات التي سيتم اختبارها، وأهمية الدراسة النظرية والتطبيقية، فضلاً عن التعريف بالمفاهيم الاصطلاحية والإجرائية المستخدمة. يُختتم الفصل بتوضيح التبويب العام للدراسة.

## - الفصل الثاني: الإطار النظري والدراسات السابقة

يستعرض هذا الفصل الأساس النظري الذي تعتمد عليه الدراسة، من خلال تحليل الأدبيات العلمية المتعلقة بأنظمة المراقبة الذكية، وأهميتها في الأمن الصناعي. كما يتناول النظريات ذات الصلة، مثل نظرية النظم الذكية، ونظرية اتخاذ القرار المدعوم بالذكاء الاصطناعي، إلى جانب تحليل كيفية عمل تقنيات الذكاء الاصطناعي في مجال الكشف عن التهديدات الأمنية. بالإضافة إلى ذلك، يُخصص جزء من هذا الفصل لاستعراض الدراسات السابقة ذات الصلة، سواء المحلية أو العالمية، مع تحليل أوجه التشابه والاختلاف بينها وبين الدراسة الحالية، وتحديد الفجوات البحثية التي تسعى هذه الدراسة إلى سدها.

### - الفصل الثالث: الإجراءات المنهجية للدراسة

يركز هذا الفصل على تصميم البحث ومنهجيته، حيث يوضح طبيعة الدراسة الكمية، ونوع المنهج المستخدم، والذي يعتمد على الأساليب الإحصائية في تحليل البيانات. كما يحدد مجتمع الدراسة وعينتها، سواء من حيث التوزيع المكاني (المنشآت الصناعية المستهدفة)، أو التوزيع الزمني (الفترة الزمنية لجمع البيانات وتحليلها)، أو التوزيع البشري (الفئات المستهدفة مثل العاملين في الأمن الصناعي والمختصين بالتكنولوجيا الأمنية).

كما يوضح هذا الفصل الأدوات المستخدمة في جمع البيانات، وهي الاستبيانات المغلقة باستخدام مقياس ليكرت، ويشرح كيفية تصميمها، وضبط صدقها وثباتها. كما يُحدد تقنيات التحليل الإحصائي التي سيتم استخدامها لاختبار الفرضيات، مثل الإحصاء الوصفي، وتحليل التباين، والانحدار اللوجستي وغيرها من الأساليب المناسبة لطبيعة البيانات.

### - الفصل الرابع: تحليل البيانات ومناقشة النتائج

في هذا الفصل، يتم عرض البيانات التي تم جمعها من المشاركين، وتحليلها باستخدام البرامج الإحصائية المتقدمة مثل SPSS أو R. يتم تقديم الجداول والرسوم البيانية التي تعكس نتائج الاستبيانات، مع تفسير هذه النتائج وربطها بفرضيات الدراسة. كما يناقش هذا الفصل مدى تحقق الفرضيات التي تم وضعها مسبقاً، مع تحليل مدى قوة العلاقة بين كفاءة أنظمة المراقبة الذكية ومدى قدرتها على الكشف عن التهديدات في الأمن الصناعي. ويتم كذلك مقارنة النتائج التي تم التوصل إليها مع نتائج الدراسات السابقة، مما يساعد في وضع الدراسة ضمن السياق البحثي الأوسع.

### - الفصل الخامس: النتائج والتوصيات والمقترحات المستقبلية

يُعد هذا الفصل من أهم أجزاء الدراسة، حيث يُلخص الباحث أبرز النتائج التي توصل إليها بناءً على التحليل الإحصائي والمناقشات السابقة. كما يتضمن توصيات عملية موجهة للمؤسسات الصناعية لتعزيز استخدام أنظمة المراقبة الذكية وتحسين كفاءتها.

ويشمل الفصل أيضاً اقتراحات لدراسات مستقبلية يمكن أن تُبنى على هذه الدراسة، مثل توسيع نطاق البحث ليشمل قطاعات أخرى، أو تحليل تأثير دمج تقنيات جديدة في أنظمة المراقبة، مثل إنترنت الأشياء (IoT) أو تحليل البيانات الضخمة (Big Data).

(Data Analytics). يُختتم الفصل بعرض الخاتمة العامة للدراسة، والتي تلخص أبرز ما تم تحقيقه، وأهمية البحث في تطوير

سياسات الأمن الصناعي.

#### - الخاتمة والملاحق

يتضمن هذا القسم قائمة بالمصادر والمراجع التي اعتمدت عليها الدراسة، وفقًا لنظام التوثيق الأكاديمي. كما يُضاف إليه أي

ملاحق تحتوي على الاستبيانات المستخدمة، أو تفاصيل إضافية ذات صلة بعملية البحث.

## المراجع:

### - المراجع العربية

- اشتية, م. ع. (2024). الذكاء الاصطناعي ودوره في الحد من الجرائم "دراسة تحليلية تطبيقية". 2(8). Retrieved from [https://journal.aau.ac.ae/files/1726034983\\_full\\_article.pdf](https://journal.aau.ac.ae/files/1726034983_full_article.pdf)
- على, ر. س. (2023). استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم . Retrieved from [https://jdl.journals.ekb.eg/article\\_316481\\_71362d586288a1e271f163f9c939959b.pdf](https://jdl.journals.ekb.eg/article_316481_71362d586288a1e271f163f9c939959b.pdf)
- عوضين, ف. (2022). استخدامات تقنيات الذكاء الاصطناعي بين المشروعية وعدم المشروعية . Retrieved from [https://ncj.journals.ekb.eg/article\\_251652\\_9add795f1a1e75ff804b121763f85aac.pdf](https://ncj.journals.ekb.eg/article_251652_9add795f1a1e75ff804b121763f85aac.pdf)

### - المراجع الأجنبية

- Al-Hashemi, S. Q. (2024). Development of Smart Video Surveillance Systems: Technical and Security Challenges in Urban Environments. Retrieved from [https://www.researchgate.net/publication/385507305\\_Development\\_of\\_Smart\\_Video\\_Surveillance\\_Systems\\_Technical\\_and\\_Security\\_Challenges\\_in\\_Urban\\_Environments](https://www.researchgate.net/publication/385507305_Development_of_Smart_Video_Surveillance_Systems_Technical_and_Security_Challenges_in_Urban_Environments)
- Aminu, M. (2024). Enhancing Cyber Threat Detection through Real-time Threat Intelligence and Adaptive Defense Mechanisms. Retrieved from [https://www.researchgate.net/publication/382782321\\_Enhancing\\_Cyber\\_Threat\\_Detection\\_through\\_Real-time\\_Threat\\_Intelligence\\_and\\_Adaptive\\_Defense\\_Mechanisms](https://www.researchgate.net/publication/382782321_Enhancing_Cyber_Threat_Detection_through_Real-time_Threat_Intelligence_and_Adaptive_Defense_Mechanisms)
- Anagnostopoulos, T. T. (2021). Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A Survey. Retrieved from [https://www.researchgate.net/publication/354770276\\_Challenges\\_and\\_Solutions\\_of\\_Surveillance\\_Systems\\_in\\_IoT-Enabled\\_Smart\\_Campus\\_A\\_Survey](https://www.researchgate.net/publication/354770276_Challenges_and_Solutions_of_Surveillance_Systems_in_IoT-Enabled_Smart_Campus_A_Survey)
- Ganeshan, C. (2018). Smart Industrial System for Monitoring, Control and Security Using Internet of Things. Retrieved from [https://www.researchgate.net/publication/329391722\\_Smart\\_Industrial\\_System\\_for\\_Monitoring\\_Control\\_and\\_Security\\_Using\\_Internet\\_of\\_Things](https://www.researchgate.net/publication/329391722_Smart_Industrial_System_for_Monitoring_Control_and_Security_Using_Internet_of_Things)

- George, A. S. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. Retrieved from [https://www.researchgate.net/publication/378078435\\_Cyber\\_Threats\\_to\\_Critical\\_Infrastructure\\_Assessing\\_Vulnerabilities\\_Across\\_Key\\_Sectors](https://www.researchgate.net/publication/378078435_Cyber_Threats_to_Critical_Infrastructure_Assessing_Vulnerabilities_Across_Key_Sectors)
- George, A. S. (2024). The Fourth Industrial Revolution: A Primer on Industry 4.0 and its Transformative Impact. Retrieved from [https://www.researchgate.net/publication/378261588\\_The\\_Fourth\\_Industrial\\_Revolution\\_A\\_Primer\\_on\\_Industry\\_4\\_0\\_and\\_its\\_Transformative\\_Impact](https://www.researchgate.net/publication/378261588_The_Fourth_Industrial_Revolution_A_Primer_on_Industry_4_0_and_its_Transformative_Impact)
- Ghosh, M. (2021). Introduction to Artificial Intelligence. Retrieved from [https://www.researchgate.net/publication/351758474\\_Introduction\\_to\\_Artificial\\_Intelligence](https://www.researchgate.net/publication/351758474_Introduction_to_Artificial_Intelligence)
- Islam, M. A. (2024). Impact of Big Data Analytics on Digital Marketing: Academic Review. Retrieved from [https://www.researchgate.net/publication/380000313\\_Impact\\_of\\_Big\\_Data\\_Analytics\\_on\\_Digital\\_Marketing\\_Academic\\_Review](https://www.researchgate.net/publication/380000313_Impact_of_Big_Data_Analytics_on_Digital_Marketing_Academic_Review)
- Karunarathna, I. (2024). The Crucial Role of Data Collection in Research: Techniques, Challenges, and Best Practices. Retrieved from [https://www.researchgate.net/publication/383155720\\_The\\_Crucial\\_Role\\_of\\_Data\\_Collection\\_in\\_Research\\_Techniques\\_Challenges\\_and\\_Best\\_Practices](https://www.researchgate.net/publication/383155720_The_Crucial_Role_of_Data_Collection_in_Research_Techniques_Challenges_and_Best_Practices)
- Kumar, S. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Retrieved from <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2>
- Myagmar-Ochir, Y. (2023). A Survey of Video Surveillance Systems in Smart City. 12(17). Retrieved from <https://www.mdpi.com/2079-9292/12/17/3567>
- Nankya, M. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. 23(21). Retrieved from <https://www.mdpi.com/1424-8220/23/21/8840>
- Olawade, D. B. (2024). Smart waste management: A paradigm shift enabled by artificial intelligence. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2949750724000385>
- Ozkan, M. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. Retrieved from [https://www.researchgate.net/publication/377747343\\_A\\_Comprehensive\\_Survey\\_E](https://www.researchgate.net/publication/377747343_A_Comprehensive_Survey_E)

valuating\_the\_Efficiency\_of\_Artificial\_Intelligence\_and\_Machine\_Learning\_Techniques\_on\_Cyber\_Security\_Solutions

- Paul, A. L. (2024). The Role of Artificial Intelligence in Enhancing Data Security. Retrieved from [https://www.researchgate.net/publication/381004546\\_The\\_Role\\_of\\_Artificial\\_Intelligence\\_in\\_Enhancing\\_Data\\_Security](https://www.researchgate.net/publication/381004546_The_Role_of_Artificial_Intelligence_in_Enhancing_Data_Security)
- Phillips-Wren, G. (2017). Intelligent Systems to Support Human Decision Making. Retrieved from [https://www.researchgate.net/publication/313474343\\_Intelligent\\_Systems\\_to\\_Support\\_Human\\_Decision\\_Making](https://www.researchgate.net/publication/313474343_Intelligent_Systems_to_Support_Human_Decision_Making)
- Qin, Y. (2023). Artificial Intelligence and Economic Development: An Evolutionary Investigation and Systematic Review. 15. Retrieved from <https://link.springer.com/article/10.1007/s13132-023-01183-2>
- Reniers, G. (2020). What safety models and principles can be adapted and used in security science? 64. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0950423019307612>
- Renukappa, S. (2022). Evaluation of challenges for adoption of smart healthcare strategies. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2352648322000642>
- Rodríguez-Espíndola, O. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0040162522000944>
- Saunders, M. N. (2023). Research Methods for Business Students. Retrieved from [https://www.researchgate.net/publication/240218229\\_Research\\_Methods\\_for\\_Business\\_Students](https://www.researchgate.net/publication/240218229_Research_Methods_for_Business_Students)
- Wang, Z. (2024). Artificial Intelligence in Cybersecurity Threat Detection. Retrieved from [https://www.researchgate.net/publication/384127618\\_Artificial\\_Intelligence\\_in\\_Cybersecurity\\_Threat\\_Detection](https://www.researchgate.net/publication/384127618_Artificial_Intelligence_in_Cybersecurity_Threat_Detection)
- Yazdi, M. (2024). Navigating the Power of Artificial Intelligence in Risk Management: A Comparative Analysis. 10(2). Retrieved from <https://www.mdpi.com/2313-576X/10/2/42>