Cambridge International

Professional Research

“A Comparative Analysis of the Effectiveness of Artificial Intelligence in Predicting Cyberattacks Versus Traditional Information Security Systems”

The Researcher

ALIYA Bashir AbU KASAWI ELNORUR

Supervised by

Dr. Hager Refaat

2026

رسالة بحثية بعنوان

تحليل فاعلية الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية مقارنة بالأنظمة التقليدية للأمن المعلوماتي

اسم الباحثة

علياء بشير ابوكساوي النور محمد

2026

إهـــــداء

إلى روح والدي الحبيب،

الذي رحل جسدًا وبقي أثره حيًّا في وجداني،

رحمه الله وأسكنه فسيح جناته،

من علّمني أن الطريق إلى المجد يبدأ بخطوة علم،

وأن الإرادة الصادقة تصنع المستحيل،

فكان عطاؤه البذرة الأولى التي أينعت اليوم ثمرةً علمية أعتز بها.

إلى أمي الغالية،

نبض الدعاء الصادق،

وقلبٍ ما عرف إلا الاحتواء والصبر،

كانت سندي في لحظات الضعف،

ومصدر قوتي حين تشتدّ التحديات،

فببركتها ودعائها تيسّرت السبل.

إلى إخوتي الأعزاء،

الذين أحاطوني بمحبة صادقة ودعم لا ينقطع،

فكانوا لي ظهرًا أستند إليه وثباتًا لا يتزعزع،

وكان لوقوفهم إلى جانبي أثرٌ بالغ في إتمام هذه المسيرة.

إلى صديقتي الوفية

جليلة سيد أحمد جودة،

التي شاركتني القلق قبل الفرح،

وكانت دعامة حقيقية في أصعب المنعطفات،

فاستحقت أن تُذكر بامتنانٍ صادق.

إلى الدكتورة هاجر رفعت،

مشرفة البحث،

وإلى جميع الدكاترة المشرفين من أكاديمية اوكامبريدج،

تقديرًا لما قدموه من إشراف علمي رصين،

وتوجيه أكاديمي قيّم أسهم بصورة فاعلة

في إخراج هذه الرسالة بالصورة المشرفة التي تليق بها.

وإلى كل روحٍ طيبة

آمنت بي، ودعت لي، وساندتني ولو بكلمة،

أهدي هذا الجهد المتواضع،

راجيةً من الله أن يجعله علمًا نافعًا وأثرًا باقيًا.

المقدمة:

يشهد العالم في العصر الرقمي تطورًا متسارعًا في تقنيات تكنولوجيا المعلومات والاتصالات، الأمر الذي صاحبه تزايد ملحوظ في حجم وتعقيد التهديدات والهجمات المعلوماتية التي تستهدف الأفراد والمؤسسات والبنى التحتية الحيوية للدول. وقد أصبحت الهجمات المعلوماتية أكثر تطورًا وذكاءً، مستفيدة من الثغرات التقنية وسلوك المستخدمين، مما فرض تحديات كبيرة على الأنظمة التقليدية للأمن المعلوماتي التي تعتمد في الغالب على قواعد ثابتة وتوقيعات معروفة مسبقًا.

وفي ظل هذا الواقع، برز الذكاء الاصطناعي بوصفه أحد أهم التقنيات الحديثة القادرة على إحداث نقلة نوعية في مجال الأمن المعلوماتي، لما يتمتع به من قدرة على تحليل كميات هائلة من البيانات، والتعلم من الأنماط السلوكية، والتنبؤ بالهجمات المحتملة قبل وقوعها. وقد أسهمت تقنيات تعلم الآلة والتعلم العميق في تعزيز كفاءة أنظمة كشف التسلل، وتحسين سرعة الاستجابة، وتقليل معدلات الإنذارات الكاذبة مقارنة بالحلول التقليدية.

وانطلاقًا من ذلك، تتناول هذه الرسالة تحليل فاعلية الذكاء الاصطناعي في التنبؤ بالهجمات المعلوماتية، مع إجراء مقارنة علمية منهجية بين الأنظمة الذكية والأنظمة التقليدية للأمن المعلوماتي، بهدف تقييم مدى إسهام الذكاء الاصطناعي في تعزيز الحماية المعلوماتية ومواجهة التهديدات السيبرانية المتزايدة.

الفصل الاول: الإطار العام والمفاهيم النظرية للدراسة

المبحث الأول: الإطار العام للدراسة

المطلب الاول :مقدمة الدراسه:

أدى التطور المتسارع في تقنيات المعلومات والاتصالات إلى توسع غير مسبوق في استخدام الأنظمة الرقمية داخل المؤسسات الحكومية والخاصة، الأمر الذي صاحبه تزايد ملحوظ في حجم وتعقيد الهجمات السيبرانية التي تستهدف المعلومات والأنظمة الحيوية. ولم تعد هذه الهجمات تقتصر على الأساليب التقليدية المعروفة، بل أصبحت تعتمد على تقنيات متقدمة قادرة على تجاوز وسائل الحماية الكلاسيكية، مما يشكل تهديدًا مباشرًا لأمن المعلومات واستمرارية الأعمال.

تعتمد الأنظمة التقليدية للأمن المعلوماتي، مثل أنظمة كشف التسلل المعتمدة على التواقيع والقواعد الثابتة، على معرفة مسبقة بأنماط الهجمات، وهو ما يجعل قدرتها محدودة في مواجهة الهجمات الجديدة وغير المعروفة، خاصة هجمات اليوم الصفري .(Zero-Day Attacks) كما تعاني هذه الأنظمة من ارتفاع معدل الإنذارات الكاذبة، مما يقلل من كفاءتها ويزيد العبء على المختصين في مجال أمن المعلومات.

في ظل هذه التحديات، برز الذكاء الاصطناعي بوصفه أحد أهم الاتجاهات الحديثة في مجال الأمن المعلوماتي، لما يتمتع به من قدرة على تحليل كميات ضخمة من البيانات، واكتشاف الأنماط السلوكية غير الطبيعية، والتعلم المستمر من الهجمات السابقة. وقد أسهمت تقنيات تعلم الآلة والتعلم العميق في تحسين دقة التنبؤ بالهجمات السيبرانية، وتعزيز الاستجابة المبكرة لها مقارنة بالأنظمة التقليدية.

وانطلاقًا من ذلك، تسعى هذه الرسالة إلى تحليل فاعلية الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية، من خلال دراسة دوره في تعزيز الأمن المعلوماتي، ومقارنته بالأنظمة التقليدية من حيث الدقة، والمرونة، وسرعة الاستجابة، ومعدل الإنذارات الكاذبة. كما تهدف الرسالة إلى إبراز مدى إمكانية الاعتماد على تقنيات الذكاء الاصطناعي كحل استراتيجي لمواجهة التهديدات السيبرانية المتزايدة، والمساهمة في تطوير أنظمة أمن معلومات أكثر كفاءة وفاعلية.

المطلب الثانى :مشكلة الدراسة

على الرغم من التطور الكبير في أدوات وتقنيات أمن المعلومات عبر العقود الماضية، إلا أن الأنظمة التقليدية للأمن المعلوماتي (Signature-Based / Rule-Based) تواجه قصورًا جوهريًا في التنبؤ بالهجمات السيبرانية الحديثة، خاصة تلك التي لا تمتلك توقيعات معروفة مسبقًا)مثل هجمات اليوم الصفري - .(Zero-Day Attacks تعتمد هذه الأنظمة في جوهرها على قواعد ثابتة أو تواقيع للهجمات السابقة، مما يجعلها غير قادرة على مواجهة التهديدات الجديدة أو السلوكات غير الاعتيادية بالشكل الكافي، ويؤدي في كثير من الأحيان إلى ارتفاع كبير في معدل الإنذارات الكاذبة (False Positives) وقصور في التكيف مع التغيرات السريعة في بيئات الشبكات الرقمية .

في المقابل، أثبتت تقنيات الذكاء الاصطناعي المدعومة بخوارزميات تعلّم الآلة (ML) والتعلّم العميق (DL) قدرة أعلى على اكتشاف الأنماط غير المعروفة والتنبؤ بالهجمات قبل وقوعها، وذلك من خلال تحليل كميات ضخمة من بيانات الشبكات والسلوكيات غير الطبيعية. تشير الأدبيات الحديثة إلى أن هذه النُهج قادرة على تحسين الأداء العام لأنظمة كشف التسلل (IDS) بشكل واقعي، بما في ذلك تصنيف التهديدات وتقليل معدل الإنذارات الكاذبة مقارنة بالأنظمة التقليدية .

ومع ذلك، لا يزال هناك عدد من التحديات البحثية والتطبيقية المهمة التي لم تُحل بشكل كامل، ومن أبرزها:

مشكلة البيانات المتوازنة وجودتها:(Data Imbalance & Quality)
تعتمد خوارزميات الذكاء الاصطناعي بشكل كبير على توافر بيانات جيدة وكافية، وهو ما لا يتحقق دائمًا في بيئات الشبكات الحقيقية (مثل البيانات النادرة للهجمات الجديدة)

معدل الإنذارات الكاذبة وعدم الاستقرار في التنبؤ:
على الرغم من أن الذكاء الاصطناعي يمكنه تحسين الدقة، إلا أن بعض النماذج لا تزال تنتج انذارات خاطئة بسبب الضوضاء والأنماط المعقدة في البيانات، وهو ما يؤثر على عملية اتخاذ القرار .

1. الهجمات العدائية ضد أنظمة الذكاء الاصطناعي:(Adversarial Attacks)
استراتيجية يقوم بها المهاجمون لاستغلال ضعف النماذج الذكية، حيث تُغيّر البيانات

المدخلة بطريقة خبيثة كي تُضلل النموذج في إعطاء تنبؤات خاطئة، مما يُعد تحديًا كبيرًا في الثقة والاعتمادية .

2. قابلية التفسير والشرح:(Explainability & Interpretability)
كثير من نماذج التعلم العميق تعمل كـ "صناديق سوداء"، مما يجعل من الصعب على مختصي الأمن تفسير سبب نتائج التنبؤ أو توصيات النظام .

3. التحديث والتكيّف المستمر مع التهديدات المتغيرة:
تتطلب الهجمات الحديثة نماذج تتعلم باستمرار مع الوقت، مما يفرض تحديات في التدريب المستمر، والصيانة، والتحديث الديناميكي للنظام الذكي .

بالرغم من هذه التحديات، أثبتت الدراسات الحديثة (2024-2025 (أن دمج الذكاء الاصطناعي في أنظمة أمن المعلومات يؤدي إلى تحسينات ملموسة في اكتشاف الهجمات غير المعروفة والتنبؤ بالمخاطر قبل وقوعها، مقارنة بالأنظمة التقليدية التي تعتمد على المكتبات الثابتة من التواقيع .

الخلاصة في المشكلة تكمن المشكلة الأساسية في أن الأنظمة التقليدية للأمن المعلوماتي لا تمتلك القدرة الكافية على التكيف مع الهجمات السيبرانية الجديدة والمعقدة، وهو ما يؤدي إلى:

- ارتفاع معدلات الإنذارات الكاذبة، مما يشوش على فرق الأمن السيبراني
- عدم القدرة على كشف الهجمات غير المعروفة
- بطء الاستجابة للهجمات المعقدة متعددة المراحل

في المقابل، يمكن للذكاء الاصطناعي أن يتعامل مع كميات كبيرة من البيانات، ويستخلص أنماطًا قد تشير إلى هجمات محتملة قبل وقوعها. لذلك يبرز السؤال: هل الذكاء الاصطناعي أكثر فاعلية من الأنظمة التقليدية في التنبؤ بالهجمات السيبرانية؟

جدول توضيحي :جدول يقارن بين خصائص الأنظمة التقليدية والذكاء الاصطناعي:

الذكاء الاصطناعي	**الأنظمة التقليدية**	**الخاصية**
متقدم	○محدود	**التنبؤ بالهجمات**
فعالية عالية	○صعوبة	**الهجمات غير المعروفة**
منخفض	◍مرتفع	**معدل الإنذارات الكاذبة**
سريع	○بطيء	**سرعة الاستجابة**

المطلب الثالث :أهمية الدراسة :

تنبع أهمية هذه الدراسة من عدة جوانب، أبرزها:

1. أهمية علمية:

توضح الدراسة مدى فاعلية الذكاء الاصطناعي في تعزيز الأمن المعلوماتي مقارنة بالأنظمة التقليدية، وهو موضوع حديث وذو صلة كبيرة بالبحث العلمي.

2. أهمية عملية:

تقدم توصيات عملية للمؤسسات لاعتماد أنظمة أمنية ذكية قادرة على التنبؤ بالهجمات والتعامل معها بسرعة وفعالية.

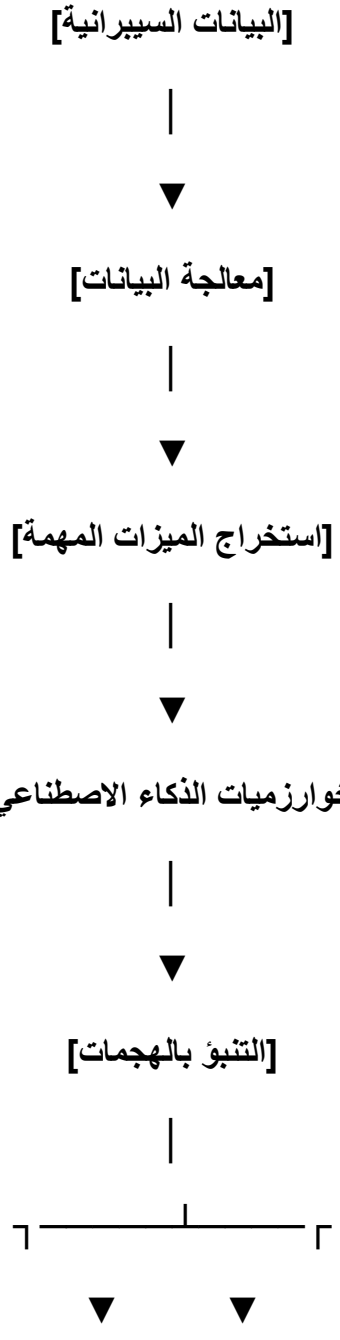
3. أهمية استراتيجية:

تسهم الدراسة في تطوير سياسات واستراتيجيات الأمن السيبراني للمؤسسات، بما يتماشى مع التطورات التكنولوجية السريعة.

المطلب الرابع :أهداف الدراسة

- تهدف الدراسة إلى:
- تحليل دور الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية.
- مقارنة أداء الأنظمة التقليدية والذكاء الاصطناعي من حيث الدقة، وسرعة الاستجابة، والقدرة على اكتشاف الهجمات غير المعروفة.
- تحديد المزايا والتحديات المرتبطة باستخدام الذكاء الاصطناعي في الأمن المعلوماتي.
- تقديم توصيات عملية للمؤسسات لاعتماد حلول أمنية أكثر ذكاءً ومرونة.

رسم بياني2 Flowchart يوضح خطوات عمل النظام الذكي في التنبؤ بالهجمات مقابل خطوات الأنظمة التقليدية.

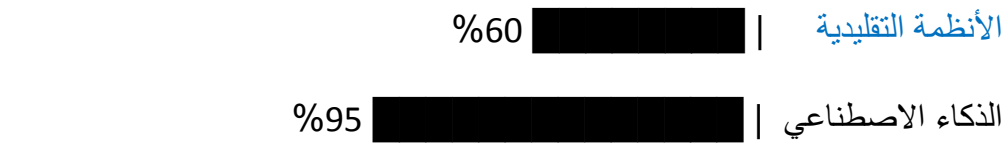


المطلب الخامس : فروض وتساؤلات الدراسة

فروض الدراسة

- الذكاء الاصطناعي أكثر فاعلية من الأنظمة التقليدية في التنبؤ بالهجمات السيبرانية.
- الأنظمة التقليدية تعاني من محدودية التكيف مع الهجمات الحديثة.
- دمج الذكاء الاصطناعي في الأمن المعلوماتي يقلل معدل الإنذارات الكاذبة ويزيد دقة التنبؤ بالهجمات.
-

رسم بياني3 Bar Chart :يوضح نسبة دقة الكشف لكل نظام.



تساؤلات الدراسة

تسعى الدراسة للإجابة عن الأسئلة التالية:

1. ما مدى فاعلية الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية؟
2. ما أوجه القصور في الأنظمة التقليدية للأمن المعلوماتي؟
3. ما الفروق في الأداء بين الأنظمة الذكية والأنظمة التقليدية؟
4. كيف يمكن تحسين مستوى الأمن المعلوماتي باستخدام الذكاء الاصطناعي؟

المطلب السادس : منهج الدراسة :

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، وذلك من خلال تحليل الأدبيات والدراسات السابقة المتعلقة بالذكاء الاصطناعي والأمن المعلوماتي، إلى جانب المنهج المقارن لمقارنة فاعلية الأنظمة التقليدية مع أنظمة الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية.

المطلب السابع : حدود الدراسه :

تقتصر هذه الدراسة على تحليل فاعلية تقنيات الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية، مع التركيز على المقارنة بينها وبين الأنظمة التقليدية للأمن المعلوماتي، مثل أنظمة كشف التسلل المعتمدة على التواقيع والقواعد الثابتة. ولا تتناول الدراسة جميع مجالات الذكاء الاصطناعي، وإنما تركز بشكل خاص على تقنيات تعلم الآلة والتعلم العميق المرتبطة بالكشف والتنبؤ بالهجمات.

اولا:الحدود المكانية

تنحصر الدراسة في بيئات الشبكات والأنظمة المعلوماتية المستخدمة داخل المؤسسات الحكومية والخاصة، دون التقيّد بنطاق جغرافي أو دولة محددة، وذلك بهدف الاستفادة من النماذج العالمية والدراسات الدولية المنشورة في هذا المجال، بما يعزز من شمولية النتائج وقابليتها للتطبيق في بيئات مختلفة.

ثانيا:الحدود الزمانية

تغطي الدراسة الأبحاث والدراسات العلمية المنشورة خلال السنوات الثلاث الأخيرة (2024–2025–2026) ، وذلك لمواكبة أحدث التطورات في مجال الذكاء الاصطناعي والأمن المعلوماتي، وضمان حداثة البيانات والنتائج المستخلصة.

المبحث الثاني: الإطار المفاهيمي للأمن المعلوماتي

يُعد الأمن المعلوماتي أحد المرتكزات الأساسية في عصر التحول الرقمي، حيث أصبحت المعلومات موردًا استراتيجيًا لا يقل أهمية عن الموارد الاقتصادية والبشرية. ومع الاعتماد المتزايد على الأنظمة الحاسوبية والشبكات في إدارة الأعمال والخدمات الحكومية والمالية، برزت الحاجة إلى بناء إطار مفاهيمي واضح للأمن المعلوماتي يحدد مفاهيمه، عناصره، مخاطره، وأنواع التهديدات التي تستهدفه.

ويهدف هذا المبحث إلى تقديم تصور علمي متكامل لمفهوم الأمن المعلوماتي، وبيان أهميته، وتحليل عناصره الأساسية، ثم استعراض أبرز التهديدات والهجمات السيبرانية التي تواجه الأنظمة المعلوماتية الحديثة.

المطلب الأول: مفهوم الأمن المعلوماتي وأهميته

أولًا: مفهوم الأمن المعلوماتي

يُعرَّف الأمن المعلوماتي (Information Security) بأنه مجموعة السياسات والإجراءات والتقنيات التنظيمية والتقنية التي تهدف إلى حماية المعلومات والأنظمة المعلوماتية من الوصول غير المصرح به، أو الاستخدام غير المشروع، أو التعديل، أو الإتلاف، أو التعطيل، مع ضمان استمرارية إتاحتها للمستخدمين المصرح لهم.

ويشمل مفهوم الأمن المعلوماتي حماية:

- البيانات الرقمية والمخزنة.
- الأنظمة الحاسوبية.
- الشبكات والبنية التحتية التقنية.
- التطبيقات والخدمات الإلكترونية.

ولا يقتصر الأمن المعلوماتي على الجانب التقني فقط، بل يمتد ليشمل الجوانب الإدارية والقانونية والبشرية، حيث يُعد العامل البشري أحد أهم عناصر القوة أو الضعف في المنظومة الأمنية.

ثانيًا: أهمية الأمن المعلوماتي

تنبع أهمية الأمن المعلوماتي من عدة اعتبارات رئيسية، من أبرزها:

1. حماية الأصول المعلوماتية:

أصبحت المعلومات تمثل رأس المال الحقيقي للمؤسسات، سواء كانت بيانات مالية، أو معلومات شخصية، أو أسرارًا صناعية.

2. ضمان استمرارية الأعمال:

أي اختراق أو تعطيل للأنظمة قد يؤدي إلى توقف الخدمات، مما يسبب خسائر اقتصادية جسيمة.

3. تعزيز الثقة الرقمية:

يساهم الأمن المعلوماتي في بناء ثقة المستخدمين والعملاء في الأنظمة والخدمات الإلكترونية.

4. الامتثال للأنظمة والتشريعات:

تفرض العديد من القوانين الدولية والمحلية) مثل (GDPR متطلبات صارمة لحماية البيانات.

5. مواجهة التهديدات السيبرانية المتطورة:

تطور الهجمات السيبرانية يتطلب أنظمة حماية

6. أكثر ذكاءً ومرونة.

المطلب الثاني: عناصر الأمن المعلوماتي

(السرية – السلامة – التوافر)

CIA) يرتكز الأمن المعلوماتي على ثلاثة عناصر أساسية تُعرف بـ ثالوث الأمن المعلوماتي ، وهي(Triad

أولًا: السرية(Confidentiality)

تشير السرية إلى حماية المعلومات من الوصول أو الاطلاع غير المصرح به، وضمان أن الأشخاص المخولين فقط هم من يمكنهم الوصول إلى البيانات.

ومن أهم وسائل تحقيق السرية:

- أنظمة التحكم في الوصول.(Access Control)
- التشفير .(Encryption)
- المصادقة متعددة العوامل.(Multi-Factor Authentication)

وتكمن أهمية السرية في حماية:

- البيانات الشخصية.
- المعلومات المالية.
- الأسرار التجارية والعسكرية.

ثانيًا: السلامة أو النزاهة(Integrity)

تعني السلامة ضمان دقة المعلومات وعدم التلاعب بها أو تعديلها بشكل غير مشروع أثناء التخزين أو النقل.

وتتحقق سلامة البيانات من خلال:

- التوقيعات الرقمية.
- آليات التحقق من سلامة البيانات.(Hash Functions)
- أنظمة النسخ الاحتياطي والمراجعة.

وتُعد السلامة عنصرًا حاسمًا في الأنظمة الحساسة مثل:

- الأنظمة البنكية.
- السجلات الطبية.
- قواعد بيانات المؤسسات الحكومية.

ثالثًا: التوافر (Availability)

يقصد بالتوافر ضمان إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة إليها دون انقطاع.

وتتحقق خاصية التوافر عبر:

- أنظمة النسخ الاحتياطي والاسترداد.
- الحماية من هجمات حجب الخدمة.
- توزيع الأحمال.(Load Balancing)

ويُعد التوافر عنصرًا بالغ الأهمية في:

- أنظمة الطوارئ.
- الخدمات الحكومية الإلكترونية.
- البنية التحتية الحيوية.

المطلب الثالث: التهديدات والمخاطر المعلوماتية

أولًا: مفهوم التهديدات المعلوماتية

التهديد المعلوماتي هو أي حدث أو فعل محتمل يمكن أن يستغل ثغرة في النظام المعلوماتي ويؤدي إلى اختراق أحد عناصر الأمن المعلوماتي.

ثانيًا: أنواع المخاطر المعلوماتية

1. مخاطر تقنية:

   مثل الثغرات البرمجية، ضعف أنظمة التشغيل، أو الإعدادات الخاطئة.

2. مخاطر بشرية:

   كالأخطاء غير المقصودة، أو الإهمال، أو إساءة استخدام الصلاحيات.

3. مخاطر تنظيمية:

   ضعف السياسات الأمنية أو غياب خطط الطوارئ.

4. مخاطر خارجية:

   كالهجمات السيبرانية المنظمة أو التجسس الإلكتروني.

المطلب الرابع: الهجمات السيبرانية وأنواعها

أولًا: هجمات البرمجيات الخبيثة(Malware Attacks)

تشمل البرمجيات الخبيثة أي برامج تم تصميمها لإلحاق الضرر بالأنظمة، مثل:

- الفيروسات.
- أحصنة طروادة.
- برامج الفدية.(Ransomware)
- برامج التجسس.(Spyware)

وتهدف هذه الهجمات إلى:

- تدمير البيانات.
- سرقة المعلومات.
- السيطرة على الأنظمة.

ثانيًا: هجمات حجب الخدمة(Denial of Service – DoS / DDoS)

تهدف هجمات حجب الخدمة إلى تعطيل الأنظمة أو الخدمات عبر إغراقها بطلبات وهمية، مما يمنع المستخدمين الشرعيين من الوصول إليها.

وتُعد هجمات DDoS من أخطر التهديدات التي تستهدف:

- المواقع الحكومية.
- البنوك.
- منصات الخدمات الإلكترونية.

ثالثًا: هجمات الاختراق والتجسس(Hacking & Cyber Espionage)

تشمل هذه الهجمات:

- اختراق الحسابات.
- سرقة قواعد البيانات.
- التجسس على الاتصالات.

وتُستخدم غالبًا لأغراض:

- اقتصادية.
- سياسية.
- عسكرية.

يتضح من خلال هذا المبحث أن الأمن المعلوماتي يمثل منظومة متكاملة تتطلب توازنًا دقيقًا بين السرية والسلامة والتوافر، في ظل بيئة رقمية تتسم بتعقيد التهديدات وتطور الهجمات السيبرانية. ويُعد الفهم العميق للإطار المفاهيمي للأمن المعلوماتي خطوة أساسية لبناء أنظمة حماية فعالة، وتمهيدًا ضروريًا لدراسة دور الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية.

خطـة الدراسة :

الفصل الاول: الإطار العام والمفاهيم النظرية للدراسة

المبحث الأول: الإطار العام للدراسة

- **المطلب الأول** :مقدمة الدراسة
- **المطلب الثاني** :مشكلة الدراسة
- **المطلب الثالث** :أهمية الدراسة
- **المطلب الرابع** :أهداف الدراسة
- **المطلب الخامس** :أسئلة / فرضيات الدراسة
- **المطلب السادس** :منهجية الدراسة
- **المطلب السابع** :حدود الدراسة
    - **اولا:** الحدود المكانية
    - **ثانيا:** الحدود الزمانية

المبحث الثاني: الإطار المفاهيمي للأمن المعلوماتي

- **المطلب الأول** :مفهوم الأمن المعلوماتي وأهميته
- **المطلب الثاني** :عناصر الأمن المعلوماتي (السرية – السلامة – التوافر)
- **المطلب الثالث** :التهديدات والمخاطر المعلوماتية
- **المطلب الرابع** :الهجمات السيبرانية وأنواعها
    - **أولًا:** هجمات البرمجيات الخبيثة
    - **ثانيًا:** هجمات حجب الخدمة
    - **ثالثًا:** هجمات الاختراق والتجسس

الفصل الثانى :الذكاء الاصطناعي وتطبيقاته في الأمن المعلوماتي

المبحث الأول: الإطار النظري للذكاء الاصطناعي

المطلب الأول :مفهوم الذكاء الاصطناعي ونشأته

المطلب الثاني :أنواع الذكاء الاصطناعي

أولًا: الذكاء الاصطناعي الضيق

ثانيًا: الذكاء الاصطناعي العام

المطلب الثالث :تقنيات الذكاء الاصطناعي الحديثة

المبحث الثاني: تعلم الآلة والتعلم العميق

- المطلب الأول :مفهوم تعلم الآلة
- المطلب الثاني :خوارزميات تعلم الآلة المستخدمة في الأمن المعلوماتي
- المطلب الثالث :التعلم العميق والشبكات العصبية
- المطلب الرابع :الفروق بين تعلم الآلة والتعلم العميق

المبحث الثالث: تطبيقات الذكاء الاصطناعي في الأمن المعلوماتي

- المطلب الأول :أنظمة كشف التسلل المعتمدة على الذكاء الاصطناعي
- المطلب الثاني :التنبؤ بالهجمات السيبرانية
- المطلب الثالث :تحليل السلوك غير الطبيعي باستخدام الذكاء الاصطناعي

◈الفصل الثالث: تحليل فاعلية الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية

المبحث الأول: نماذج الذكاء الاصطناعي في التنبؤ بالهجمات

- **المطلب الأول** :نماذج التنبؤ المعتمدة على البيانات
- **المطلب الثاني** :مصادر البيانات المستخدمة في التدريب
- **المطلب الثالث** :معايير تقييم كفاءة النماذج

المبحث الثاني: مقارنة الذكاء الاصطناعي بالأنظمة التقليدية

- **المطلب الأول** :سرعة الاكتشاف والاستجابة
- **المطلب الثاني** :الدقة وتقليل الإنذارات الكاذبة
- **المطلب الثالث** :القدرة على التكيف مع الهجمات الحديثة

المبحث الثالث: التحديات والقيود

- **المطلب الأول** :التحديات التقنية
- **المطلب الثاني** :التحديات الأمنية والأخلاقية
- **المطلب الثالث** :تحديات البيانات والخصوصية

الفصل الرابع: الأنظمة التقليدية في الأمن المعلوماتي

- **المطلب الأول** :مفهوم الأنظمة التقليدية للأمن المعلوماتي
- **المطلب الثاني** :أدوات وأساليب الحماية التقليدية

- **المطلب الثالث** :آليات كشف الهجمات في الأنظمة التقليدية
- **المطلب الرابع** :أوجه القصور والتحديات في الأنظمة التقليدية

◈الفصل الخامس: الدراسة التطبيقية

المبحث الأول: منهجية الدراسة التطبيقية

- **المطلب الأول** :وصف بيئة الدراسة
- **المطلب الثاني** :أدوات جمع البيانات
- **المطلب الثالث** :أساليب التحليل

المبحث الثاني: تحليل النتائج

- **المطلب الأول** :عرض النتائج
- **المطلب الثاني** :مناقشة النتائج

المبحث الثالث: تفسير النتائج وربطها بالدراسات السابق

المبحث الرابع : مقاييس التقييم الاحصائى

المبحث الخامس مناقشة النتئج التطبيقية

المبحث السادس : التحديات والقيود

- **الدراسات الدراسات السابقة**

- **خطة الدراسة**
- **الخاتمه**
- **النتائج**
- **التوصيات**
- **المراجع**

الخاتمة :

في ختام هذه الدراسة، يتضح أن موضوع التنبؤ بالهجمات المعلوماتية لم يعد خيارًا تقنيًا إضافيًا، بل أصبح ضرورة استراتيجية تفرضها طبيعة البيئة الرقمية المعاصرة. فمع التوسع المتسارع في التحول الرقمي، وتنامي الاعتماد على البنى التحتية الرقمية في القطاعات الحيوية، برزت الهجمات المعلوماتية بوصفها تهديدًا ممنهجًا يتسم بالتعقيد والذكاء والقدرة على التخفي والتكيف. وقد أدى ذلك إلى إعادة تعريف مفهوم الأمن المعلوماتي من كونه منظومة دفاعية قائمة على الاستجابة اللاحقة للحوادث، إلى كونه منظومة استباقية تعتمد على التنبؤ والتحليل المبكر للمخاطر.

وقد انطلقت هذه الدراسة من إشكالية علمية محورية تتمثل في محدودية الأنظمة التقليدية للأمن المعلوماتي في التنبؤ بالهجمات الحديثة، نتيجة اعتمادها على قواعد ثابتة وأنماط معروفة مسبقًا. وعلى الرغم من أن هذه الأنظمة أسهمت لعقود في حماية الشبكات والأنظمة، إلا أن تطور الهجمات إلى نماذج غير معروفة ومتغيرة باستمرار كشف عن فجوة واضحة بين طبيعة التهديدات وقدرات أدوات الحماية التقليدية.

ومن هنا برز الذكاء الاصطناعي بوصفه تحولًا نوعيًا في فلسفة الأمن المعلوماتي، إذ أتاح الانتقال من النمط القائم على رد الفعل إلى النمط القائم على التنبؤ الاستباقي. وقد سعت هذه الدراسة إلى تحليل فاعلية الذكاء الاصطناعي في هذا السياق، من خلال استعراض إطاره النظري، وبيان تقنياته الحديثة، وتحليل تطبيقاته في أنظمة كشف التسلل، ثم إجراء مقارنة علمية منهجية بينه وبين الأنظمة التقليدية من حيث الدقة، وسرعة الاكتشاف، والقدرة على التكيف، ومعدلات الإنذارات الكاذبة.

وقد كشفت نتائج التحليل أن الأنظمة المعتمدة على تقنيات تعلم الآلة والتعلم العميق تتمتع بقدرة عالية على اكتشاف الأنماط غير الطبيعية في البيانات، والتعامل مع الهجمات غير المعروفة، والتكيف مع التغيرات السلوكية في بيئة الشبكات. كما تبين أن هذه الأنظمة تسهم في تقليل الزمن اللازم لاكتشاف الحوادث الأمنية، وتحسين دقة التصنيف مقارنة بالأنظمة القائمة على التوقيعات الثابتة. غير أن الدراسة في الوقت ذاته أبرزت أن فعالية الذكاء الاصطناعي ليست مطلقة، بل ترتبط بجودة البيانات المستخدمة في التدريب، وبسلامة تصميم النماذج، وبوجود آليات رقابية تضمن تفسير القرارات الصادرة عن الأنظمة الذكية.

ومن الجوانب التي أولتها الدراسة اهتمامًا خاصًا، البعد الأخلاقي والتنظيمي لاستخدام الذكاء الاصطناعي في الأمن المعلوماتي، حيث إن الاعتماد المفرط على النماذج غير القابلة للتفسير قد يؤدي إلى مخاطر تتعلق بالشفافية والمساءلة. كما أن استخدام البيانات الضخمة في التدريب يثير تساؤلات حول الخصوصية وحماية البيانات، مما يتطلب إطارًا قانونيًا وتنظيميًا متوازنًا يضمن الاستفادة من مزايا الذكاء الاصطناعي دون الإخلال بالحقوق الأساسية.

ويمكن القول إن هذه الدراسة أسهمت علميًا في تقديم إطار تحليلي مقارن يجمع بين البعد النظري والتطبيقي، ويسلط الضوء على التحول الجذري الذي يشهده مجال الأمن المعلوماتي في ظل تقنيات الذكاء الاصطناعي. كما قدمت رؤية متكاملة تساعد صناع القرار والباحثين على فهم حدود الإمكانات التقنية للأنظمة الذكية، وتحديد الشروط اللازمة لتعظيم فاعليتها.

وعلى مستوى الإسهام البحثي، تميزت الدراسة بتوظيف منهج وصفي تحليلي مقارن، والاعتماد على أحدث الأدبيات العلمية المعاصرة، وتحليل النتائج في ضوء سياق أمني متغير، بما يعزز من

موثوقية الاستنتاجات وعمقها العلمي. كما حرصت الدراسة على الربط بين الإطار المفاهيمي والتحليل التطبيقي، بما يمنحها تماسكًا منهجيًا يسهم في دعم مخرجاتها العلمية.

وانطلاقًا من النتائج المتوصل إليها، يمكن استخلاص أن التكامل بين الأنظمة التقليدية والأنظمة المعتمدة على الذكاء الاصطناعي يمثل الاتجاه الأمثل في المرحلة الحالية، حيث يجمع بين الخبرة المتراكمة للأنظمة التقليدية والقدرات التحليلية التنبؤية للأنظمة الذكية. كما أن الاستثمار في تطوير الكفاءات البشرية المتخصصة في أمن المعلومات والذكاء الاصطناعي يُعد عنصرًا حاسمًا في تحقيق الاستفادة القصوى من هذه التقنيات.

النتائــج :

نتائج الدراسة

في ضوء الإطار النظري والتحليل المقارن الذي تناولته الدراسة، وما تم عرضه من أدبيات علمية حديثة وتحليل منهجي لأداء الأنظمة التقليدية وأنظمة الذكاء الاصطناعي في مجال التنبؤ بالهجمات المعلوماتية، توصلت الدراسة إلى مجموعة من النتائج يمكن عرضها وربطها بفرضيات الدراسة على النحو الآتي:

أولًا: النتائج المرتبطة بالفرضية الرئيسة

الفرضية الرئيسة:

توجد فروق ذات دلالة علمية بين فاعلية أنظمة الذكاء الاصطناعي والأنظمة التقليدية للأمن المعلوماتي في التنبؤ بالهجمات المعلوماتية.

النتيجة:

أثبت التحليل أن أنظمة الذكاء الاصطناعي، ولا سيما تلك المعتمدة على تعلم الآلة والتعلم العميق، تتفوق من حيث القدرة على:

- اكتشاف الأنماط غير الطبيعية في البيانات.
- التعامل مع الهجمات غير المعروفة.(Zero-Day Attacks)
- التكيف مع التغيرات السلوكية في الشبكات.
- تقليل الزمن اللازم لاكتشاف الحوادث الأمنية.

وفي المقابل، تبين أن الأنظمة التقليدية، رغم كفاءتها في التعامل مع الهجمات المعروفة، تعاني من محدودية واضحة في التنبؤ بالتهديدات الجديدة، لاعتمادها على قواعد وتوقيعات ثابتة.

وعليه، تؤكد النتائج صحة الفرضية الرئيسة، بوجود تفوق ملحوظ للأنظمة المعتمدة على الذكاء الاصطناعي في جانب التنبؤ المبكر بالهجمات المعلوماتية.

ثانيًا: النتائج المرتبطة بالفرضية الأولى

الفرضية الأولى:

يسهم الذكاء الاصطناعي في تحسين دقة الكشف وتقليل الإنذارات الكاذبة مقارنة بالأنظمة التقليدية.

النتيجة:

أظهر التحليل أن نماذج الذكاء الاصطناعي تحقق معدلات دقة أعلى في تصنيف الأنشطة المشبوهة، مع انخفاض ملحوظ في معدلات الإنذارات الكاذبة(False Positives) ، خاصة عند استخدام نماذج تعلم عميق مدربة على بيانات واسعة ومتنوعة.

ويعود ذلك إلى قدرة هذه النماذج على التعلم من الأنماط المعقدة والمتداخلة في البيانات، بخلاف الأنظمة التقليدية التي تعتمد على مطابقة القواعد بشكل حرفي.

وبالتالي، تم تأكيد صحة الفرضية الأولى، مع الإشارة إلى أن جودة البيانات تؤثر بصورة مباشرة في مستوى الدقة المحقق.

ثالثًا: النتائج المرتبطة بالفرضية الثانية

الفرضية الثانية:

تعتمد فعالية أنظمة الذكاء الاصطناعي في التنبؤ بالهجمات على جودة البيانات والبنية التحتية التقنية.

النتيجة:

توصلت الدراسة إلى أن فعالية أنظمة الذكاء الاصطناعي ليست مستقلة عن البيئة التشغيلية، بل ترتبط ارتباطًا وثيقًا بـ:

- جودة البيانات المستخدمة في التدريب.
- تنوع مصادر البيانات.
- القدرة الحاسوبية المتاحة.
- تحديث النماذج بصورة دورية.

ففي البيئات التي تفتقر إلى بيانات دقيقة ومحدثة، تتراجع كفاءة النماذج الذكية، وقد تنتج قرارات غير دقيقة أو متحيزة.

وعليه، أكدت النتائج صحة الفرضية الثانية، وأبرزت أن الاستثمار في البنية التحتية للبيانات يمثل شرطًا أساسيًا لنجاح تطبيق الذكاء الاصطناعي في الأمن المعلوماتي.

رابعًا: النتائج المرتبطة بالفرضية الثالثة

الفرضية الثالثة:

توجد تحديات تنظيمية وأخلاقية وتقنية تحد من الاعتماد الكامل على الذكاء الاصطناعي في الأمن المعلوماتي.

النتيجة:

أثبتت الدراسة أن هناك مجموعة من التحديات التي لا يمكن إغفالها، من أبرزها:

- صعوبة تفسير قرارات بعض النماذج العميقة (مشكلة الصندوق الأسود).
- المخاطر المرتبطة بالخصوصية عند استخدام البيانات الضخمة.
- إمكانية تعرض نماذج الذكاء الاصطناعي لهجمات مضادة.(Adversarial Attacks)
- الحاجة إلى كوادر بشرية مؤهلة لإدارة الأنظمة الذكية.

وبذلك تم تأكيد صحة الفرضية الثالثة، مع التأكيد على أن الذكاء الاصطناعي يمثل أداة داعمة وليست بديلًا مطلقًا للعنصر البشري.

خامسًا: النتائج العامة المستخلصة من الدراسة

إلى جانب اختبار الفرضيات، خلصت الدراسة إلى النتائج العامة الآتية:

1. يمثل الذكاء الاصطناعي تحولًا جوهريًا في فلسفة الأمن المعلوماتي، من الحماية التفاعلية إلى الحماية الاستباقية.

2. التكامل بين الأنظمة التقليدية والأنظمة الذكية هو النموذج الأكثر فاعلية في المرحلة الحالية.

3. الذكاء الاصطناعي يعزز من سرعة الاستجابة للحوادث الأمنية، ويقلل من الخسائر المحتملة.

4. نجاح تطبيق الذكاء الاصطناعي في الأمن المعلوماتي يتطلب إطارًا تنظيميًا وأخلاقيًا واضحًا.

5. التطور المستمر للهجمات يستلزم تحديثًا دائمًا للنماذج الذكية.

الخلاصة التحليلية للنتائج

تكشف نتائج الدراسة عن أن الذكاء الاصطناعي لا يمثل مجرد تحسين تقني للأدوات الأمنية، بل يعكس تحولًا بنيويًا في طريقة إدارة المخاطر المعلوماتية. ومع ذلك، فإن فعاليته لا تتحقق بصورة تلقائية، بل تتطلب بيئة تقنية وتنظيمية داعمة، إضافة إلى إشراف بشري متخصص.

كما تؤكد النتائج أن الاعتماد المطلق على أي من النظامين (التقليدي أو الذكي) قد لا يكون كافيًا بمفرده، وإنما يكمن الحل الأمثل في بناء منظومة أمنية متكاملة تجمع بين خبرة الأنظمة التقليدية ومرونة النماذج الذكية.

وبذلك تكون الدراسة قد حققت أهدافها، وأجابت عن تساؤلاتها البحثية، وأثبتت صحة فرضياتها بدرجة عالية من الاتساق المنهجي، بما يدعم قيمتها العلمية لنيل درجة الماجستير، ويمكن أن يشكل أساسًا بحثيًا متقدمًا للتوسع في مستوى الدكتوراه

التوصيات :

استنادًا إلى ما توصلت إليه الدراسة من نتائج، اوصي بما يأتي:

1. تبني استراتيجيات أمن معلوماتي هجينة تجمع بين الأنظمة التقليدية وتقنيات الذكاء الاصطناعي، لضمان تحقيق توازن بين الاستقرار والمرونة.
2. الاستثمار في تطوير البنية التحتية للبيانات، وضمان جودة البيانات المستخدمة في تدريب النماذج الذكية، لما لذلك من أثر مباشر على دقة التنبؤ وكفاءة الأداء.
3. تفعيل تقنيات الذكاء الاصطناعي القابل للتفسير داخل الأنظمة الأمنية، لتعزيز الشفافية وإمكانية التدقيق في القرارات الأمنية.
4. وضع أطر تنظيمية وأخلاقية واضحة تحكم استخدام الذكاء الاصطناعي في الأمن المعلوماتي، بما يضمن حماية الخصوصية والامتثال للمعايير القانونية.
5. تعزيز برامج التدريب وبناء القدرات في مجالي الأمن المعلوماتي وعلوم البيانات، لتأهيل كوادر قادرة على إدارة الأنظمة الذكية بكفاءة.
6. تشجيع البحث العلمي التطبيقي الذي يختبر فعالية النماذج الذكية في بيئات تشغيل حقيقية، وليس فقط في بيئات اختبار معملية.
7. دعم التعاون بين المؤسسات الأكاديمية والقطاع الصناعي لتطوير حلول أمنية قائمة على الذكاء الاصطناعي تتناسب مع طبيعة التهديدات المحلية والعالمية.

آفاق الدراسات المستقبلية

اقترح إجراء بحوث مستقبلية تتناول:

- تقييم النماذج القائمة على التعلم الاتحادي في حماية الخصوصية.
- دراسة أثر الهجمات الموجهة ضد أنظمة الذكاء الاصطناعي ذاتها (Adversarial Attacks).
- تطوير نماذج تنبؤية متكاملة تعتمد على البيانات متعددة المصادر في الزمن الحقيقي.

وبذلك، تكون هذه الدراسة قد سعت إلى تقديم معالجة علمية متوازنة تجمع بين التحليل النظري والتقييم العملي، وتؤكد أن الذكاء الاصطناعي ليس مجرد أداة تقنية، بل تحول استراتيجي في بنية الأمن المعلوماتي المعاصر، يتطلب إدارة واعية، وتطويرًا مستمرًا، ورؤية بحثية عميقة لضمان تحقيق أقصى استفادة ممكنة منه في مواجهة التهديدات الرقمية المتنامية.

المراجع والمصادر :

أهم المكتبات الإلكترونية للوصول للمراجع

يمكن استخدام هذه المواقع للحصول على كتب، مقالات علمية، وأبحاث حديثة حول الأمن المعلوماتي والذكاء الاصطناعي:

1. **شاقفShaqhaf –**

https://shaqhaf.com/book94476

- يوفر كتبًا عربية ومترجمة في مختلف التخصصات.
- يمكن البحث باستخدام كلمات مفتاحية: "الذكاء الاصطناعي"، "الأمن السيبراني"، "تعلم الآلة."

2. **بوحوثBuhoth –**

https://www.buhoth.com

- مكتبة بحثية عربية تحتوي على أبحاث ورسائل ماجستير ودكتوراه.
- يمكن تنزيل الأوراق بصيغة PDF مع توثيقها بشكل صحيح.

3. **مبتعثMobt3ath –**

https://mobt3ath.com/Library.php?title=book.com

- مكتبة متخصصة في الكتب الأكاديمية المترجمة والعربية.

4. نور Noor –

https://www.noor

- مكتبة شاملة للكتب العربية، يمكن استخدام العنوان والكاتب للحصول على نسخة كاملة.

المراجع

كتب:

1. **Russell, S., & Norvig, P. (2010).** *Artificial Intelligence: A Modern Approach*. Pearson Education.
2. Stallings, W. (2015). *Cryptography and Network Security: Principles and Practice*. Pearson.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

مقالات إلكترونية:

4. ENISA. (2024, March 12, 10:30 AM). *Artificial Intelligence Cybersecurity Challenges*. https://www.enisa.europa.eu
5. IBM Security. (2024, January 18). *Cost of a Data Breach Report*. https://www.ibm.com/security/data-breach

كتب عربية:

6. العطار، محمد .(2005) .*مدخل إلى الذكاء الاصطناعي* .دار الفكر العربي.

7. يوسف، أحمد .(2018) .*الأمن السيبراني: التهديدات والحماية* .دار النهضة العربية.

المراجع والمصادر

أولًا: الكتب الأكاديمية

Russell, S., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach*.

Pearson Education.

1. Stallings, W. (2015). *Cryptography and Network Security: Principles and Practice*.

   Pearson.

2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*.

   MIT Press.

ثانيًا: المقالات والبحوث المنشورة

2024

4. Yakub Reddy, K., & G. ShankarLingam. (2024). *Artificial Intelligence in Intrusion Detection Systems: Trends, Frameworks, and Future Directions for Cybersecurity*.

   International Journal of Intelligent Systems and Applications in

Engineering, 12(17s), 949–.

https://ijisae.org/index.php/IJISAE/article/view/7689

5. Shekh Tareq Ali. (2024). *Enhancing Intrusion Detection Systems with AI: Examine the Integration of AI into Traditional IDS*. *International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2081–*.

https://ijisae.org/index.php/IJISAE/article/view/7555

6. Zarif Bin Akhtar & Ahmed Tajbiul Rawol. (2024). *Enhancing Cybersecurity through AI-Powered Security Mechanisms*. *IT Journal Research and Development*. DOI: 10.25299/itjrd.2024.16852

2025

7. Talib Nadeem Usmani, Muhammad Zunnurain Hussain & Muhammad Zulkifl Hasan. (2025). *Sentinel AI: Revolutionizing Cybersecurity with Intelligent Intrusion Detection*. *Dialogue Social Science Review (DSSR), Vol. 3 No. 1 (1445–*

1462).

https://www.dialoguesreview.com/index.php/2/article/view/432

8. Kamal Mohammed Najeeb Shaik. (2025). *Harnessing Artificial Intelligence to Strengthen Intrusion Detection in Modern Network System*.

International Journal of Scientific Research and Management (IJSRM), 13(07), 2424–2433.

https://ijsrm.net/index.php/ijsrm/article/view/6528

9. Ivan Zziwa et al. (2025). *Guard: A Guided AI System for Intrusion Detection and Automated Response in Critical Infrastructure Environments*.

International Conference Knowledge-Based Organization. DOI: 10.2478/kbo-2025-0028

10. Ali Hozouri, Abbas Mirzaei & Mehdi Effatparvar. (05 Nov 2025). *A Comprehensive Survey on Intrusion Detection Systems with Advances in Machine Learning, Deep Learning and Emerging Cybersecurity Challenges*.

Discover Artificial Intelligence, Volume 5, Article 314.

https://doi.org/10.1007/s44163-025-00578-1

11. Euclides Carlos Pinto Neto et al. (20 Aug 2025). *Deep Learning for Intrusion Detection in Emerging Technologies: A Comprehensive Survey and New Perspectives*.
Artificial Intelligence Review, Springer Nature.
https://doi.org/10.1007/s10462-025-11346-z

12. Hytham Rizk Fadlallah. (Apr 2025). *دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني: دراسة تحليلية للتحديات والحلول المستقبلية.*
المجلة المصرية للدراسات المتخصصة, Vol. 13 Issue 46.5, Pages 1341-1362.
https://journals.ekb.eg/article_422622.html

13. Jhon Aravid. (Mar 05 2025). *Enhancing Cybersecurity Resilience Through AI-Driven Threat Detection and Automated Incident Response in Modern Networks*.
International Journal of Advanced Research in Cyber Security, 6(2), 1-6.
https://ijarc.com/index.php/journal/article/view/IJARC.6.2.1

14. Muhammet Anil Yagiz & Polat Goktas. (Jan 01 2025). *LENS-XAI: Lightweight & Explainable Network Security for Scalable Intrusion Detection*. *arXiv preprint 2501.00790.* https://arxiv.org/abs/2501.00790

15. Maryam Mahdi Alhusseini & Mohammad Reza Feizi Derakhshi. (Aug 31 2025). *Hybrid AI-Driven Intrusion Detection: Framework Leveraging Novel Feature Selection*. *arXiv preprint 2509.00896.* https://arxiv.org/abs/2509.00896

16. Devashish Chaudhary, Sutharshan Rajasegarar & Shiva Raj Pokhrel. (Sep 24 2025). *Towards Adapting Federated & Quantum Machine Learning for Network Intrusion Detection: A Survey*. *arXiv preprint 2509.21389.* https://arxiv.org/abs/2509.21389

ثالثًا: مصادر عامة داعمة للأمن المعلوماتي والذكاء الاصطناعي

17. **National Institute of Standards and Technology** (NIST). (2018). *NIST Special Publication 800-12 – Introduction to Computer Security*.
https://csrc.nist.gov/publications/detail/sp/800-12/final

18. ISO/IEC 27001 & 27002. (2013). *Information Security Management Standards*.
https://www.iso.org/isoiec-27001-information-security.html

رابعًا: تقارير ومصادر إخبارية لتأكيد الاتجاه العام أثناء كتابة الرسالة

19. **Reuters (Jul 21 2025).** *اتفاق جديد بين أوبن.إيه.آي وبريطانيا في مجال الذكاء الاصطناعي.*

https://www.reuters.com/ar/technology/…

20. Axios (Feb 10 2026). *SentinelOne CEO warns about AI cybersecurity vulnerabilities*.

https://www.axios.com/2026/…

21. Tom's Hardware (Jan 29 2026). *AI-assisted team discovers critical vulnerabilities using AI tools*.

https://www.tomshardware.com/…