دور الذكاء الاصطناعي AI في تعزيز أمن وكفاءة أنظمة إنترنت الأشياء IOT

فيصل الهادي محمد شهوب

كلية طرابلس للعلوم والتقنية. طرابلس, ليبيا

shhoob@gmail.com

وسام الدوكالي شندور

كلية طرابلس للعلوم والتقنية. طرابلس, ليبيا

w.shandour@outlook.com

تاريخ الاستلام:
2024/04/06م
القبول:
2024/05/08م
تاريخ النشر:
2024/06/01م

ملخص البحث:

يشهد العالم انتشارًا واسعًا لتقنية إنترنت الأشياء التي تغزو جميع جوانب حياتنا. هذه التقنية تسمح للأجهزة بالتواصل وتبادل البيانات، تقدم العديد من الفوائد، لكنها تثير أيضًا مخاوف أمنية وخصوصية كبيرة. أحد القضايا الرئيسية التي تواجه إنترنت الأشياء هو الأمان، يمكن للمخترقين استغلال ثغرات أمان الأجهزة لسرقة البيانات الحساسة أو تعطيل الأنظمة الحيوية. بالإضافة إلى ذلك، فإن الخصوصية تشكل تحديًا كبيرًا، حيث يمكن جمع كميات هائلة من البيانات الشخصية من خلال أجهزة إنترنت الأشياء، مما يفتح الباب أمام الاستخدامات غير المشروعة لهذه البيانات.

لحسن الحظ، يقدم الذكاء الاصطناعي حلولًا واعدة لمواجهة هذه التحديات. يمكن استخدام تقنيات الذكاء الاصطناعي مثل التعلم الآلي وتحليل البيانات الضخمة للكشف عن التهديدات بشكل استباقي، والاستجابة لها بسرعة وكفاءة. كما يمكن للذكاء الاصطناعي تحسين أمان الأجهزة من خلال اكتشاف الثغرات الأمنية وإصلاحها بشكل تلقائي. دور الذكاء الاصطناعي لا يقتصر في إنترنت الأشياء على الأمن فقط ، يمكن أيضًا تحسين كفاءة الأنظمة، وتوفير تجربة مستخدم أفضل، وتطوير تطبيقات جديدة مبتكرة. على سبيل المثال، يمكن للذكاء الاصطناعي تحليل البيانات التي تجمعها أجهزة إنترنت الأشياء للتنبؤ باحتياجات المستخدمين وتقديم توصيات مخصصة.

تهدف هذه الورقة البحثية إلى دراسة التكامل بين الذكاء الاصطناعي وإنترنت الأشياء، مع التركيز بشكل خاص على كيفية استغلال قدرات الذكاء الاصطناعي لتعزيز أمن وكفاءة أنظمة إنترنت الأشياء. سنتناول في البداية التحديات والمخاطر الأمنية التي تواجه هذه الأنظمة، ثم ننتقل إلى مناقشة دور الذكاء الاصطناعي في اكتشاف التهديدات والاستجابة لها بشكل فعال. بالإضافة إلى ذلك، سنستكشف كيفية تطبيق تقنيات الذكاء الاصطناعي لبناء أنظمة إنترنت أشياء أكثر ذكاءً وقدرة على التكيف مع التغيرات المتسارعة.

الكلمات المفتاحية: الذكاء الاصطناعي , إنترنت الأشياء الأنظمة الذكية , التهديدات السيبرانية , خوارزميات التعلم الآلي.

الإحالة: بأسلوب نظام جميعة علم النفس الأمريكية الإصدار السابع..

The role of artificial intelligence (AI) in enhancing the security and efficiency of Internet of Things (IoT) systems.

FAISAL ELHADE MOHANNED SHHOOB
Tripoli College of Science and Technology
shhoob@gmail.com

WESSAM AlDUKALI SHANDOUR
Tripoli College of Science and Technology
w.shandour@outlook.com

Received (date):
.../..../2024
Accepted (date):
..../.../2024
Published (date):
...../.../2024

Abstract: (12 cm)

The world is witnessing a widespread proliferation of Internet of Things technology, permeating every aspect of our lives. This technology empowers devices to communicate and exchange data, offering numerous benefits but also raising significant security and privacy concerns. One of the primary challenges facing the IoT is security; hackers can exploit device vulnerabilities to steal sensitive data or disrupt critical systems. Additionally, privacy poses a significant challenge, as vast amounts of personal data can be collected through IoT devices, opening the door to the misuse of this data.

Fortunately, artificial intelligence offers promising solutions to address these challenges. Artificial intelligence techniques such as machine learning and big data analysis can be used to proactively detect threats and respond to them quickly and efficiently. AI can also enhance device security by automatically detecting and patching vulnerabilities. The role of AI in the Internet of Things is not limited to security; it can also improve system efficiency, provide a better user experience, and develop innovative new applications. For example, AI can analyze data collected by IoT devices to predict user needs and provide personalized recommendations.

This research paper aims to investigate the integration of artificial

intelligence and the Internet of Things, with a particular focus on how AI can be leveraged to enhance the security and efficiency of IoT systems. We will initially address the security challenges and threats facing these systems, followed by a discussion on the role of AI in detecting and responding to threats effectively. Additionally, we will explore how AI techniques can be applied to build more intelligent and adaptable IoT systems.

Keyword Artificial Intelligence (AI), Internet of Things (IoT) Intelligent Systems, Cyber Threats, Machine Learning Algorithms.

1- الإطار العام للدراسة

1-1 المقدمة

يشهد عالمنا تحولاً رقميًا سريعًا مدفوعًا بتطور تقنيات الذكاء الاصطناعي وإنترنت الأشياء. حيث تُتيح هذه التقنيات إمكانيات هائلة لتحسين مختلف جوانب حياتنا. في إنترنت الأشياء، يمكن أن يكون 'الشيء' أي كائن مادي، من الأجهزة المنزلية إلى السيارات، مزودة بتقنية تسمح لها بالاتصال بالإنترنت وتبادل البيانات. تتنوع الأجهزة التي تشكل إنترنت الأشياء بشكل كبير، بدءًا من أجهزة الاستشعار الحرارية وصولاً إلى الأجهزة المعقدة مثل السيارات والطائرات ذاتية القيادة. تتيح التكنولوجيا المضمنة للأجهزة جمع البيانات من بيئتها (درجة الحرارة، الرطوبة، الحركة) وتحليلها واتخاذ قرارات بناءً عليها، دون الحاجة إلى تدخل بشري. إنترنت الأشياء يعتمد بشكل أساسي على الاتصال بين الأشياء والتطبيقات السحابية، مما يتيح تبادل البيانات وتحليلها وتقديم خدمات ذكية للمستخدمين(Mouha , 2021)

إنترنت الأشياء هي شبكة واسعة من الأجهزة والأشياء المتصلة بالإنترنت، هذه الأجهزة قادرة على جمع البيانات وتبادلها وتحليلها، مما يتيح لنا اتخاذ قرارات أكثر ذكاءً وتحسين كفاءة العمليات. على سبيل المثال ثلاجة تطلب تلقائيًا الحليب عندما ينفد، نظام إضاءة يتكيف مع حالتك المزاجية، أو سيارة تسير ذاتياً. كل هذا وأكثر أصبح ممكنًا بفضل إنترنت الأشياء. (Atzori et al., 2010)

وقد أشار (Whitmore et al., 2015). الى أن الإنترنت يشهد تطوراً متسارع من صفحات الويب الثابتة إلى شبكات تفاعلية تسمح للمستخدمين بمشاركة المعلومات الى ظهور الويب الدلالي، الذي أتاح الى الآلات من فهم معنى المعلومات الموجودة على الويب، وهذا بدوره سمح بفتح آفاق جديدة للذكاء الاصطناعي. وفي دراسة أخرى قام بها (García وأخرون , 2018) أشار الى أن الذكاء الأصطناعي هو قدرة الآلة على أداء المهام المعرفية التي تتطلب عادةً ذكاءً بشرياً، أما إنترنت الأشياء فهو شبكة من الأشياء المادية المضمنة بأجهزة استشعار وبرامج وتقنيات أخرى بغرض ربط البيانات وتبادلها مع الأجهزة والأنظمة الأخرى عبر الإنترنت. في حين أشار (Tomasik,2016) الى أن الذكاء الاصطناعي، مجال علمي يهتم بتصميم أنظمة قادرة على محاكاة القدرات الذهنية للإنسان، مثل التعلم والتفكير وحل المشاكل، وعندما يتم دمج الذكاء الاصطناعي مع إنترنت الأشياء ، نحصل على أنظمة أكثر ذكاءً وقدرة على التكيف مع المتغيرات. على سبيل المثال، يمكن للذكاء الاصطناعي تحليل البيانات التي تجمعها أجهزة إنترنت الأشياء والتنبؤ بالأعطال قبل حدوثها أو أكتشاف المخاطر والتهديدات ومواجهتها أو تقديم توصيات مخصصة للمستخدمين.

2-1 مشكلة الدراسة

لايزال البحث الأكاديمي حول أنترنت الأشياء في مراحله الأولى، ولكن لديه القدرة على لعب دور متزايد في ضمان حدود أمان وموثوقية أنترنت الأشياء، ومع تزايد الاعتماد على هذه الأنظمة في مختلف المجالات أصبح تأمينها أولوية قصوى. بالمقابل تلعب تقنيات الذكاء الاصطناعي دورًا محوريًا؛ يمكنها تحليل كميات هائلة من البيانات والكشف عن الأنماط غير الطبيعية. واستنادا على ذلك ولغرض الإلمام بموضوع الدراسة يمكن صياغة مشكلة البحث في السؤال الرئيس التالي :

كيف يمكن الاستفادة من تقنيات الذكاء الاصطناعي لتعزيز أمن وكفاءة أنظمة إنترنت الأشياء؟

ويتفرع من هذا السؤال عدداً من الأسئلة الفرعية:

- ما هي أبرز التهديدات الأمنية التي تتعرض لها أنظمة إنترنت الأشياء؟
- كيف يمكن للذكاء الاصطناعي أن يساهم في الكشف عن هذه التهديدات والتصدي لها؟
- ما هي تأثيرات الذكاء الاصطناعي على أداء وكفاءة أنظمة إنترنت الأشياء؟

3-1 أهمية الدراسة

تُعتبر تقنية إنترنت الأشياء شبكة متنامية من الأجهزة المترابطة التي تجمع وتبادل البيانات حول العالم، مما يفتح آفاقًا جديدة في مجالات عديدة. ولكن مع هذا التطور السريع، تظهر تحديات أمنية كبيرة، مثل خطر الاختراق والوصول غير المصرح به إلى البيانات الحساسة. يهدف هذا البحث إلى تسليط الضوء على هذه التحديات الأمنية، واستكشاف دور الذكاء الاصطناعي في تعزيز أمن وكفاءة أنظمة إنترنت الأشياء. من خلال دمج قدرات الذكاء الاصطناعي مع مرونة إنترنت الأشياء، يمكن تطوير أنظمة أكثر ذكاءً وقدرة على التكيف مع التهديدات المتطورة.يسعى الباحثان إلى إجراء دراسة شاملة لتقييم أثر هذا الدمج على الأمن، وتحديد أفضل الممارسات لضمان حماية البيانات والأجهزة المتصلة. كما يهدف البحث إلى إثراء المعرفة المحلية في هذا المجال، وتشجيع المزيد من الباحثين على الانخراط في هذا المجال الواعد.

4-1 فرضيات الدراسة

تتركز هذه الورقة على فرضية رئيسية وهي تأثير الذكاء الاصطناعي في تعزيز أمن وكفاءة أنظمة أنترنت الأشياء. ويتفرع من هذه الفرضية الفرضيات الفرعية التالية:

- تحديد التحديات والمخاطر التي تواجه أنظمة انترنت الاشياء

- مامدى تأثير تقنيات الذكاء الاصطناعي في التخفيف من المخاطر والتهديدات والتحديات التي تواجه أنظمة أنترنت الأشياء.
- أثر تقنيات الذكاء الاصطناعي في تعزيز كفاءة أنظمة أنترنت الأشياء.

1-5 منهجية الدراسة

اعتمدت هذه الورقة على المنهج الوصفي للإجابة على أسئلة البحث، وذلك من خلال المسح المكتبي للمجلات العلمية والدوريات الصادرة عن المنظمات الدولية المتخصصة والبحوث والدراسات الجامعية الاجنبية والعربية ، حيث تمت مناقشة القضايا الأمنية والتحديات التي تواجه أنظمة أنترنت الأشياء ودور تقنيات الذكاء الأصطناعي في المساهمة في رفع مستوى الامن والكفاءة في أنظمة أنترنت الأشياء.

1-6 الدراسات السابقة

1-6-1 دراسة (Geir & Abomhara، 2014) بعنوان الأمن والخصوصية في إنترنت الأشياء: الوضع الحالي والقضايا المفتوحة.

تُسلّط هذه الدراسة الضوء على التحديات الأمنية والخصوصية التي تواجه أنظمة إنترنت الأشياء وتُناقش العديد من التهديدات والمخاطر التي تُهدّد هذه الأنظمة، مثل هجمات البرامج الضارة، هجمات رفض الخدمة، انتهاكات البيانات وانتهاكات الخصوصية. وتُقدم الدراسة أيضًا مجموعة من الحلول المقترحة لحماية البيانات في إنترنت الأشياء تشمل التشفير، المصادقة، تحديد المعدل، تقنيات التخفيف من هجمات رفض الخدمة الموزعة(DDoS)، خوارزميات الذكاء الأصطناعي وبروتوكولات التشفير خفيفة الوزن ، الحوسبة السحابية.

1-6-2 دراسة Borgohain) وآخرون، 2015) بعنوان استطلاع حول قضايا الأمن والخصوصية لإنترنت الأشياء

قامت هذه الدراسة بإستعراض شامل لمخاطر الأمان والخصوصية التي تواجه إنترنت الأشياء، كما أستعرضت التهديدات والمخاطر. وأشارت الدراسة أيضًا إلى مجموعة من التحديات التي تُواجه معالجة هذه المخاطر، تشمل:

- وعي المستخدم والمطور المنخفض: عدم إدراك المستخدمين والمطورين لمخاطر الأمان والخصوصية.
- موارد الأجهزة المحدودة: تُصعّب تنفيذ حلول أمان شاملة على الأجهزة ذات الإمكانيات المحدودة.
- عدم تجانس النظام: يُصعّب تطوير حلول أمان فعالة لجميع أنظمة إنترنت الأشياء المتنوعة.

3-6-1 دراسة (García وأخرون , 2018) بعنوان مراجعة الذكاء الاصطناعي في إنترنت الأشياء.

أستعرضت هذه الدراسة التطورات الحديثة في الذكاء الاصطناعي وإنترنت الأشياء، وناقشت التحديات في هذا المجال، حيث عرّف المؤلفون الذكاء الاصطناعي بأنه "قدرة الآلة على أداء المهام المعرفية التي تتطلب عادةً ذكاءً بشرياً" وإنترنت الأشياء على أنه "شبكة من الأشياء المادية المضمنة بأجهزة استشعار وبرامج وتقنيات أخرى بغرض ربط البيانات وتبادلها مع الأجهزة والأنظمة الأخرى عبر الإنترنت." . ثم تستمر الورقة في مناقشة مجموعة متنوعة من التطورات الحديثة في الذكاء الاصطناعي وإنترنت الأشياء، بما في ذلك:

- التعلم العميق: نوع من التعلم الآلي الذي يستخدم الشبكات العصبية الاصطناعية للتعلم من البيانات، حيث تم استخدام التعلم العميق لتطوير مجموعة متنوعة من تطبيقات الذكاء الاصطناعي في إنترنت الأشياء، مثل التعرف على الصور، ومعالجة اللغة الطبيعية.
- حوسبة الحافة: نموذج حوسبة موزع يجعل الحساب وتخزين البيانات أقرب إلى الأجهزة التي يتم فيها إنشاء البيانات حيث يمكنه من تقليل زمن الوصول وتحسين الأداء.
- حوسبة الضباب: نموذج حوسبة موزع يوفر طبقة من الحوسبة وتخزين البيانات بين حافة الشبكة والسحابة، يمكن أن يوفر موارد إضافية لمعالجة البيانات وتخزينها.

تختتم الدراسة بمناقشة التحديات في تقنيتي الذكاء الاصطناعي وإنترنت الأشياء، منها الحاجة إلى المزيد من البيانات لتدريب خوارزميات الذكاء الاصطناعي والحاجة إلى تطوير معايير جديدة لقابلية التشغيل البيني لإنظمة أنترنت الأشياء.

4-6-1 دراسة(Azrour وآخرون، 2021) بعنوان أمن إنترنت الأشياء: التحديات والقضايا الرئيسية

قامت هذه الدراسة بتسليط الضوء على القضايا والتحديات الأمنية التي تواجه أنظمة إنترنت الأشياء وهي:

- الذاكرة المحدودة : قدرة معالجة محدودة تُعيق تنفيذ حلول أمانية فعّالة.
- الاعتماد على الأسرار المشتركة: مخاطر مشاركة كلمات السر بين الأجهزة المتصلة.
- هجمات رفض الخدمة: إغراق الأجهزة بحركة المرور لمنعها من العمل.
- هجمات إعادة التشغيل : سرقة البيانات وإعادة تشغيلها لاحقًا للوصول غير المصرح به.
- هجمات تخمين كلمة المرور: محاولة تخمين كلمات المرور للوصول إلى الأنظمة.
- هجمات الإنتحال: إنتحال شخصية المستخدمين الشرعيين للوصول إلى البيانات.

وأستخلصت الدراسة إلى أن أمن إنترنت الأشياء يعتبر تقنية معقدة ولكن يمكن التخفيف من مخاطرها من خلال نشر حلول أمنية مخصصة و تثقيف المستخدمين والمطورين حول المخاطر الأمنية.

5-6-1 دراسة (Kah Phooi Seng,2022)الذكاء الاصطناعي إنترنت الأشياء: نموذج جديد لشبكات الاستشعار الموزعة

تقدم هذه الدراسة نظرة شاملة عن التحديات والفرص المتاحة في مجال إنترنت الأشياء الذكي. ركزت هذه الدراسة على تقارب تقنيات الاستشعار، الأجهزة ، والطاقة من أجل إنترنت الأشياء الذكي (AIoT). ، كيفية دمج تقنيات الذكاء الاصطناعي مع تقنيات إنترنت الأشياء لتحسين كفاءة وفعالية الأنظمة. تناولت الدراسة عدة محاور رئيسية وهي كالتالي:

- تقارب الاستشعار والحوسبة والإدارة: بحثت الدراسة في كيفية تحسين كفاءة استهلاك الطاقة في أجهزة الاستشعار من خلال تقنيات الضغط الحسي (Compressive sensing) وتقنيات التعلم العميق. كما ناقشت أهمية الحوسبة الحدية (Edge computing) وإدارة الأجهزة المتعددة بشكل فعال.
- نقل الطاقة اللاسلكي: بحثت الدراسة في تقنيات نقل الطاقة اللاسلكي بين الأجهزة لتحسين عمر البطارية في أجهزة إنترنت الأشياء ، كما ناقشت تحديات الأمان في مجال نقل الطاقة اللاسلكي.
- تقارب الاتصالات والشبكات: بحثت الدراسة في أهمية تقنيات الذكاء الاصطناعي في تحسين أداء شبكات إنترنت الأشياء، مثل تقنيات التعلم المعزز لتحسين جدولة الموارد وتقنيات التعلم العميق لتحسين كشف التداخل و تقنيات الشبكات الافتراضية (SDN) في إدارة شبكات إنترنت الأشياء الذكية.

6-6-1 دراسة (Alheadary ,Wael G, 2024) بعنوان تأثيرات إنترنت الأشياء والذكاء الاصطناعي على الخدمات اللوجستية في إدارة سلسلة التوريد

ناقشت هذه الدراسة تأثيرات إنترنت الأشياء والذكاء الاصطناعي على اللوجستيات في إدارة سلسلة التوريد من خلال دمج إنترنت الأشياء والذكاء الاصطناعي في إدارة سلسلة التوريد. أقترحت الدراسة إطارًا جديدًا يستخدم أجهزة استشعار إنترنت الأشياء لجمع البيانات ويستخدم الذكاء الاصطناعي لتحليل البيانات لمساعدة المؤسسات على إعادة تصور إدارة سلسلة التوريد واللوجستيات الخاصة، يتكون الإطار من خمس مراحل:

- استخدام أجهزة استشعار إنترنت الأشياء وأجهزتها : تتصل أجهزة إنترنت الأشياء ببوابة أو جهاز حافة يمكن من خلاله مشاركة بيانات الاستشعار التي تجمعها ؛ تجد هذه البيانات طريقها إلى السحابة لتحليلها أو تحليلها محليًا بواسطة البوابة.
- تحليل البيانات باستخدام الذكاء الاصطناعي: يتم استخدام الذكاء الاصطناعي لتحليل البيانات التي تم جمعها من أجهزة استشعار إنترنت الأشياء للتنبؤ بالمخاطر واتخاذ القرارات وتحسين الكفاءة .
- اتخاذ القرارات: يتم استخدام نتائج تحليل البيانات لاتخاذ القرارات بشأن إدارة سلسلة التوريد

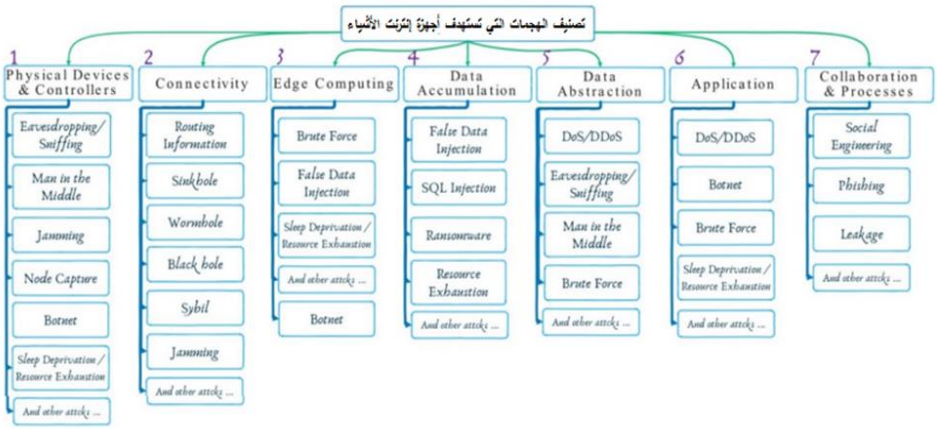
واللوجستيات

- التنفيذ: يتم تنفيذ القرارات المتخذة في المرحلة السابقة. قد يتضمن ذلك تغيير العمليات أو الأنظمة.
- التقييم: يتم تقييم تأثير القرارات المتخذة على أداء سلسلة التوريد، يمكن استخدام هذه المعلومات لتحسين الإطار في المستقبل.

2- المحور الأول

2-1 التهديدات والمخاطر التي تواجه أنترنت الأشياء

يمكن أعتبار حماية أنظمة أنترنت الأشياء قضية رئيسية في مجال تكنولوجيا المعلومات ، إلا أنها لا تزال تحظى باهتمام أقل مقارنة بالأنظمة التقليدية، يعود ذلك جزئيًا إلى حداثة هذه التقنية وتنوع الأجهزة والكائنات المتصلة بها، مما يجعل وضع معايير أمنية موحدة أمرًا صعبًا.لاسيما أن إنترنت الأشياء يمثل نظامًا بيئيًا فريدًا يتميز بتنوع الأجهزة والكائنات وارتفاع مستوى الترابط، مما يجعله عرضة لأنواع جديدة ومتطورة من التهديدات والتحديات.على سبيل المثال عدم تأمين أجهزة إنترنت الأشياء بشكل كافٍ يمكن أن يؤدي إلى انتهاكات للخصوصية وتعطيل الخدمات وخسائر مالية كبيرة. الشكل رقم (1) يوضح أبرز الهجمات التي تستهدف أجهزة إنترنت الأشياء (Harith,2023).



الشكل (1) أبرز الهجمات التي تستهدف أجهزة إنترنت الأشياء

2-1-1 هجمات البرامج الضارة Malware attacks

أي نوع من البرامج الضارة المصممة لإحداث ضرر لجهاز الكمبيوتر أو الخادم أو العميل أو شبكة الكمبيوتر أو البنية التحتية وتُعتبر أجهزة إنترنت الأشياء عرضة لمجموعة متنوعة من هجمات البرامج الضارة، نظرًا لطبيعتها المتصلة وسهولة اختراقها نسبيًا، يمكن أن يكون لهذه الهجمات تأثير كبير على المؤسسات ، بما في ذلك (Evans, 2011):

- تعطيل البنية التحتية الحيوية: يمكن استخدام البرامج الضارة للسيطرة على أجهزة إنترنت الأشياء المستخدمة في البنية التحتية الحيوية، مثل أنظمة الطاقة والنقل، مما يتسبب في انقطاعات واسعة النطاق.
- سرقة البيانات الحساسة : يمكن استهداف أجهزة إنترنت الأشياء لجمع البيانات الشخصية أو المالية الحساسة، مثل معلومات بطاقات الائتمان.
- الإضرار بالسمعة : يمكن استخدام هجمات البرامج الضارة لتشويه سمعة الأفراد أو المؤسسات من خلال نشر معلومات مضللة.

وأشار (Singh et al, 2014) إلى أن هجمات البرامج الضارة على أنترنت الأشياء عادة ما تكون بسبب:

- نقص الأمان: غالبًا ما تكون أجهزة أنترنت الأشياء غير آمنة بشكل افتراضي، مع كلمات مرور ضعيفة وبرامج ثانوية قابلة للاختراق .
- الافتقار إلى المصادقة والترخيص: قد لا تتطلب أجهزة أنترنت الأشياء مصادقة قوية أو ترخيصًا للوصول إلى الشبكات، مما يجعلها سهلة الاستهداف من قبل المتسللين .
- نقص التحديثات: قد لا يتم تحديث برامج أجهزة أنترنت الأشياء بإنتظام، مما يترتب عليه ثغرات أمنية يمكن للمتسللين والمهاجمين استغلالها .

2-1-2 هجمات حجب الخدمة (DoS) Distributed Denial of Service Attacks

يمكن وصف هجمات رفض الخدمة (DoS/DDoS) بأنها هجمات إلكترونية تهدف إلى تعطيل خدمة معينة عن عمد، مما يمنع المستخدمين الشرعيين من الوصول إليها . يتم تنفيذ هذه الهجمات عادةً عن طريق إغراق الجهاز المستهدف، غالبًا ما يكون خادمًا، بحجم هائل من البيانات أو الطلبات. هذه البيانات تُرسَل من شبكة واسعة من الأجهزة المصابة، والتي تعرف باسم " الروبوتات". وتُصنف هجمات رفض الخدمة بشكل عام إلى نوعين رئيسيين (2019، وأخرون، Koroniotis):

- **الهجمات الحجمية: Volumetric Attacks** تهدف إلى تجاوز قدرة الجهاز المستهدف على التعامل مع حجم البيانات الهائل المرسل إليه. هذا الحجم الزائد من البيانات يؤدي إلى إبطاء الخدمة أو تعطيلها بشكل كامل.

- **الهجمات القائمة على البروتوكول: Protocol-based attacks** تستغل نقاط ضعف في بروتوكولات الاتصال المستخدمة، مثل بروتوكول TCP/IP .هذه الهجمات تهدف إلى استنفاد موارد الجهاز المستهدف، مثل وحدة المعالجة المركزية أو الذاكرة، مما يجعله غير قادر على الاستجابة للطلبات الشرعية.

تهدد هجمات حجب الخدمة(Rehman, 2021) أجهزة إنترنت الأشياء بإغراقها بحركة المرور أو استهلاك مواردها، مما يعطل الخدمات ويسبب خسائر مالية. وأشارت دراسة أجراها (gh et al Sin ,2014) الى أن هجمات حجب الخدمة ناجمة عن زيادة تعقيد البنية التحتية لأنظمة أنترنت الأشياء وانتشار الأجهزة المتصلة بشبكة الإنترنت. كما أكدت كلا الدراستين الى أن هجمات حجب الخدمة على أنظمة أنترنت الأشياء تكون بسبب أن أجهزة أنترنت الأشياء عادة تكون غير آمنة بشكل افتراضي مع كلمات مرور ضعيفة وكذلك الافتقار إلى مراقبة هذه الأجهزة بشكل فعال، مما يجعل من السهل على المهاجمين اختراقها والاستيلاء عليها. وقد جاء في دراسة أخرى قام بها (Rehman et al., 2023) ، الى أنه يمكن أن يكون لهجمات حجب الخدمة على أنظمة أنترنت الأشياء تأثير سلبي بما في ذلك:

- انقطاع الخدمة الخدمات الأساسية، مثل خدمات الطاقة والنقل والرعاية الصحية.
- يمكن أن تتسبب في خسائر مالية ضخمة للأعمال والشركات بسبب توقف الخدمات.
- يمكن أن تُستخدم لتعطيل الأنظمة الحيوية، أنظمة السلامة في المصانع أو المرافق الحيوية أو النووية.

3-1-2 اختراق البيانات Data Breach

جاء في دراسة (2019، وأخرون، Koroniotis) أن مجموعة من الهجمات التي يسعى فيها المهاجم إلى اختراق أمن جهاز ما وبالتالي الحصول على حق الوصول غير المصرح به إلى البيانات، وبالتالي يستطيع هذا الجهاز المهاجم البعيد الحصول على بيانات حساسة. عادةً ما يستخدم المهاجمون منهجية التهديد المستمر المتقدم (APT) بالتزامن مع هجمات سرقة المعلومات، لزيادة كفاءة هجماتهم.

ويُعتبر خرق البيانات تهديدًا خطيرًا لأجهزة إنترنت الأشياء ويمكن أن تُؤدي خروقات البيانات إلى كشف معلومات سرية، أو خاصة، أو محمية، أو حساسة، مما قد يُسبب ضررًا كبيرًا للأفراد والشركات، وقد أظهرت عدة دراسات منها (Vojković et al., 2020) و (Obaidat et al., 2022) الى أن أجهزة إنترنت الأشياء عرضة بشكل خاص لخرق البيانات بسبب:

- نقص الأمان: تكون أجهزة إنترنت الأشياء غير آمنة بشكل افتراضي.
- قد لا يتم تحديث برامج أجهزة إنترنت الأشياء بانتظام، مما يترك ثغرات أمنية يمكن استغلالها.
- الافتقار إلى الوعي: قد لا يكون المستخدمون على دراية بالمخاطر الأمنية المرتبطة بأجهزة إنترنت الأشياء،

ولا يتخذون الخطوات اللازمة لحمايتها، ويمكن أن يكون لخرق البيانات على أجهزة إنترنت الأشياء عواقب وخيمة، بما في ذلك:

- يمكن للمهاجمين استخدام البيانات المسروقة من أجهزة إنترنت الأشياء لسرقة هوية الأفراد، وارتكاب الاحتيال المالي لسرقة الأموال من الحسابات المصرفية أو بطاقات الائتمان. ويمكن استخدام البيانات الشخصية المسروقة من أجهزة إنترنت الأشياء لتشويه سمعة الأفراد أو الشركات.
- يمكن استخدام أجهزة إنترنت الأشياء المخترقة لشن هجمات مثل هجمات حجب الخدمة مما يؤدي إلى تعطيل الخدمات الأساسية

2-1-4 انتهاك الخصوصية Violation Of Privacy

تُطرح أجهزة إنترنت الأشياء تحديات كبيرة حول الخصوصية والأمان، حيث تقوم بجمع ونقل كميات هائلة من البيانات الحساسة ، ,هناك بعض التحديات أشار اليها (Ogonji et al., 2020) :

- البيانات الضخمة: جمع كميات هائلة من البيانات الشخصية والبيئية .
- نقص الأمان: ثغرات أمنية يمكن للمهاجمين استغلالها .
- الافتقار إلى الشفافية: عدم وضوح كيفية جمع البيانات وأحتمالية استخدامها لمراقبة المستخدم.
- قلة التحكم: نقص تحكم المستخدم في بياناته .

2-1-5 نقص الوعي الأمني بين مستخدمي إنترنت الأشياء

تتطلب أجهزة إنترنت الأشياء أنظمة إدارة شاملة لمراقبة الأجهزة وتحديثها وتأمينها. بدون إدارة فعالة، يمكن أن تصبح أجهزة إنترنت الأشياء قديمة، مما يجعلها عرضة للتهديدات الأمنية الجديدة. وتشير الدراسات إلى أن الوعي الأمني المحدود لدى الأفراد والشركات العاملة في مجال إنترنت الأشياء يساهم بشكل كبير في زيادة المخاطر الأمنية المرتبطة بهذه الأجهزة. وأظهرت دراسة(Saqib, 2022) إن نقص الوعي الأمني يمثل تحديًا في مجال إنترنت الأشياء، خاصة في ظل تزايد إستخدام هذه الأجهزة وأظهرت الدراسة أن :

- 25% فقط من مستخدمي إنترنت الأشياء في مصر على دراية بمخاطر سرقة البيانات الشخصية أو استخدام أجهزتهم لشن هجمات برامج الفدية.
- 30% فقط من مستخدمي إنترنت الأشياء يعرفون كيفية حماية أجهزتهم.

كما يمكن أن يكون لنقص الوعي الأمني عواقب وخيمة (Koohang et al., 2022).، مثل:

- استخدام أجهزة إنترنت الأشياء لشن هجمات برامج الفدية.
- انتهاكات البيانات. سرقة معلومات بطاقات الائتمان.

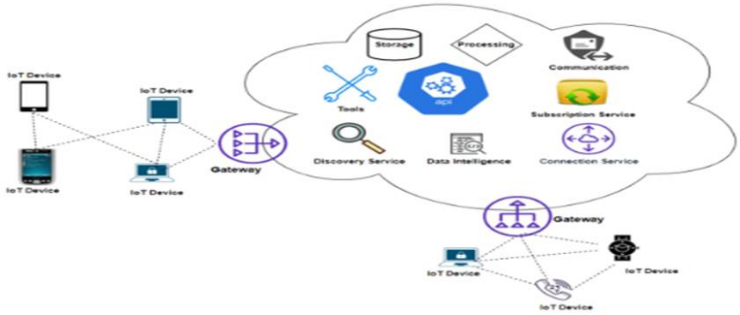
2-2 التحديات التي تواجه انترنت الاشياء

2-2-1 الموارد المحدودة Limited Resources

تُعتبر الموارد المحدودة لأجهزة إنترنت الأشياء مثل قوة المعالجة المحدودة والذاكرة المحدودة وسعة التخزين المحدودة وعمر البطارية المحدود، أحد أهم التحديات الأمنية التي تواجه هذه التقنية. قامت دراسة Sadhu et al. 2022)) بالبحث في هذه التحديات وحددت حلولًا محتملة، وتوصلت الى ما يلي:

- تُشكل الموارد المحدودة تحديًا أمنيًا كبيرًا لأجهزة إنترنت الأشياء.
- تشمل الحلول المحتملة تطوير حلول أمنية خفيفة الوزن واستخدام خدمات الأمان السحابية واستخدام الذكاء الاصطناعي والتعلم الآلي.

وجاء أيضاً في دراسة أخرى أجراها (Alam,2021) إلى أن منصات أنترنت الأشياء المستندة إلى السحابة يمكن أن تُقلل من العبء الأمني على الأجهزة محدودة الموارد، حيث تعتمد هذه المنصات على الموارد والخدمات السحابية لجمع البيانات ونقلها وتحليلها ومعالجتها وتخزينها، مما يقلل من الحاجة إلى قدرات معالجة قوية على الأجهزة نفسها. ويوضح الشكل رقم (2) نموذجًا لمنصة إنترنت الأشياء المستندة إلى السحابة لتطوير التطبيقات.



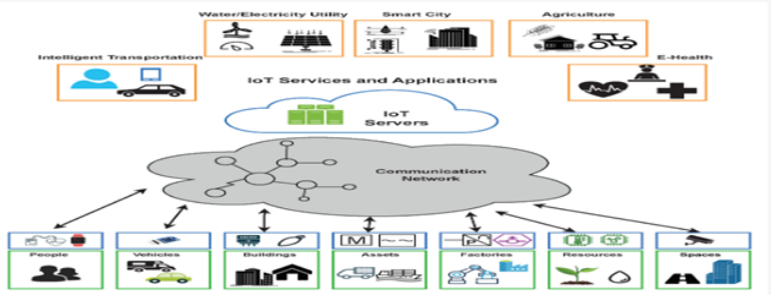
الشكل رقم (2) منصة إنترنت الأشياء المستندة إلى السحابة لتطوير التطبيقات.

2-2-2 عدم تجانس أنظمة إنترنت الأشياء Heterogeneity Of IoT Systems

ترتبط مليارات الأشياء والأجهزة بالإنترنت، هذه الأجهزة المتصلة غير متجانسة ولديهم معايير وتقنيات مختلفة تتواصل من خلال بروتوكولات مختلفة. يُعد التنوع الكبير في أنظمة إنترنت الأشياء عائقًا أمام التكامل والتشغيل السلس بين الأجهزة المختلفة. وعلى الرغم من ذلك، فإن هذا التنوع يفتح آفاقًا واسعة للابتكار وتطوير تطبيقات جديدة ومبتكرة. وقد أكدت دراسة أجراها (Razzaque وأخرون , 2015) على هذه التحديات، حيث أبرزت النتائج التالية:

- يُشكل عدم التجانس تحديًا كبيرًا لإنترنت الأشياء.
- التقييس ضروري لجعل أنظمة إنترنت الأشياء أكثر قابلية للتشغيل البيني.
- استخدام التجريد لإخفاء تعقيد أنظمة إنترنت الأشياء غير المتجانسة عن المستخدمين والمطورين.
- يمكن استخدام المحاكاة الافتراضية لإنشاء بيئات معزولة لأنظمة إنترنت الأشياء غير المتجانسة، مما قد يحسن أداء الأمان.

وجاء في دراسة أخرى حول عدم تجانس إنترنت الأشياء (Zafar وآخرون، 2023) إلى أنّه على الرغم من كونه تحديًا، إلا أنه سمة أساسية لإنترنت الأشياء تُتيح فرصًا للابتكار.واقترحت الدراسة حلولًا مشابهة لتلك التي اقترحها (Razzaque وآخرون , 2015) مع التركيز بشكل خاص على إمكانية استخدام التجريد والمحاكاة الافتراضية لإنشاء تطبيقات جديدة ومبتكرة. ويوضح الشكل رقم (3) نموذجًا مجردًا أساسيًا لإنترنت الأشياء.



الشكل (3) النموذج التجريدي الأساسي لإنترنت الأشياء

3-2-2 تعقيد أنظمة إنترنت الأشياء Complexity Of IoT Systems

تتطلب الشبكات الضخمة والمعقدة لنظام اتصالات أنترنت الأشياء مستوى كبيرًا من استهلاك الطاقة، مما يجعل من الصعب الحفاظ على اتصالات إنترنت الأشياء وعمليات النقل في الوقت الفعلي. وإن التعقيد المتزايد لأنظمة إنترنت الأشياء، والذي تم توثيقه في دراسات سابقة يؤدي إلى عواقب وخيمة على مستوى انتشار هذه التقنية وتبنها على نطاق واسع. ووفقًا لما جاء في دراسة أجراها كلاً من :

(Hassan وآخرون , 2020) و(Park وأخرون,2017) فإن هذا التعقيد ناتج عن عدد من العوامل:

- عدم التجانس: تنوع بروتوكولات الاتصال ومعايير البيانات والأجهزة والشركات المصنعة.
- الحجم: النطاق الهائل لأنظمة إنترنت الأشياء، والتي تتضمن مليارات الأجهزة المترابطة.
- الديناميكية: التغيرات المستمرة في أنظمة إنترنت الأشياء، مثل إضافة أو إزالة أجهزة وتحديث البرامج.
- الأمن: القضايا الأمنية المرتبطة بأنظمة إنترنت الأشياء.
- نقص المعايير: قلة المعايير الموحدة لتصميم وتطوير أنظمة إنترنت الأشياء.

3-المحور الثاني الذكاء الاصطناعي وأهميته

يتميز الذكاء الاصطناعي بقدرته على اتخاذ قرارات منطقية وعقلانية، مدفوعاً بكميات هائلة من البيانات وتحليلات معقدة. وبحسب دراسة أجراها (G Yashodha et al, 2021)، يمكن للذكاء الاصطناعي في العديد من الحالات، تجاوز القدرات البشرية في اتخاذ القرارات الدقيقة والسريعة، مع تقليل نسبة الأخطاء إلى حد كبير. بالإضافة إلى ذلك، لا يتأثر الذكاء الاصطناعي بالعوامل العاطفية والتعب، مما يجعله أداة قوية في مجالات تتطلب استجابة سريعة ودقيقة. في هذا السياق، يعتبر الذكاء الاصطناعي ركيزة أساسية لتعزيز الأمن والكفاءة في أنظمة إنترنت الأشياء ؛ حيث أشار موقع IBM الى تزايد عدد الأجهزة المتصلة بالإنترنت وتنوع البيانات التي يتم جمعها، بالتالي أصبح من الضروري الاعتماد على أدوات ذكية لتحليل هذه البيانات واستخلاص المعلومات ، كما أن الذكاء الاصطناعي يمكن أن يساهم في اكتشاف التهديدات الأمنية المحتملة والتصدي لها بشكل فوري، مما يحمي أنظمة أنترنت الأشياء من الهجمات السيبرانية.

وشهدت السنوات الأخيرة تطوراً ملحوظاً في مجال إنترنت الأشياء، مدفوعاً بالتقدم الهائل في أجهزة الاستشعار، ومعالجة البيانات، وتقنيات الاتصالات. هذا التطور أدى إلى انتشار مليارات الأجهزة المتصلة بالإنترنت، مما أوجد بيئة غنية بالبيانات تتطلب حلولاً ذكية لإدارتها وتحليلها. بالمقابل فإن دمج الذكاء الاصطناعي مع إنترنت الأشياء يمثل نقلة نوعية، حيث يمكن للذكاء الاصطناعي أن يمنح الأجهزة المتصلة القدرة على التعلم من البيانات واتخاذ القرارات بشكل مستقل والتكيف مع المتغيرات البيئية. يُطلق على هذا التكامل "إنترنت الأشياء بالذكاء الاصطناعي (AIoT)." . (2022, Seng KP) ويمكن تلخيص هذا التكامل في أربعة جوانب رئيسية والشكل رقم (4) يوضح بنية AIoT :.

- البنى والتقنيات: دمج الذكاء الاصطناعي والحوسبة المتقدمة لتوفير بنية تحتية قوية لـ AIoT.
- أجهزة الاستشعار: استخدام أجهزة استشعار ذكية قادرة على جمع وتحليل البيانات بفعالية.
- الاتصالات: تطوير شبكات اتصالات عالية السرعة وكفاءة لدعم تطبيقات AIoT.
- التطبيقات: تطوير تطبيقات متنوعة تستفيد من قدرات الذكاء الاصطناعي لتحسين مختلف المجالات.

الشكل رقم (4) يوضح بنية AIoT

3-1 أدوات الأمن السيبراني المدعومة بالذكاء الاصطناعي

يشير موقع ميكروسوفت الى أن الذكاء الإصطناعي يمثل ثورة في مجال الأمن السيبراني، حيث يمكّن الأنظمة من التعلم من البيانات وتحليلها بشكل أسرع وأكثر دقة من البشر. يتم استخدام الذكاء الاصطناعي في مجموعة متنوعة من أدوات الأمن السيبراني، بما في ذلك :

- جدران الحماية من الجيل التالي: تتجاوز هذه الجدران التقليدية بفضل الذكاء الاصطناعي الذي يمكنها من اكتشاف تهديدات جديدة ومعقدة، مثل الهجمات المستهدفة التي تستهدف نقاط ضعف محددة في الأنظمة.
- حلول أمان نقاط النهاية: تساعد هذه الحلول على حماية الأجهزة الفردية، مثل أجهزة الكمبيوتر المحمولة والهواتف الذكية، من التهديدات. يستخدم الذكاء الاصطناعي لتحليل سلوك الجهاز والكشف عن أي أنشطة غير طبيعية، مثل محاولات الوصول غير المصرح بها أو تنزيل برامج ضارة.
- أنظمة كشف ومنع التطفل على الشبكة: تقوم هذه الأنظمة بمراقبة حركة المرور الشبكية للكشف عن الهجمات. يستخدم الذكاء الاصطناعي لتحليل كميات هائلة من البيانات في الوقت الفعلي، مما يسمح بالكشف عن التهديدات في مراحلها المبكرة.
- حلول الأمن السحابي: مع تزايد اعتماد المؤسسات على السحابة، أصبح تأمين البيانات في السحابة أمرًا بالغ الأهمية. يساعد الذكاء الاصطناعي في حماية البيانات السحابية من خلال تحليل حركة المرور السحابية والكشف عن أي تهديدات محتملة.
- أجهزة إنترنت الأشياء: مع انتشار أجهزة إنترنت الأشياء، أصبح تأمين هذه الأجهزة أمرًا ضروريًا. يستخدم الذكاء الاصطناعي لتحليل البيانات التي يتم جمعها من هذه الأجهزة والكشف عن أي أنماط غير طبيعية تشير إلى وجود تهديد.

3-2 أنظمة إنترنت الأشياء المدعومة بالذكاء الاصطناعي

3-2-1 تحليل البيانات و التنبؤ

يمتلك الذكاء الاصطناعي القدرة على تحليل كميات هائلة من البيانات التي تولّدها أجهزة إنترنت الأشياء، وذلك بكفاءة ودقة تفوق القدرات البشرية من خلال تطبيق تقنيات مثل التعلم الآلي والشبكات العصبية، ويمكنه أيضاً التنبؤ بالتهديدات واكتشاف الأنماط الشاذة والتهديدات المحتملة في البيانات بسهولة وسرعة .

أظهرت دراسة حديثة أجراها (Binhammad و أخرون , 2024) أن الذكاء الاصطناعي، وبالأخص تقنيات التعلم الآلي، قد مكّنت الأنظمة من تحليل كميات هائلة من البيانات بسرعة ودقة عاليتين؛ هذا الأمر ساهم بشكل كبير في الكشف المبكر عن التهديدات المحتملة مما سمح لخبراء الأمن بالأستجابة بشكل أسرع وأكثر فعالية ، لذلك

فإن قدرة الذكاء الاصطناعي على التنبؤ بالتهديدات المستقبلية تمثل قفزة نوعية في مجال الأمن السيبراني وذلك بفضل التقدم المذهل في قوة الحوسبة الذي أدى إلى ظهور تقنيات متقدمة مثل التعلم العميق والشبكات العصبية. وأشارت الدراسة أيضاً الى أنه تم دمج الذكاء الاصطناعي في نماذج الأمن السيبراني للكشف عن عمليات التطفل على الشبكة والبرامج الضارة والثغرات الأمنية. تسمح خوارزميات التعلم الآلي بمعالجة كميات هائلة من البيانات وتحديد التهديدات الأمنية المحتملة في وقت مبكر، وتقوم هذه الخوارزميات بإجراء تحليل تنبؤي مما يسمح لخبراء الأمن بتوقع الخروقات الأمنية وتجنبها قبل حدوثها.

وأظهرت دراسة أخرى أجراها(Alheadary , Wael G2024.) أن دمج الذكاء الاصطناعي مع أجهزة إنترنت الأشياء مثل GPS وRFID وأجهزة الاستشعار يمثل نقلة نوعية في مجال أمن سلسلة التوريد؛ وذلك من خلال تحليل البيانات الضخمة التي تجمعها هذه الأجهزة ، والذي يُمكن الذكاء الاصطناعي من إكتشاف أي انحرافات عن المسار الطبيعي لسلسلة التوريد، مما يتيح الكشف المبكر عن تهديدات محتملة مثل التزوير، السرقة أو التخريب، وبالتالي يمكن للمؤسسلت تقليل الخسائر المالية وتحسين سمعتها.علاوة على ذلك، فإن الذكاء الأصطناعي يتيح اتخاذ إجراءات استباقية لمنع وقوع الحوادث مما يعزز مرونة سلسلة التوريد وقدرتها على مواجهة التحديات .

وجاء في دراسة (Meneghello , 2019)، أن الذكاء الاصطناعي وإنترنت الأشياء يوفرا إطارًا شاملاً لتحسين عمليات إدارة سلسلة التوريد وجعلها أكثر مرونة وأمانًا ، وأن الجمع بين إنترنت الأشياء والذكاء الاصطناعي يمثل تقنية قوية يمكن أن تساعد المؤسسات على تحسين عملياتها وتطوير منتجاتها. في هذا السياق نجد أن إنترنت الأشياء يمكن أن تجمع كميات هائلة من البيانات حول العمليات التشغيلية، أو أي عمليات أخرى ولكن تحليل هذه البيانات واستخراج قيمة منها، يتطلب الذكاء الاصطناعي؛ على سبيل المثال، يمكن لأجهزة استشعار إنترنت الأشياء المثبتة في المصانع مراقبة خط إنتاج ، ولكن الذكاء الاصطناعي هو الذي يحلل بيانات الاستشعار ويتنبئ بالمشاكل المحتملة وأتخاذ الإجراءات الوقائية ، والذي سيؤدي إلى تقليل وقت التعطل وتحسين الإنتاجية. كما يمكن للذكاء الاصطناعي تحليل بيانات إنترنت الأشياء لفهم احتياجات العملاء بشكل أفضل وتطوير منتجات وخدمات تلبي تلك الاحتياجات.

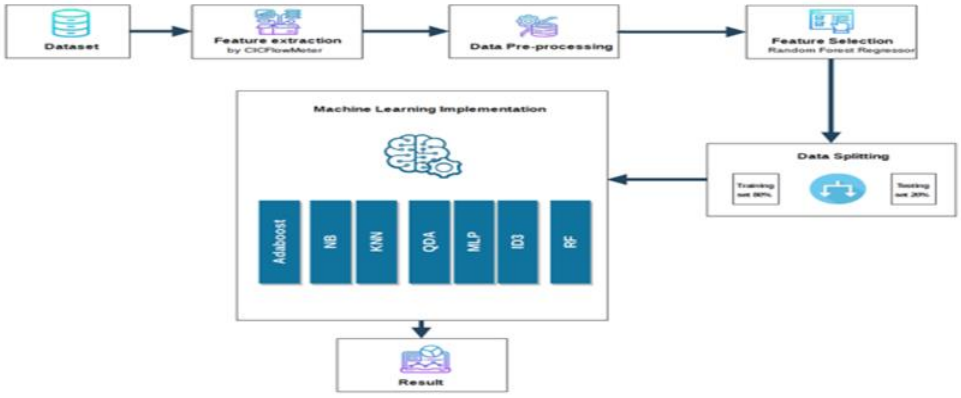
من خلال التعاريف السابقة نجد أن الذكاء الأصطناعي هو مجال من من التكنولوجيا يهدف الى تصميم أنظمة قادرة على تنفيد مهام تتطلب الذكاء البشري مثل التعلم من البيانات وأتخاذ القرارات وحل المشاكل المعقدة ، يعتمد الذكاء الاصطناعي على مجموعة متنوعة من التقنيات منها تقنية التعلم الآلي والتي تتيح لأنظمة أنترنت الأشياء تعلم كيفية أداء المهام دون الحاجة إلى برمجة صريحة لكل مهمة.

وتعتبر تقنيات التعلم الآلي حجر الزاوية في مجال أمن الشبكات الحديث، حيث تساهم بشكل كبير في تحسين قدرات المؤسسات على اكتشاف الهجمات الإلكترونية وتقليل المخاطر الأمنية. يعتمد مبدأ عمل التعلم الآلي في هذا المجال على تحليل كميات هائلة من البيانات المتعلقة بحركة الشبكات، وتحديد الأنماط السلوكية الطبيعية

والشاذة . وأشارت دراسة قام بها (Alsubhi , ,Alsamiri 2019) الى أنه توجد طريقتان رئيسيتان لتطبيق التعلم الآلي في اكتشاف الهجمات:

- التحليل القائم على التوقيع: يعتمد على تحديد أنماط حركة مرور معروفة مرتبطة بهجمات محددة، مثل هجمات حجب الخدمة أو هجمات الاستطلاع. يتم إنشاء "توقيعات" لهذه الأنماط، وعندما يتم اكتشاف تطابق بين حركة المرور الحالية والتوقيعات، يتم اعتبار ذلك مؤشرًا على حدوث هجوم.
- التحليل القائم على الشذوذ: يهدف إلى تحديد أي انحرافات عن السلوك الطبيعي لحركة الشبكة. يتم تدريب نماذج التعلم الآلي على بيانات تمثل السلوك الطبيعي، ثم تستخدم للكشف عن أي أنماط شاذة قد تشير إلى وجود هجوم.

وقد أجرت الدراسة تقييماً شاملاً لأداء خوارزميات التعلم الآلي في اكتشاف الهجمات على شبكات إنترنت الأشياء من خلال أقتراح نهج يستخدم مجموعة بيانات واسعة تحتوي على أنواع مختلفة من الهجمات تم تحديثها في مختبر نطاق الإنترنت في المركز الأسترالي للأمن السيبراني (ACCS)، بعد ذلك تم تطبيق أداة CICFlowMeter لأستخراج ميزات قائمة على تدفق حركة مرور البيانات ، ومن تم تطبيق سبعة خوارزميات للتعلم الآلي لتحليل هذه البيانات والشكل رقم (5) يقدم نظرة عامة على النهج المقترح.



الشكل رقم (5) نظرة عامة على النهج المقترح(Alsubhi , ,Alsamiri 2019)

أظهرت نتائج الدراسة الى أن خوارزمية الغابة العشوائية (Random Forest) قد حققت أداءً متميزًا في تحديد الميزات الهامة في البيانات، مما ساهم في تحسين دقة اكتشاف الهجمات، كما أوضحت الدراسة أن التعلم الآلي يمكن أن يكون أداة قوية في حماية شبكات إنترنت الأشياء من التهديدات المتزايدة. ولضمان أداء عالٍ لأنظمة الكشف عن التهديدات القائمة على التعلم الآلي، كان من الضروري اختيار الميزات المناسبة لحركة الشبكة. في هذه

الدراسة ، تم استخدام خوارزمية الغابة العشوائية (Random Forest) لحساب أهمية كل ميزة في البيانات، مما ساهم في تحديد الميزات الأكثر تأثيرًا على أداء النظام.

3-2-3 الأتمتة

عملية استبدال المهام المتكررة أو المعقدة التي يقوم بها البشر بآلات أو أنظمة تعمل بشكل آلي. أظهرت دراسات متعددة منها (G Yashodha et al, 2021) و(Rao K,Naganathan,2018) إلى أن الأتمتة هي استخدام التكنولوجيا لتنفيذ المهام بشكل أسرع وأكثر دقة وكفاءة، فبدلاً من قيام الإنسان بكتابة تقارير روتينية أو إدخال البيانات يدويًا ، يمكن لأجهزة الكمبيوتر القيام بذلك بشكل آلي. بالمقابل يلعب الذكاء الإصطناعي دوراً حاسماً في تطوير الأتمتة، حيث يمكّن الآلات من التعلم من البيانات واتخاذ القرارات بشكل مستقل. على سبيل المثال، يمكن للروبوتات التي تعمل بالذكاء الاصطناعي تجميع المنتجات في المصانع بدقة عالية وسرعة فائقة، ويمكن للسيارات ذاتية القيادة التنقل في المدن دون تدخل بشري. مستقبل الأتمتة واعد، حيث تتجه العديد من المجالات مثل الطب والتصنيع و الزراعة نحو تبني المزيد من الحلول الآلية.

4-2-3 إدارة أفضل للمخاطر

يستطيع الذكاء الاصطناعي جمع وتحليل كميات هائلة من البيانات التي تولّدها أجهزة إنترنت الأشياء في الوقت الفعلي، وهذا بدوره يتيح تحديد المخاطر المحتملة وتوقعها وأتخاذ قرارات أكثر دقة وسرعة . وتساعد أنظمة الاستجابة للحوادث القائمة على الذكاء الإصطناعي المؤسسات على اكتشاف المشاكل والتعامل معها في الوقت الفعلي؛ ويمكن أيضاً لهذه الأنظمة تحليل كميات هائلة من البيانات من مصادر مختلفة مثل حركة الشبكة والسجلات وأجهزة النهاية، وغيرها؛ كما أنها تتحكم في المشاكل الأمنية وتحدد أولوياتها بناءً على العواقب، ويمكن لهذه الأنظمة إكتشاف الحوادث في الوقت الفعلي والاستجابة بشكل استباقي لمنع التصعيد، ويمكن له أيضاً تحديد أنماط نقاط الضعف الإجرائية في الحوادث السابقة، مما يضمن عمليات استجابة لامركزية. (2024 , أخرون و Binhammad)

5-2-3 تحسين الكفاءة التشغيلية

دراسة أجراها (Alheadary , .Wael G2024) حول دمج إنترنت الأشياء والذكاء الاصطناعي في إدارة سلسلة التوريد. حيث تم تصميم نهج جديد يسمى IoT-AI-SCM لدمج هاتين التقنيتين في إدارة سلسلة التوريد. يتكون هذا النهج من ست خطوات رئيسية: استخدام أجهزة الاستشعار، جمع البيانات، تخزين البيانات، تطبيق الذكاء الاصطناعي وتحليل البيانات، والتخطيط الذكي. باختصار يمكن لهذا النهج أن يساعد المؤسسات على إعادة تصميم سلسلة التوريد الخاصة من خلال إستخدام الميزات الأساسية لإنترنت الأشياء والذكاء الاصطناعي ، على

سبيل المثال تحسين إدارة المخزون، تحسين الصيانة التنبؤية، مما يؤدي إلى زيادة الكفاءة التشغيلية وخفض التكاليف وتحقيق النجاح في نهاية المطاف. ويقدم الجدول رقم (1) فوائد دمج الذكاء الأصطناعي وأنترنت الاشياء لتحسين كفاءة التشغيل لأنظمة أنترنت الأشياء.

الجدول رقم (1) فوائد دمج الذكاء الأصطناعي وأنترنت الأشياء

مرتكز على	انترنت الأشياء و الذكاء الاصطناعي	الفائدة
تحسين الرؤية وتتبع البضائع	أجهزة استشعار إنترنت الأشياء وخوارزميات الذكاء الاصطناعي	معلومات في الوقت الفعلي عن الموقع ودرجة الحرارة وغيرها من الظروف
إدارة المخزون المُحسنة	تحليلات تنبؤية مدفوعة بالذكاء الاصطناعي	توقعات دقيقة للطلب، تقليل حالات نفاد المخزون، وتقليل المخزون الزائد
تحسين الخدمات اللوجستية والنقل	تحسين مسار قائم على الذكاء الاصطناعي وإدارة المركبات	كفاءة مُحسنة، تكاليف مُخفضة، وتجربة عملاء أفضل
إدارة المخاطر الاستباقية	اكتشاف الشذوذ والتعرف على الأنماط المدفوعة بالذكاء الاصطناعي	تحديد وتخفيف حالات تعطيل سلسلة التوريد المحتملة
زيادة مرونة سلسلة التوريد واستجابتها	دمج إنترنت الأشياء والذكاء الاصطناعي	اتخاذ قرارات أسرع، وقابلية أفضل للتكيف مع التغيرات في ظروف السوق

وأظهرت دراسة حديثة أجرتها (KAPSARC ,2024) أن الذكاء الاصطناعي يلعب دورًا حاسمًا في تحسين كفاءة النقل وتقليل أثره البيئي. من خلال تحليل كميات هائلة من البيانات المستمدة من أجهزة الاستشعار، يمكن للذكاء الاصطناعي اتخاذ قرارات ذكية لتحسين إدارة حركة المرور، وتخطيط المسارات، وتحسين سلوك القيادة. وذلك عن طريق :

- **إدارة حركة المرور الذكية:** التحكم الذكي في إشارات المرور وتنظيم تدفق المركبات لتقليل الازدحام.
- تحسين سلوك القيادة: تزويد السائقين بمعلومات حول عادات القيادة الخاصة بهم، مما يساعدهم على تقليل استهلاك الوقود.
- **تخطيط مسارات أكثر كفاءة:** باستخدام خوارزميات الذكاء الاصطناعي لتحديد أقصر الطرق وأكثرها كفاءة.
- **صيانة تنبؤية:** من خلال تحليل بيانات المركبات لتوقع الأعطال قبل حدوثها.

وأشارت الدراسة أيضاً الى أن الذكاء الاصطناعي سيمثل قفزة نوعية في قطاع النقل، حيث يساهم في بناء أنظمة نقل أكثر استدامة وكفاءة ، وهذا بدوره يؤدي بشكل مباشر إلى :

- **تقليل الانبعاثات:** يؤدي تحسين كفاءة الطاقة إلى خفض انبعاثات الغازات الدفيئة والتلوث.
- **زيادة السلامة:** يساعد الذكاء الاصطناعي في منع الحوادث من خلال مراقبة حالة المركبات والتنبؤ بالمخاطر.
- تحسين تجربة المستخدم: يوفر الذكاء الاصطناعي خدمات نقل أكثر ملاءمة وراحة للمستخدمين.

4-الأستنتاجات

خلصت هذه الورقة إلى ضرورة وضع أطر عمل تنظيمية شاملة لحماية أنظمة إنترنت الأشياء. يجب تعزيز أمن هذه الأنظمة من خلال اعتماد جدران حماية متعددة وتحديث دوري لمعلومات تسجيل الدخول الافتراضية. كما يجب تقسيم هذه الأنظمة إلى أقسام منفصلة لتقليل نقاط الضعف المحتملة وتشفير شبكات Wi-Fi بشكل قوي.

يمكن الاستفادة من الذكاء الاصطناعي بشكل كبير في تعزيز أمن أنظمة إنترنت الأشياء، وذلك من خلال استخدام خوارزميات التعلم الآلي لتحليل سلوك الأجهزة والشبكات والكشف عن أي انحرافات عن السلوك الطبيعي. يمكن تدريب هذه النماذج على التعرف على أنماط الهجمات المعروفة والجديدة، مما يسمح بأتمتة عمليات الاستجابة للحوادث الأمنية. بالإضافة إلى ذلك، يمكن استخدام الذكاء الاصطناعي للتحكم في أجهزة إنترنت الأشياء بشكل آلي للحد من انتشار التهديدات.

للحفاظ على خصوصية البيانات، يجب استخدام تقنيات التشفير التفاضلي لحماية البيانات أثناء تدريب

نماذج التعلم الآلي. كما يمكن استخدام الذكاء الاصطناعي للكشف عن أي تعديل غير مصرح به للبيانات التي يتم جمعها من أجهزة إنترنت الأشياء. يمكن أيضًا الاستفادة من الذكاء الاصطناعي للتنبؤ بفشل الأجهزة قبل حدوثه واتخاذ الإجراءات اللازمة، وتحسين كفاءة الطاقة في الأجهزة المتصلة، وتوفير تجربة مستخدم أكثر أمانًا وسهولة.

من الضروري التأكد من جودة البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي لضمان فعالية هذه النماذج في الكشف عن التهديدات وحماية الأنظمة

5-الخلاصة

يلعب الذكاء الاصطناعي دورًا هامًا في حماية بيئة إنترنت الأشياء من التهديدات الأمنية، حيث يقدم إمكانيات هائلة لتحسين الأمن السيبراني في إنترنت الأشياء. هدفت هذه الورقة إلى استكشاف دمج تقنيتي الذكاء الاصطناعي وإنترنت الأشياء لتحسين الأمن في بيئة إنترنت الأشياء ، وذلك بمناقشة المخاطر والتحديات الأمنية التي تواجه أنظمة إنترنت الأشياء، كما تم مناقشة كيفية استخدام تقنيات الذكاء الاصطناعي للتغلب على هذه التهديدات والتحديات. وأستخلصت هذه الدراسة إلى أن التعلم الآلي يمثل تقدمًا كبيرًا في مجال أمن الشبكات وخاصة شبكات أنترنت الأشياء، حيث يستطيع إكتشاف الهجمات بشكل أكثر فعالية وحماية الأنظمة من التهديدات المتطورة.. ويمكن للذكاء الاصطناعي أن يساهم بشكل كبير في تقليل التكاليف التشغيلية وتحسين الأداء والاستدامة. ومع ذلك، يجب معالجة التحديات المتعلقة بجودة البيانات والتكلفة والأمن لتحقيق أقصى استفادة من هذه التقنية.

ومع ذلك، فإن اختيار النهج الأمثل يعتمد على نوع البيانات المتاحة، الموارد الحسابية والهدف من نظام الكشف عن التهديدات. وختاماً، تحقيق أمن إنترنت الأشياء يتطلب نهجًا متعدد الجوانب يشمل التعاون بين الجهات المعنية، وضع أطر عمل تنظيمية شاملة لحماية أنظمة إنترنت الأشياء ، الحلول الأمنية المدعومة بالذكاء الاصطناعي ورفع مستوى الوعي لدى المستخدمين. نأمل أن تقدم هذه الورقة مساهمة قيمة وأن تساعد في تطوير حلول جديدة لتحسين الأمن والكفاءة في هذا المجال المتنامي.

6-المراجع

.1 Mouha, R. (2021) .Internet of Things (IoT). Journal of Data Analysis and Information Processing, 9, 77-101. doi: 10.4236/jdaip.2021.92006.

.2 Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

.3 Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The internet of things—Key applications and challenges. Journal of network and computer applications, 52, 22-35.

.4 Tomasik, Brian, (2016) : Artificial Intelligence And Its Implications For Future Suffering, Foundational Research Institute, U.S. https://longtermrisk.org/files/artificial-intelligence-and-its-implications-for-future-suffering.pdf

.5 Sadhu PK, Yanambaka VP, Abdelgawad A. Internet of Things: Security and Solutions Survey. Sensors (Basel). 2022 Sep 30;22(19):7433. doi: 10.3390/s22197433. PMID: 36236531; PMCID: PMC9571254.

.6 Alam, T. Cloud-Based IoT Applications and Their Roles in Smart Cities. Smart Cities 2021, 4, 1196-1219. https://doi.org/10.3390/smartcities4030064

.7 Xiao, Liang et al. "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" IEEE Signal Processing Magazine 35 (2018): 41-49.https://e-tarjome.com/storage/panel/fileuploads/2019-07-06/1562410880_E11424-e-tarjome.pdf.

.8 Razzaque, Mohammad Abdur & Milojevic, Marija & Palade, Andrei & Clarke, Siobhán. (2015). Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal. 3. 1-1. 10.1109/JIOT.2015.2498900.

.9 Zafar, A.; Samad, F.; Syed, H.J.; Ibrahim, A.O.; Alohaly, M.; Elsadig, M. An Advanced Strategy for Addressing Heterogeneity in SDN-IoT Networks for Ensuring QoS. Appl. Sci. 2023, 13, 7856. https://doi.org/10.3390/app13137856

.10 Hassan, R.; Qamar, F.; Hasan, M.K.; Aman, A.H.M.; Ahmed, A.S. Internet of Things and Its Applications: A Comprehensive Survey. Symmetry 2020, 12, 1674. https://doi.org/10.3390/sym12101674

.11 Park, K.; Park, J.; Lee, J. An IoT System for Remote Monitoring of Patients at Home. Appl. Sci. 2017, 7, 260. https://doi.org/10.3390/app7030260

.12 Køien, Geir & Abomhara, Mohamed. (2014). Security and privacy in the Internet of Things: Current status and open issues. 10.1109/PRISMS.2014.6970594.

.13 Borgohain, Tuhin & Kumar, Uday & Sanyal, Sugata. (2015). Survey of Security and Privacy Issues of Internet of Things. International Journal of Advanced Networking and Applications. 6. 2372-2378.

.14 González García, Cristian & Núñez Valdez, Edward & García Díaz, Vicente & Pelayo García-Bustelo, B. & Cueva Lovelle, Juan. (2018). A Review of Artificial Intelligence in the Internet of Things. International Journal of Interactive Multimedia and Artificial Intelligence. 5. 1. 10.9781/ijimai.2018.03.004.

.15 Mourade Azrour, Jamal Mabrouki, Azidine Guezzaz, Ambrina Kanwal, "Internet of Things Security: Challenges and Key Issues", Security and Communication Networks, vol. 2021, Article ID 5533843, 11 pages, 2021.

.16 Seng KP, And LM, Ngharamike E. Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks. International Journal of Distributed Sensor Networks. 2022.

.17 https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity

.18 Wael G. Alheadary (2024). The impacts of the internet of things and artificial intelligence on logistics in supply chain management. International Journal of Advanced and Applied Sciences, 11(1), Pages: 161-168

.19 Abdulkarim, Harith(2023). Review on machine learning and deep learning algorithms for IoT security. International Journal of Nonlinear Analysis and Applications, volume 14, number 5, pages: 27-35.

.20 Evans, D. (2011). The internet of things: How the next evolution of the internet is changing the world. Cisco Internet Business Solutions Group (IBSG).

.21 P Singh , M Mishra , P N Barwal (2014). Analysis of security issues and their solutions in wireless LAN. IEEE Xplore Digital.

.22 N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," Future Generation Computer Systems, vol. 100, pp. 779–796, 2019.

.23 Rehman, S. U., Abdullah, M., & Shahzad, M. (2021). DoS Attacks on the Internet of Things: A Survey. IEEE Access, 9, 110493-110513.

.24 Rehman, Shafiq & Manickam, Selvakumar & Firdous, Nur. (2023). Impact of DoS/DDoS attacks in IoT environment: A study. AIP Conference Proceedings. 020020. 10.1063/5.0150000.

.25 Goran Vojković and Melita Milenković. (2020). IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. Business Systems Research Journal. 11. 167-185. https://www.sciendo.com/article/10.2478/bsrj-2020-0033

.26 Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers 2020, 9, 44. https://doi.org/10.3390/computers9020044.

.27 Mark Mbock Ogonji, George Okeyo, Joseph Muliaro Wafula,A survey on privacy and security of Internet of Things,Computer Science Review,Volume 38,2020,100312,ISSN 1574-0137,

.28 Manasha Saqib, Ayaz Hassan Moon, A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication,Computers & Security,Volume 125, 2023, 103053, ISSN 0167-4048.
https://www.sciencedirect.com/science/article/abs/pii/S016740482200445X?via%3Dihub

.29 Alex Koohang,Carol Springer Sargent,Jeretta Horn Nord,Joanna Paliszkiewicz Internet of Things (IoT): From awareness to continued use.International Journal of Information Management. Elsevier. Volume 62.February 2022.

.30 Meneghello F, Calore M, Zucchetto D, Polese M, and Zanella A (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 6(5): 8182-8201. https://doi.org/10.1109/JIOT.2019.2935189.

.31 Ahmed, Bilal & Shuja, Mirza & Mishra, Hari & Qtaishat, Ahmed & Sharma, Mukesh. (2023). IoT Based Smart Systems using Artificial Intelligence and Machine Learning: Accessible and

Intelligent Solutions. 1-6. 10.1109/ISCON57294.2023.10112093.

.32 Alsamiri J, Alsubhi K. Internet of things cyber attacks detection using machine learning. Int J Adv Comput Sci Appl. 2019;10(12):627–34. https://doi.org/10.14569/ijacsa.2019.0101280

.33 G Yashodha et al 2021 IOP Conf.Role of Artificial Intelligence in the Internet of Things – A Revie. Ser.: Mater. Sci. Eng. 1055 012090

.34 Dr. Venkatesh Naganathan, Prof. Rajesh Rao K . The Evolution of Internet of Things: Bringing the power of Artificial Intelligence to IoT, its Opportunities and Challenges .International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 3, May - June 2018

.35 Mohammad Binhammad, Shaikha Alqaydi, Azzam Othman, Laila Hatim Abuljadayel. The Role of AI in Cyber Security: Safeguarding Digital Identity. Journal of Information Security Vol.15 No.2, April 30, 2024.

.36 Salem, A.H., Azzam, S.M., Emam, O.E. et al. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. J Big Data 11, 105 (2024). https://doi.org/10.1186/s40537-024-00957-y

.37 https://www.ibm.com/topics/internet-of-things.

.38 https://www.kapsarc.org/ar/research/publications/the-role-of-intelligent-transportation-systems-and-artificial-intelligence-in-energy-efficiency-and-emission-reduction/2024