فهرس المحتويات

المقدمة ٥

تعريف ٧

التاريخ ٨

الابتكار الذي يدعم ظهور (IoT) ١١

(IoT) اليوم: نقطة التحول ١٢

الإدراك لـ(IoT) ١٤

لمحة عامة عن بناء (IoT) ١٤

البناء ذو ٣ طبقات ١٥

البناء ذو ٥ طبقات ١٦

بروتوكولات اتصالات (IoT) ١٨

تنبؤات/ توقعات (IoT) ١٨

العنونة/ المعالجة ٢٠

أجهزة الاستشعار والمحركات في (IoT) ٢٢

المجسات/ المستشعرات ٢٣

المحركات/ المشغلات ٢٤

المراقب/ الموجه ٢٤

الاختلافات الهامة في (IoT) ٢٤

أهمية أجهزة الاستشعار الدقيقة ٢٥

معايرة أجهزة الاستشعار ٢٦

أهمية المعايرة الدقيقة ٢٦

تحديات جديدة => تقنيات جديدة ٢٧

تحديد تردد الراديو RFID ٢٨
منصة (IoT) ٥٣
التطبيق ٦١
المدن الذكية ٦١
تقنيات المدينة الذكية ٦١
(IoT) في المدن الذكية ٦٢
المدن الذكية والاستدامة ٦٣
التحديات في المدن الذكية ٦٥
المنازل الذكية ٦٥
تطبيقات (IoT) في المنازل الذكية ٦٦
كيف يعمل نظام الأتمتة القائم على (IoT) ٦٧
الإعداد الأساسي ٦٧
الاتصال السحابي ٦٨
المراقبة في الوقت الحقيقي والتنبيهات ٦٨
التكامل (IFTTT) ٦٩
أجهزة استشعار (IoT) لأتمتة المنزل ٦٩
(IoT) في الرعاية الصحية ٧٠
IoMT في المنزل ٧٠
IoMT على الجسد ٧١
الإدارة والتحليل للبيانات (IoT) ٧٢
دورة حياة (IoT) ٧٢
(IoT) والبيانات الكبيرة ٧٦
ما هي البيانات الكبيرة؟ ٧٦

تتميز ولكنها تكميلية ٧٨
الأمان والخصوصية في (IoT) ٧٩
المخاطر الأمنية والتحديات ٨٠
نقاط ضعف الجهاز ٨٠
سلامة البيانات وسريتها ٨٠
قنوات الاتصال غير الآمنة ٨٠
فقدان المعيار القياسي ٨١
مخاوف الخصوصية ٨١
جمع البيانات المجتاحة ٨١
تجميع البيانات وتنميطها ٨١
الخرق في البيانات ٨٢
التحكم غير الكافي للمستخدم ٨٢
الحلول الخاصة بالأمن وأفضل الممارسات ٨٢
التصميم الآمن للجهاز ٨٢
التحديثات المنتظمة وإدارة الترميم ٨٣
تجزئة الشبكة ٨٣
التقليص من البيانات وإخفاء الهوية ٨٣
الأطر والمعايير الأمنية لـ (IoT) ٨٣
التشفير في (IoT) ٨٤
نظام (Blockchain) لحفظ الأمن في (IoT) ٨٦
نظام (IoT) والذكاء الاصطناعي ٨٨
التعلم الآلي في (IoT) ٨٩
التعلم العميق (DL) في (IoT) ٩٠

تطبيقات (IoT) التي تعمل بالذكاء الاصطناعي ٩٢
المنازل الذكية..... ٩٢
القطاع الصحي..... ٩٣
الزراعة..... ٩٣
النقل ٩٤
أخلاقيات الذكاء الاصطناعي ونظام (IoT)..... ٩٤
الخاتمة..... ٩٦

المقدمة

إنترنت الأشياء (Internet of Things = IoT)هو مصطلح تقني يشير إلى تواصل مجموعة من الأجهزة المختلفة المتصلة بالإنترنت، وتشارك البيانات فيما بينها، والتفاعل مع بعضها ومع المستخدمين. بعكس الأجهزة التقليدية المتصلة بالإنترنت مثل أجهزة الكمبيوتر والهواتف الذكية. إن (IoT) يتضمن أجهزة غير مرتبطة تقليدياً بالإنترنت، مثل: المنظمات الحرارية، وعدادات المرافق، والآلات الصناعية، والمعدات الزراعية، والأجهزة القابلة للارتداء.[١]

تتمتع أجهزة (IoT) بهويات مميزة تتيح التعرف عليها على الإنترنت بسهولة، ويمكن مراقبتها والتحكم فيها وإدارتها عن بُعد. فمثلاً؛ يمكن التحكم في منظم الحرارة المتصل بالإنترنت عن بُعد من خلال التطبيق الخاص بالهاتف الذكي؛ مما يسمح للمستخدم بضبط درجة حرارة منزله أو مكتبه حتى عند مغادرته.

تبعاً لموقع (https://iot-analytics.com/)، فإنه في نهاية ٢٠٢٣م من المتوقع أن يصل عدد الأجهزة الفعالة المتصلة بالإنترنت ١٦,٧ بليون جهاز بمعدل نمو يصل إلى ١٦٪، وقد يشهد عام ٢٠٢٧م ثورة في عدد الأجهزة المتصلة حيث إنه من المحتمل أن يبلغ عدد الأجهزة الفعالة المتصلة ٢٩ بليون جهاز [٢]. وسيكون لهذه الأجهزة تطبيقات مفيدة في مجالات الرعاية الصحية، والتصنيع، والنقل، والزراعة، والطاقة، وغيرها من المجالات الأخرى.

تقوم تطبيقات (IoT) بمعالجة البيانات الواردة من الأجهزة وتوليد المعلومات، ووضعها في سياقها لتوفير رؤى مفيدة ومعلومات قابلة للتنفيذ يبنى عليها اتخاذ قرارات مناسبة. على سبيل المثال، يمكن لمصنع مزود بـ (IoT) أن يجمع بيانات عن أداء الماكينة ودرجة الحرارة ومستويات الرطوبة؛ مما يسمح لمدير المصنع بتحديد المشكلات المحتملة وتحسين الإنتاج واتخاذ القرارات.

كذلك تساهم البيانات المنظمة والمرتبة التي تجمع من أجهزة (IoT) في تقديم تصورات أولية ذات قيمة عالية، وتوفير الأداء الأكثر ذكاءً، ويتجلى ذلك في استخدام

---

١ موقع وزارة الاتصالات وتقنية المعلومات.

٢ مقالة (State of IoT 2023).

أجهزة (IoT) لمراقبة صحة المرضى عن بعد؛ مما يساعد مقدمي الرعاية الصحية على اكتشاف المشاكل المحتملة في مرحلة مبكرة قبل أن تصبح حرجة.

إن الثورة الرقمية والهرولة نحو الأتمتة وتزايد عدد الأجهزة المتصلة، وثورة الذكاء الاصطناعي، والاهتمام العالمي بـ "إنترنت الأشياء" ينذر بتغير جذري مخيف في أسلوب إدارة حياتنا وأعمالنا بكفاءة عالية تختصر الوقف والجهد.. وفي هذا الكتاب أعرض لك أيها القارئ ما تحتاجه للتعرف بشكل عام على هذا المجال وآلية عمله، وفوائده ومخاطره، وبنيته التكوينية، وتطبيقاته، وارتباطه بالذكاء الاصطناعي وتعلم الآلة والتعلم العميق، ودوره المنتظر في تطوير الخدمات والأنشطة المختلفة في حياتنا اليومية بما يساهم في تلبية الحاجات المعيشية والتعليمية والصناعية والصحية والسياحية والاقتصادية وغيرها بأفضل الطرق قدر الإمكان.

وبالله التوفيق.

تعريف

يمكن تعريف (Internet of Things = IoT)على أنه: تواصل الأجهزة المتصلة بالإنترنت والتفاهم فيما بينها من خلال برامج وتقنيات ومستشعرات مضمَّنة تتيح تبادل البيانات عبر شبكة لا سلكية دون تدخل بشري. [٣]

يرتكز نظام الـ (IoT) على شبكة عالمية ديناميكية تتميز بتكوين ذاتي قائمة على بروتوكولات اتصال موحدة وقابلة للتشغيل المتبادل فيما بينها، وتسمح بإنشاء هويات مميزة وخصائص مادية وشخصيات افتراضية لكل من الأشياء الحقيقية والخيالية. تحتوي هذه العناصر على واجهات معقدة تمكنها من مشاركة المعلومات حول الأشخاص ومحيطهم. [٤]

تعد الطبيعة الديناميكية والتكيف الذاتي إحدى الخصائص الأساسية لـ (IoT) ؛ حيث يمكن أن تتكيَّف الأنظمة والأجهزة مع البيئات المتغيرة وتتخذ الإجراء المناسب بناءً على ظروف تشغيلها. على سبيل المثال، يمكن للكاميرات الأمنية في أوقات من اليوم تغيير أوضاعها أو اتخاذ الزوايا المناسبة لها بناء على الظروف المحيطة أو المهام المطلوبة. كذلك، تتمتع الأجهزة بالقدرة على التهيئة الذاتية، لتتمكن بذلك من التعاون والتكامل لتوفير ميزات محددة.

أيضاً تعتبر معايير الاتصال القابلة للتشغيل البيني جانبًا مهمًا آخر من جوانب (IoT). يمكن للأجهزة الاتصال بالأجهزة الأخرى والبنية التحتية من خلال دعم مجموعة من البروتوكولات المختلفة. كل جهاز له هوية خاصة بالإضافة إلى معرف خاص، مثل عنوان IP أو URI. قد تتضمن أنظمة (IoT) واجهات مستخدم ذكية يمكنها التواصل مع الأشخاص والسياقات في البيئة وتعديلها اعتمادًا على السياق.

وأخيراً، عادة ما تُدمج أجهزة (IoT) في شبكة المعلومات؛ مما يسمح لها ذلك بالتفاعل وتبادل البيانات مع الأنظمة والأجهزة الأخرى. يوفر (IoT) بنية تحتية قوية يمكنها دعم إنشاء خدمات وتطبيقات متطورة من خلال دمج هذه الميزات معًا.

---

[٣] Internet-of-Things-IoT-in-5G-Mobile-Technologies-by-Jordi-Mongay-booksfree.org

[٤] IoT_in_five_days-v10_20160215

التاريخ

نشأت فكرة ربط وتوصيل "الأشياء" المادية بالإنترنت منذ إنشاء شبكة الويب العالمية في عام ١٩٨٩. وكان أحد أقدم الأمثلة على هذا النوع من التطبيقات هو Trojan Room.

في عام ١٩٩٠، ابتكر "جون رومكي" أول جهاز متصل بالإنترنت: وهو محمصة يمكن التحكم فيها عن بُعد. كان اختراع "Steve Mann" لـ WearCam في عام ١٩٩٤ بمثابة اختراق سمح بأداء شبه حقيقي باستخدام نظام ٦٤ معالجًا. وفي عام ١٩٩٧، قدم "Paul Saffo" وصفًا موجزًا لأجهزة الاستشعار وتطبيقاتها المحتملة في المستقبل.

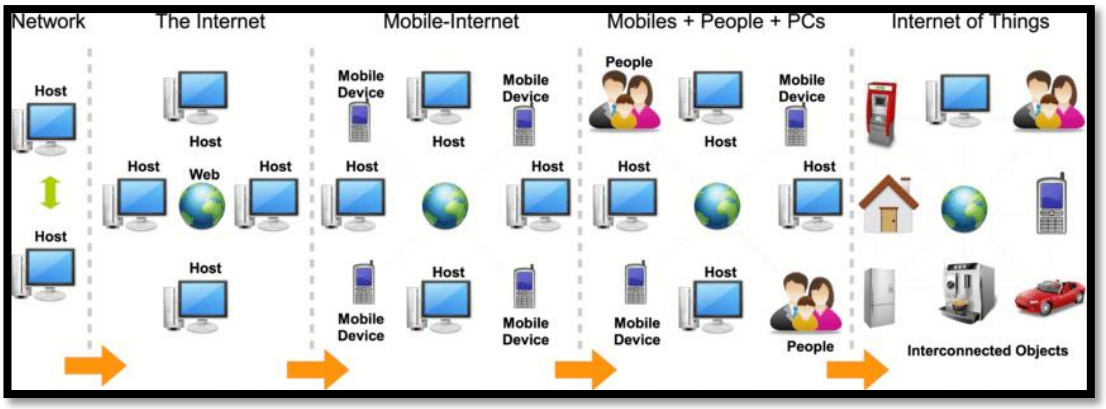
مصطلح "(IoT)" صاغه كيفن أشتون في عام ١٩٩٩، بالتزامن مع تطوير نظام عالمي لتعريف العناصر يعتمد على تقنية RFID. في عام ٢٠٠٠، أعلنت LG الضخمة، عن خططها لإطلاق ثلاجة ذكية يمكنها اكتشاف ما إذا كانت المواد الغذائية المخزنة بداخلها تتطلب التجديد أم لا.[٥]

شهد عام ٢٠٠٣ نشر تقنية تحديد الترددات الراديوية (RFID) على نطاق واسع في برنامج (Savi) للجيش الأمريكي. في نفس العام، قامت شركة "وول مارت" لتجارة التجزئة بتطبيق تقنية RFID في جميع متاجرها على مستوى العالم على نطاق واسع. في عام ٢٠٠٥، نشرت المنشورات الرئيسية مثل The Guardian وScientific American وBoston Globe العديد من المقالات حول (IoT) وآفاقها المستقبلية. في عام ٢٠٠٨، أنشأ تحالف من الشركات تحالف IPSO بهدف تعزيز استخدام بروتوكول الإنترنت (IP) في شبكات "الكائنات الذكية" وتمكين (IoT). في نفس العام، أذنت لجنة الاتصالات الفيدرالية (FCC) باستخدام "طيف الفضاء الأبيض" الذي فتح آفاقا جديدة في مجال الـ IoT. أدى إدخال IPv6 في عام ٢٠١١ إلى نمو هائل للأجهزة المترابطة، مما قاد العديد من البلدان والشركات إلى الاهتمام الفعلي بهذا المجال، وتسخير الموارد لتطويره، وتشجيع الباحثين فيه، وقد اتخذ عمالقة التكنولوجيا مثل Cisco وIBM وEricsson العديد من المبادرات التعليمية والتجارية مع (IoT).[٦]

---

[٥] https://www.visionofhumanity.org/what-is-the-internet-of-things/

[٦] the IoT supporting the cultural heritage domain analysis, design and implementation of a smart framework



الشكل ١: تاريخ (IOT)

يمكننا الآن تشغيل الأجهزة والمعدات التي نستخدمها يوميًا ومراقبتها بفضل تقنية (IoT) التي تعتمد بشكل كبير على أجهزة الاستشعار المثبتة والمنتشرة في أماكن عدة، وهي بدورها تقوم بتحويل البيانات المادية غير المعالجة إلى إشارات رقمية تُرسل إلى غرف التحكم لتحويلها إلى معلومات قابلة للفهم والتحليل، وتأطيرها ونمذجتها في مخططات ورسومات بيانية لاستيعابها وقراءتها والتعامل معها بسهولة؛ ويتيح لنا ذلك إدارة ومراقبة الأعمال، والشركات، والمهام الأكثر أهمية، والتغيرات البيئية، والنظم الأمنية والمرورية عن بُعد عبر الإنترنت من أي مكان في العالم.

تعد إنترنت الأشياء في الوقت الحالي ضرورة لا غنى عنها، حيث تتميز بكونها تعطي نظرة سريعة ورؤى حقيقية في الوقت الفعلي وتغذية راجعة مستمرة، وهذا ما يجب أن يقوم عليه أي نظام (IoT) عند تصميمه وتأسيسه.

على سبيل المثال، تقنيات المراقبة الجديدة المتقدمة للمطارات ومنشآت الطيران، مثل: أنظمة إدارة الفيديو (VMS) القوية والمفتوحة، والكاميرات البانورامية عالية الدقة؛ حيث تقوم هذه الأجهزة بمسح ومراقبة المسافرين وقراءة صورهم، ومعالجتها عبر أجهزة وبرامج حاسوبية فائقة الدقة، والتحقق من بياناتهم، وإتمام إجراءات سفرهم دون الحاجة إلى عنصر بشري، وتزويد الجهات بالمعلومات في الوقت الفعلي لاتخاذ التدابير المطلوبة والاحتياطات اللازمة.

وفي المنزل الذكي؛ كل صندوق مفاتيح كهربائي يجب أن يتصل ويربط في نظام التشغيل الآلي للمنزل، ويدار بهاتف ذكي أو جهاز تحكم عن بعد. ومع ذلك، لا يستلزم هذا السيناريو تثبيت معالج أو جهاز تخزين في كل صندوق تبديل لتجميع الإشارات ومعالجتها، ما نحتاجه فقط بشكل أساسي هو تبديل ON / OFF، وكل ما هو مطلوب للتحكم به من مسافة بعيدة هو جهاز استشعار. وهذا يختلف عن نظام تقنيات المراقبة الجديدة للمطارات حيث يتطلب لتنفيذ ذلك أجهزة حاسوبية مواصفاتها عالية وبرامج حاسوبية فائقة الدقة وأنظمة أمنية عالية الكفاءة.

نتيجة لذلك، تختلف بنية أنظمة (IoT) باختلاف البيئة التي يتم استخدامها فيها.



الشكل ٢: المنزل الذكي

الابتكار الذي دعم ظهور ونمو (IoT)

في السنوات الماضية ساهمت الأجهزة الذكية وتزايد استخدامها، وشبكة الـ (5G)، وتقنيات الحوسبة المتطورة، وبرامج الذكاء الاصطناعي وتطبيقاته، والكيانات الصناعية التكنولوجية، وتحديد عنوان فريد خاص وثابت (IP Address) لكل جهاز متصل بالإنترنت، وظهور منظمات جديدة لتطوير وتقنين المعايير الخاصة باستخدام إنترنت الأشياء في نمو الـ (IoT) بشكل كبير، ودفع عجلة تقدم الابتكارات في هذه المجالات على مستويات مختلفة.

إن دمج المستشعرات في الأجهزة هو الابتكار الذي أدى إلى ظهور إنترنت الأشياء وجعل مسألة الاستعانة به في الحياة المعاصرة تحظى بمتابعة واهتمام من مختلف العلماء والمتخصصين والباحثين في مجالات تقنيات المعلومات والاتصالات، الأمر الذي أدى إلى تنوع الابتكارات في هذا المجال.[٧]



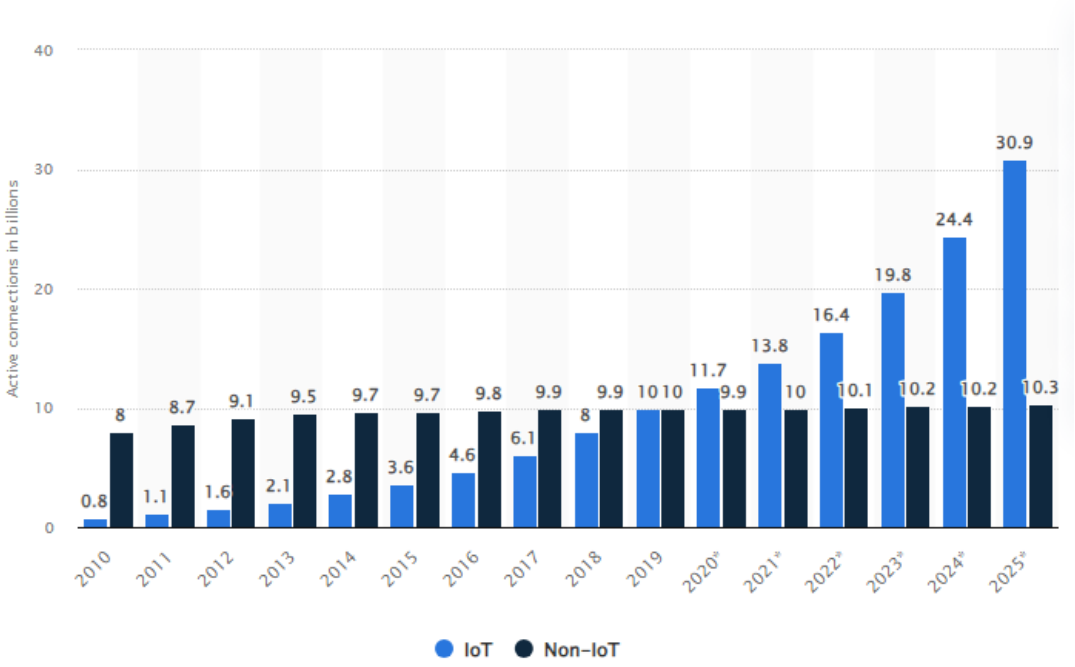
الشكل ٢: تركيب شبكة استشعار.

[٧] (Magdalena 2016).

إنترنت الأشياء (IoT) اليوم: هو نقطة التحول

من المتوقع أن يزداد عدد أجهزة (IoT) المنتشرة والمتصلة ببعضها بنسبة مذهلة تبلغ ١٠٠٠٪ بين عامي ٢٠١٠ و٢٠٣٠، لتصل إلى ما يقرب من ٢٩ بليون وحدة.

في عام ٢٠١٠، كانت أجهزة (IoT) تمثل ١٠٪ فقط من جميع الأجهزة المتصلة، ولكن بحلول عام ٢٠٢٣، زادت هذه النسبة إلى أكثر من ٥٠٪، متجاوزة الأجهزة التي لا تدعم (IoT). تجاوزت عائدات السوق العالمية لـ (IoT) ٤٠٠ مليار دولار في عام ٢٠٢٢ وتستمر في النمو بسرعة.[٨]



تعتبر وحدات التحكم الصغيرة منخفضة الطاقة (Low-power microcontrollers) مكونًا أساسيًا للعديد من أجهزة (IoT). تم توفير أكثر من ٢٨ مليار وحدة تحكم دقيقة في عام ٢٠١٨، ومن المتوقع أن يتم استخدام أكثر من ٢٥٠ مليار

[٨] IoT and non-IoT connections worldwide 2010-2025

وحدة تحكم دقيقة على مستوى العالم بحلول عام ٢٠٢٠، وصولاً إلى أكثر من ٤٠٠ مليار وحدة تحكم في عام ٢٠٢٣م.

تتصل غالبية أجهزة (IoT) بالشبكات من خلال الاتصال السلكي أو اللاسلكي، وتستخدم في مجالات متنوعة من الصناعات، مثل السيارات، والأتمتة الصناعية، والإلكترونيات الاستهلاكية للاستخدام المنزلي والشخصي، والعدادات الذكية للشبكة الذكية، وتطبيقات الرعاية الصحية، والفضاء، والدفاع.

تُدار العديد من العمليات الصناعية في عصر إنترنت الأشياء عن بعد (عبر الشبكة). فمن خلال تجميع البيانات والحصول عليها في الوقت الفعلي، وتحليلها وتصنيفها وتحويلها إلى معلومات مفيدة؛ لتقييم العمليات وسلاسل التوريد وخطوط الإنتاج والمبيعات المعقدة بشكل أفضل والتحكم فيها دون الحاجة إلى تدخل بشري.

جاءت ثورة إنترنت الأشاء Internet of Things لتقدم شكلاً جديداً لخدمات وتطبيقات الإنترنت وتحدث بذلك نقلة نوعية في أسلوب ونوع الخدمات التي تقدمها بما يحقق مستويات عالية من السهولة والسرعة في خدمة الإنسان.

فهم إنترنت الأشياء (IoT) وطبيعة عملها

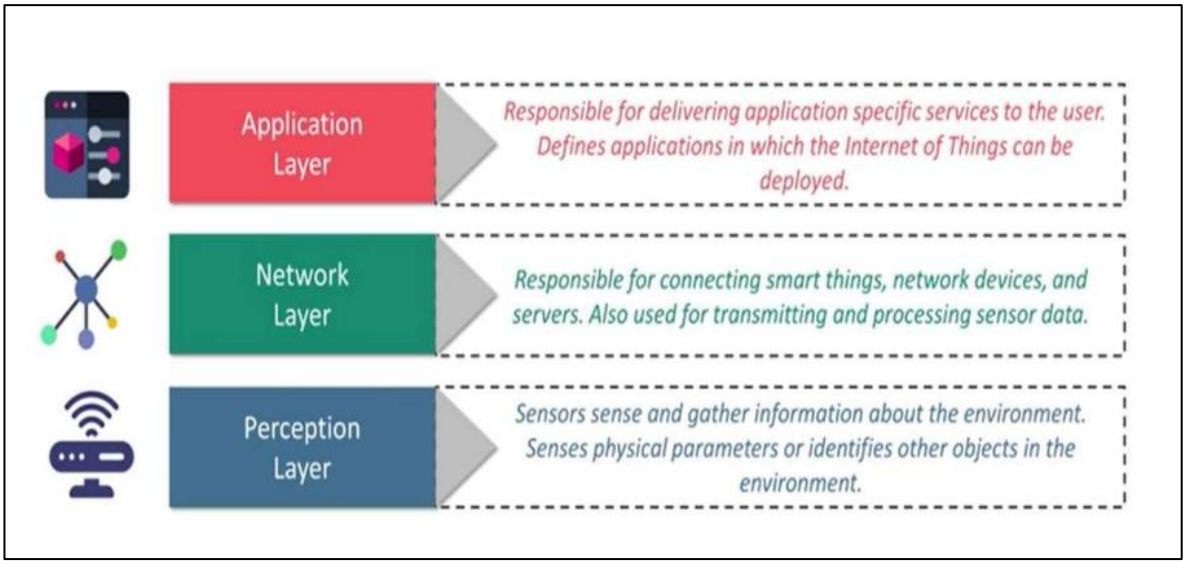
لمحة عامة عن بناء (IoT)

لتمكين وتحقيق إنترنت الأشياء (IoT) تدمج العديد من التقنيات والبروتوكولات الرئيسية، بما في ذلك WSN وRFID وM٢M، و NFC، وشبكات (PAN) Low Power Personal Area Networks. العديد من المنظمات ومجموعات الأعمال مثل شركة قوقل وأوراكل وسيسكو قامت باقتراح نظام عمل لـ (IoT)، ولكن للأسف حتى الآن لم يتفق على إطار عمل عالمي معتبر عند إنشاء أنظمة وتطبيقات إنترنت الأشياء.

إن التهديدات السيبرانية هي إحدى أهم التحديات التي تواجه تطبيقات الـ (IoT) ومستخدميها، ولذلك يجب مراعاة الصلابة الأمنية عند بناء التطبيقات والأنظمة، واعتماد إطار عمل يمتاز بالجدارة الأمنية والموثوقية يكون سداً حاجزاً ودرعاً حصينا يمنع من الوصول غير المصرح به إلى البيانات.

يجب أن تكون بنية (IoT) مرنة بما يكفي لمعالجة مجموعة متنوعة من المشكلات، بما في ذلك جودة الخدمة (QoS)، والموثوقية، وقابلية التشغيل البيني الدلالي، وإدارة الخصوصية، ودعم أنواع الأجهزة والخدمات الجديدة، وما إلى ذلك، من أجل تطوير شبكات واسعة النطاق من كائنات مقيدة تشارك في تفاعلات في الوقت الفعلي. طبقة الإدراك وطبقة الإرسال وطبقة التطبيق هي الطبقات الثلاث لمعمارية أمن (IoT) التي اقترحها قطاع تقييس الاتصالات بالاتحاد. تتكون كل طبقة من طبقات فرعية قائمة على أساس وظيفي.

البناء ذو٣ طبقات

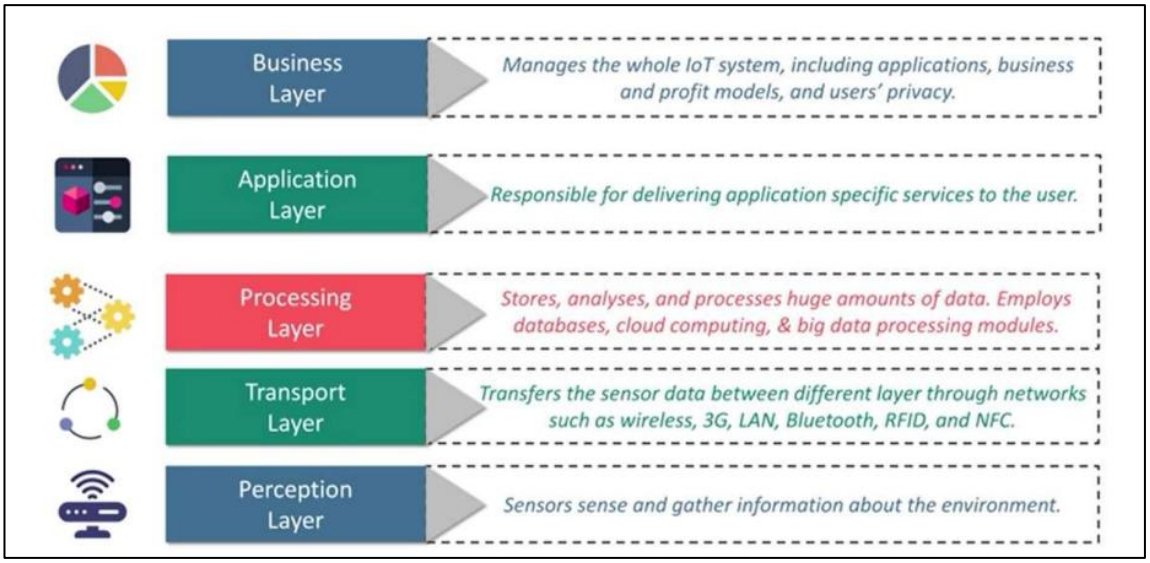


طبقة الإدراك هي الطبقة المادية التي تكتشف وتجمع البيانات حول المناطق المحيطة. وهي تتألف من مستشعرات يمكنها اكتشاف العديد من المعلمات الفيزيائية، مثل درجة الحرارة والضغط والرطوبة، فضلاً عن تحديد الكائنات الذكية الأخرى الموجودة في البيئة.

طبقة الشبكة مسؤولة عن إنشاء اتصالات مع الأجهزة الذكية الأخرى وأجهزة الشبكة والخوادم. وتتمثل مهمتها الرئيسية في تمكين نقل ومعالجة البيانات التي تم جمعها بواسطة مستشعرات طبقة الإدراك. بالإضافة إلى ذلك، توفر طبقة الشبكة ميزات مثل التوجيه والتنقل والأمن لضمان نقل البيانات بكفاءة وأمان.

طبقة التطبيق هي المسؤولة عن توفير الخدمات الخاصة بالتطبيقات للمستخدم. يحدد حالات الاستخدام المختلفة ل(IoT)، مثل المنازل الذكية والمدن الذكية والصحة الذكية. تتيح طبقة التطبيقات للمستخدمين إدارة أجهزة (IoT) الخاصة بهم والتحكم فيها، مما يوفر تكاملًا سلسًا وسهولة في الاستخدام. كما يوفر أدوات لتحليل البيانات والتصور للمساعدة في الحصول على رؤى حول البيانات التي تم جمعها بواسطة مستشعرات طبقة الإدراك.

البناء ذو ٥ طبقات



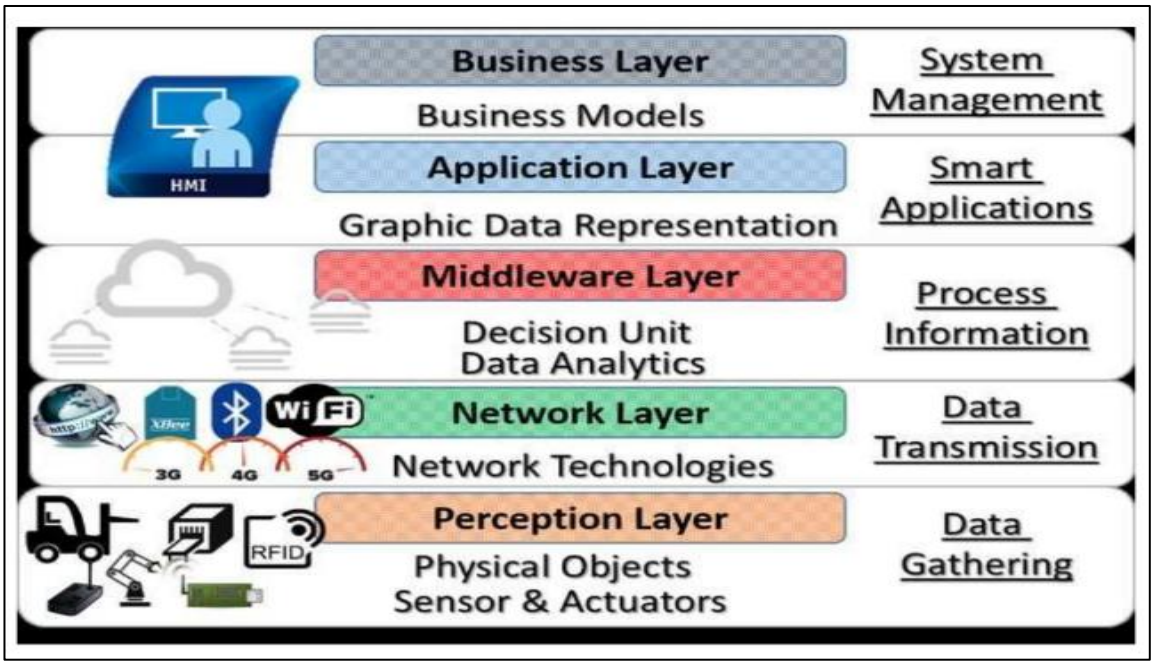
تشتمل بنية أمن (IoT) التي اقترحها الاتحاد الدولي للاتصالات أيضًا على طبقة النقل وطبقة المعالجة وطبقة الأعمال.

تعد طبقة النقل مكونًا حيويًا في بنية (IoT)، حيث إنها تسهل نقل بيانات المستشعر بين طبقة الإدراك وطبقة المعالجة باستخدام تقنيات الشبكة المختلفة مثل الشبكات اللاسلكية والجيل الثالث والشبكة المحلية والبلوتوث وRFID وNFC. تتمثل مسؤوليتها الأساسية في ضمان نقل البيانات التي تم جمعها من طبقة الإدراك بكفاءة وأمان إلى طبقة المعالجة لتحليلها وتخزينها، وأن البيانات التي تمت معالجتها يتم إرسالها مرة أخرى إلى طبقة الإدراك لاتخاذ الإجراء المناسب.

طبقة المعالجة، المعروفة أيضًا باسم طبقة البرامج الوسيطة، هي المسؤولة عن تخزين وتحليل ومعالجة الكميات الهائلة من البيانات الواردة من طبقة النقل. يعمل كوسيط بين الطبقات الدنيا والعليا ويقدم مجموعة واسعة من الخدمات للطبقات السفلى. تستفيد طبقة المعالجة من تقنيات مثل قواعد البيانات والحوسبة السحابية ووحدات معالجة البيانات الضخمة لتخزين ومعالجة وتحليل البيانات التي تم جمعها من الطبقات الدنيا.

تدير طبقة الأعمال نظام (IoT) بالكامل، بما في ذلك التطبيقات ونماذج الأعمال والربح وخصوصية المستخدم. وهي مسؤولة عن إنشاء وتنفيذ الهيكل العام لنظام (IoT)،

بما في ذلك تحديد نماذج الأعمال وتحديد التطبيقات ووضع سياسات الخصوصية والأمان. تلعب طبقة الأعمال أيضًا دورًا مهمًا في تحديد الرؤية الشاملة لنظام (IoT) وخلق بيئة يمكن أن تزدهر فيها خدمات (IoT).

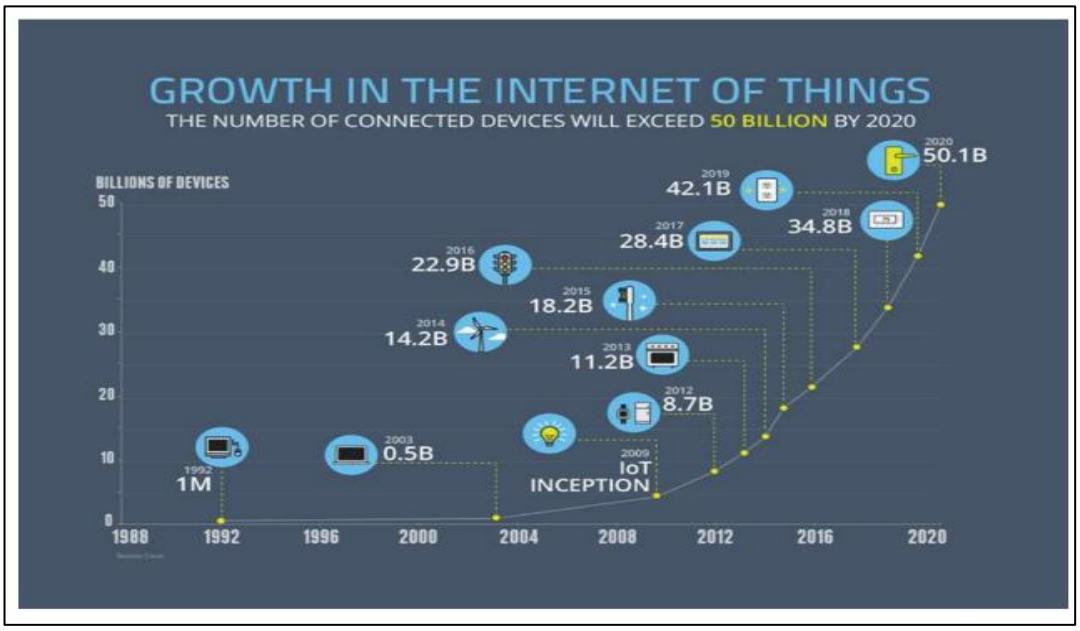


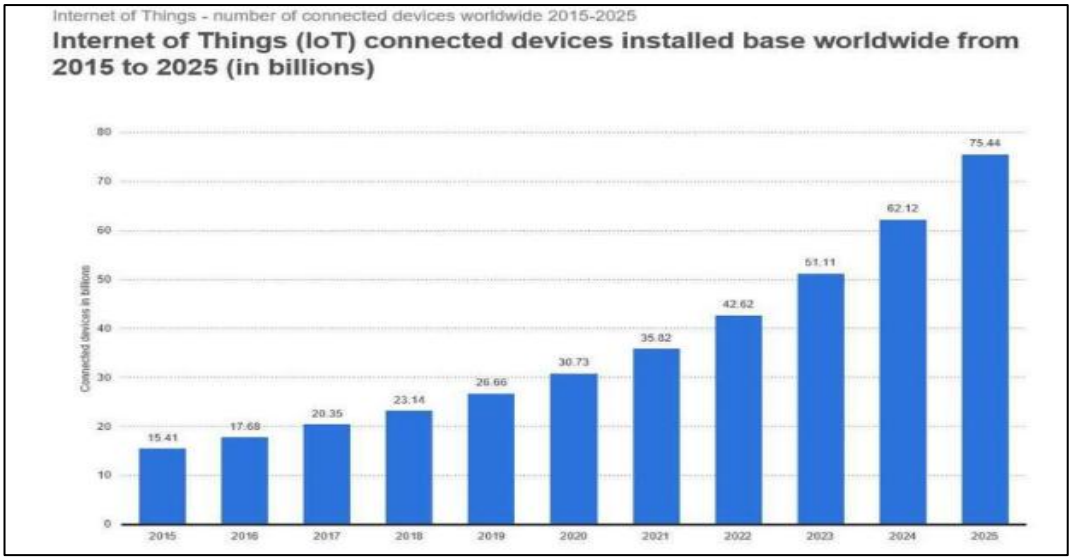
بروتوكولات اتصالات (IoT)

تنبؤات/ توقعات (IoT)

بحلول عام ٢٠٢٠، تتوقع Cisco أنه سيكون هناك أكثر من ٥٠ مليار أداة متصلة بالإنترنت، مما يوضح النمو الهائل ل(IoT). الاختراقات التكنولوجية في الشبكات، وبرامج النظام المضمنة، والأجهزة المضمنة منخفضة الطاقة، والحوسبة المتطورة تقود هذا التوسع. علاوة على ذلك، بحلول عام ٢٠٢٢، تقدر شركة Cisco أنه سيكون هناك تريليون جهاز استشعار متصل بالشبكة مدمج في العالم من حولنا، مما يوفر وفرة من البيانات لتطبيقات (IoT). في العقدين المقبلين، من المتوقع أن يزداد هذا الرقم أكثر من ذلك، ومن المحتمل أن يصل إلى ٤٥ تريليون جهاز استشعار. مع الكم الهائل من البيانات التي تم إنشاؤها بواسطة أجهزة (IoT)، من الأهمية بمكان أن يكون لديك بنية تحتية قوية، بما في ذلك طاقة المعالجة والتخزين السحابي، لإدارة البيانات وتحليلها بكفاءة.

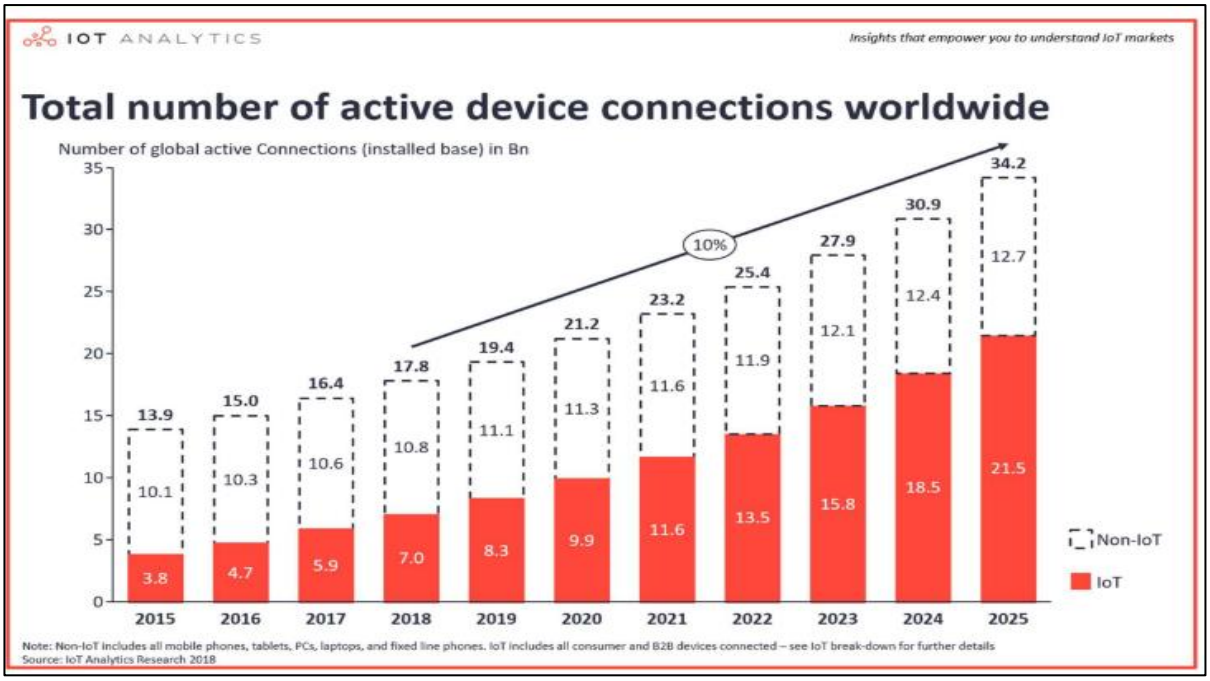
يوفر نمو (IoT) والعدد المتزايد من الأجهزة وأجهزة الاستشعار المتصلة إمكانيات جديدة للشركات والمستهلكين على حدٍ سواء، ولكنها تفرض أيضًا تحديات أمان وخصوصية كبيرة يجب معالجتها. على الرغم من هذه التحديات، من المتوقع أن تستمر الفوائد المحتملة ل(IoT) وانتشار الأجهزة وأجهزة الاستشعار المتصلة في دفع الابتكار التكنولوجي والنمو الاقتصادي في السنوات القادمة.





من المتوقع أن تصل القاعدة المثبتة لأجهزة (IoT) إلى أكثر من ٣١ مليار على مستوى العالم بحلول عام ٢٠٢٠. وسيتم تثبيت أكثر من ٧٥,٤ مليار جهاز في جميع أنحاء العالم بحلول عام ٢٠٢٥. قاعدة مثبتة للأجهزة المتصلة بـ(IoT) على مستوى العالم من ٢٠١٥ إلى ٢٠٢٥ (بالمليارات) بحسب ستاتيستا.

يوجد بالفعل أكثر من ١٧ مليار جهاز متصل قيد الاستخدام في جميع أنحاء العالم، ٧ مليارات منها عبارة عن أجهزة (IoT) (هذه الإحصائية لا تشمل الهواتف الذكية والأجهزة اللوحية وهواتف الخطوط الثابتة).

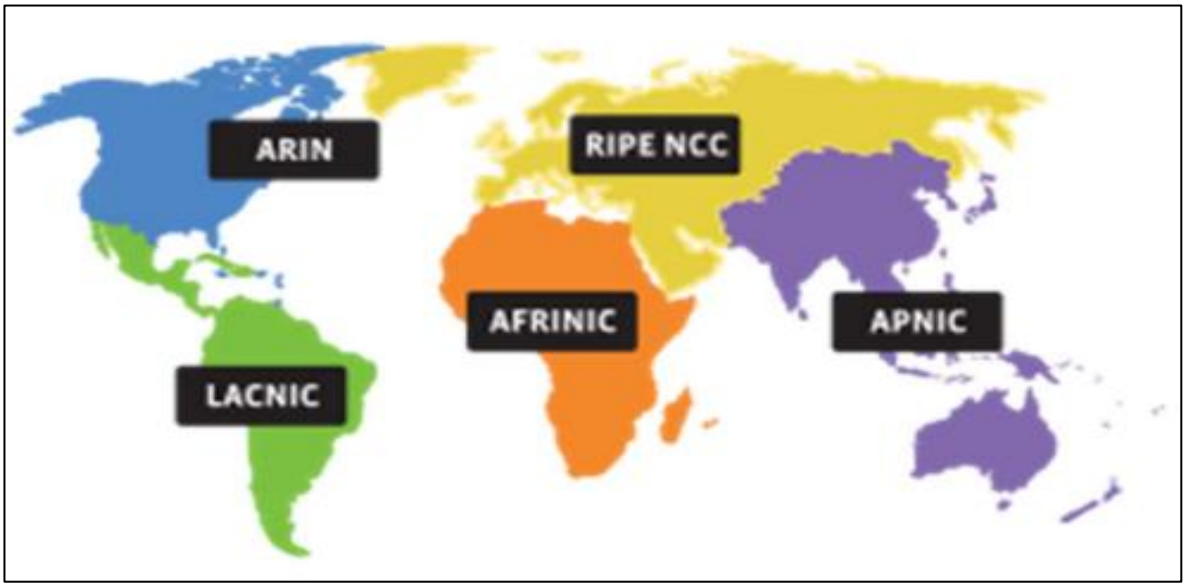


العنونة/ المعالجة

يستخدم بروتوكول IPv4، الذي كان بمثابة أساس الإنترنت لسنوات عديدة، عنوانًا من ٤ بايت لتحديد كل عقدة على الشبكة. ومع ذلك، فإن عدد عناوين IPv4 المتاحة يتناقص بسرعة، ومن المتوقع أن يتم استنفاد مجموعة عناوين IPv4 بالكامل قريبًا. تم تضخيم هذه المشكلة بسبب النمو الهائل للإنترنت والعدد المتزايد من الأجهزة المتصلة. في ٣١ يناير ٢٠١١، نفدت عناوين IANA، الكيان المسؤول عن إدارة عناوين IP. وقد تفاقم الوضع بسبب حقيقة أن العديد من سجلات الإنترنت الإقليمية (RIRs) قد استهلكت جميع احتياطيات العناوين الخاصة بهم. لا يزال بإمكان مزودي خدمة الإنترنت الفرديين الوصول إلى مجموعات عناوين IP غير المعينة ويمكنهم إعادة تدوير أي عناوين لم يعد المشتركون بحاجة إليها. ومع ذلك، هذا مجرد حل مؤقت، وقد تم تطوير تقنيات جديدة مثل IPv6 لمعالجة مشكلة استنفاد عنوان IPv4. يستخدم IPv6 عنوانًا من ١٢٨ بت، مما يوفر عددًا غير محدود من العناوين الفريدة للمستقبل المنظور.

على الرغم من أن اعتماد IPv6 كان بطيئًا، إلا أنه يكتسب قوة جذب مع استمرار تقلص مجموعة عناوين IPv4 المتاحة. يمثل استنفاد مجموعة عناوين IPv4 تحديات

كبيرة للبنية التحتية للإنترنت ويسلط الضوء على الحاجة إلى الابتكار المستمر في بروتوكولات الشبكة والبنية التحتية.



التسجيل	المنطقة المغطاة
AFRINIC	منطقة أفريقيا
APNIC	منطقة آسيا والمحيط الهادئ
ARIN	كندا والولايات المتحدة الأمريكية وبعض جزر الكاريبي
LACNIC	أمريكا اللاتينية وبعض جزر الكاريبي
RIPE NCC	أوروبا والشرق الأوسط وآسيا الوسطى

يتلقى المستخدمون عناوين IP الخاصة بهم من مزودي خدمة الإنترنت (ISPs)، الذين يقومون بتعيين عناوين IPv4 وIPv6 بطريقة هرمية. يتلقى مقدمو خدمات الإنترنت بدورهم تخصيصات عناوين IP من مجموعة متنوعة من المصادر، مثل سجل الإنترنت الإقليمي (RIR) أو سجلات الإنترنت الوطنية (NIRs) أو سجلات الإنترنت المحلية (LIRs).

تقع مسؤولية إدارة وتوزيع عناوين IP داخل مناطقها على عاتق RIRs. هذه RIRs، والتي تشمل AFRINIC لأفريقيا، وAPNIC لآسيا / المحيط الهادئ، وARIN لأمريكا الشمالية وبعض جزر الكاريبي، وLACNIC لأمريكا اللاتينية وبعض جزر الكاريبي، و RIPE

NCC لأوروبا والشرق الأوسط وآسيا الوسطى، هي المسؤولة لتخصيص عناوين IP على مستوى العالم. لضمان عدم تبديد تجمع عناوين IP المتاح، تعمل RIRs هذه جنبًا إلى جنب مع مزودي خدمة الإنترنت والمؤسسات الأخرى لإدارة توزيع عناوين IP. تلعب الطبيعة الهرمية لتخصيص عناوين IP دورًا مهمًا في ضمان تخصيص عناوين IP بكفاءة وفعالية، وأن يظل الإنترنت موثوقًا ويمكن الوصول إليه من قبل المستخدمين في جميع أنحاء العالم.

للاستفادة من الإمكانات الكاملة ل(IoT)، من الضروري تعيين معرفات وعناوين فريدة "للأشياء" المتصلة بالإنترنت. هذا يعني أن كل كائن أو جهاز يجب أن يكون له عنوان IP الخاص به ويجب أن يستخدم IP. ومع ذلك، فإن عدد عناوين IP الفريدة المطلوبة كبير نظرًا للعدد الكبير من الأجهزة التي سيتم توصيلها بالإنترنت. كان الحل لهذا التحدي هو تطوير إصدار IPv6 الجديد، والذي يستخدم عناوين ١٢٨ بت. يتيح هذا الأسلوب تخصيص عدد غير محدود تقريبًا من العناوين الفريدة للأجهزة، مما يضمن إمكانية تحديد كل "شيء" ومعالجته بشكل فريد. يعد استخدام IPv6 أمرًا بالغ الأهمية لنجاح (IoT)، حيث يضمن اتصال كل جهاز بالإنترنت ويمكنه التفاعل بسلاسة وكفاءة مع الأجهزة الأخرى. إن تحديد "الأشياء" ومعالجتها بشكل فريد هو مجرد خطوة أولى نحو إطلاق الإمكانات الكاملة ل(IoT)، ولكنه أساس حاسم يقوم عليه النظام بأكمله.

أجهزة الاستشعار والمحركات في (IoT)

(IoT) هي إحدى القوى الأساسية وراء اقتصاد البيانات الجديد. يمكن استخدام أنظمة (IoT) لمهام مثل الأتمتة التي لم تكن مخصصة لها في الأصل. هذا يرجع إلى القيمة المتزايدة للذكاء الذي ينتجه نظام (IoT). تنتج المستشعرات بيانات (IoT). بالإضافة إلى ذلك، يمكن أن تعمل مشغلات ومستشعرات (IoT) معًا لتوفير أتمتة على نطاق صناعي. أخيرًا، يمكن أن ينتج عن تحليل البيانات التي تنتجها هذه المستشعرات والمحركات بمرور الوقت معلومات تجارية ثاقبة.

التطورات الجديدة في علم المواد وتكنولوجيا النانو تدفع التقدم السريع لتكنولوجيا الاستشعار. نظرًا للتحسينات في الدقة والحجم والتكلفة، يمكن لأجهزة الاستشعار الآن قياس أو تحديد الأشياء التي لم تكن ممكنة من قبل. في الواقع، نظرًا لمدى سرعة تطور

تكنولوجيا الاستشعار، سنشهد نشر تريليون جهاز استشعار إضافي كل عام في غضون بضع سنوات.

المجسات/ المستشعرات

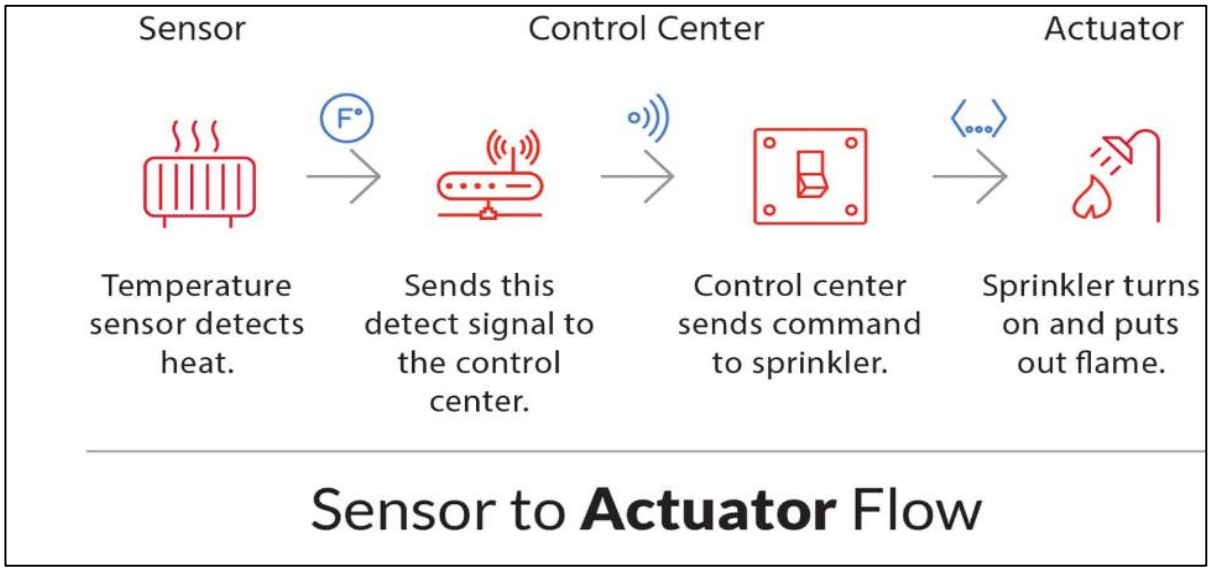
يُشار إلى المستشعر بشكل أكثر ملاءمة باسم محول الطاقة. يشار إلى أي عنصر مادي يحول أحد أشكال الطاقة إلى شكل آخر باسم محول الطاقة. نظرًا لأن النبضة الكهربائية تملي قراءة المستشعر، فإن محول الطاقة يحول ظاهرة فيزيائية إلى هذا الدافع. الميكروفون عبارة عن مستشعر يقوم بتحويل الطاقة الاهتزازية (الموجات الصوتية) إلى طاقة كهربائية بطريقة مفيدة بحيث يمكن لمكونات النظام الأخرى أن تتصل بالصوت الأصلي.

المحركات/ المشغلات

تُستخدم أنواع مختلفة من محولات الطاقة، مثل المشغلات، في العديد من أنظمة (IoT). ببساطة، يعمل المحرك على عكس المستشعر. يحول المدخلات الكهربائية إلى حركة من خلال الوسائل المادية. هناك العديد من أنواع المحركات المختلفة، بما في ذلك المحركات الكهربائية والأنظمة الهيدروليكية والأنظمة الهوائية.

المر اقب/ الموجه

قد يقوم المستشعر بجمع البيانات وإرسالها إلى مركز التحكم في إعداد تقليدي ل(IoT). هناك، الحكم يحكمه الأساس المنطقي السابق. لذلك، استجابة للإدخال المحسوس، يقوم الأمر المقابل بتشغيل مشغل. نتيجة لذلك، مع (IoT)، تتعاون أجهزة الاستشعار والمشغلات من نهايات متعارضة. لاحقًا، سنتطرق إلى مزيد من التفاصيل حول موقع مركز التحكم داخل نظام (IoT) الأكبر حجمًا.

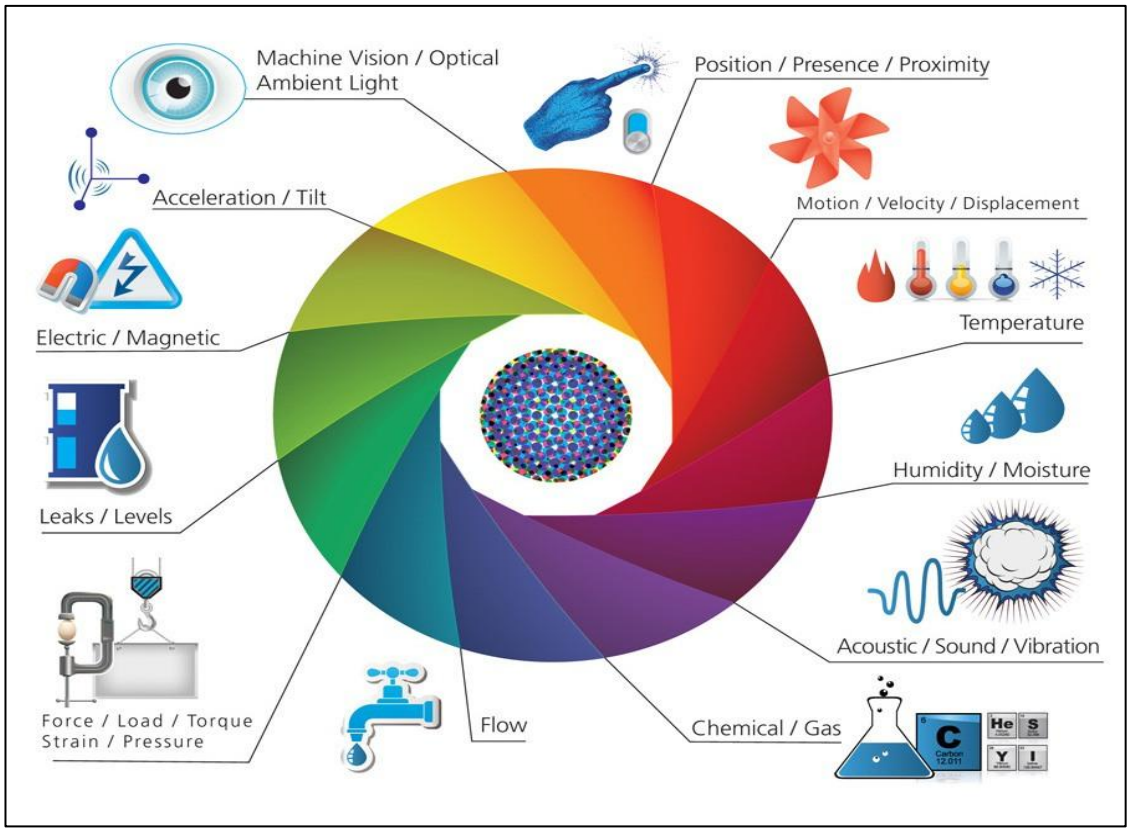


الاختلافات الهامة في (IoT)

في نظام (IoT)، هناك أنواع عديدة من أجهزة الاستشعار. تتضمن قائمة المستشعرات مستشعرات التدفق ومستشعرات درجة الحرارة ومستشعرات الجهد ومستشعرات الرطوبة والمزيد. بالإضافة إلى ذلك، هناك طرق مختلفة لقياس نفس

الشيء. المروحة الصغيرة، المشابهة لتلك الموجودة في محطة الطقس، هي إحدى طرق قياس تدفق الهواء. من ناحية أخرى، فإن استخدام هذه الطريقة للتعامل مع مركبة متحركة لن يكون عمليًا. في هذه الظروف، يمكن استخدام نهج مختلف، حيث تقيس السيارات تدفق الهواء عن طريق تسخين مكون صغير ومراقبة السرعة التي يبرد بها.

لأسباب مختلفة، هناك حاجة إلى طرق متعددة لقياس نفس الشيء. يمكن أن تحدث إجراءات متعددة بسبب متغير واحد في وقت واحد. نتيجة لذلك، يجب أن تعمل أجهزة الاستشعار والمحركات الخاصة بـ(IoT) معًا بشكل فعال.



أهمية أجهزة الاستشعار الدقيقة

لتتخيل بأنك تملك حانة تريد قياس تدفق البيرة من إحدى صنابيرك. تتمثل إحدى طرق تحقيق ذلك في تثبيت جهاز استشعار في الخط الذي يمتد من برميل البيرة إلى

الصنبور. يحتوي هذا المستشعر على الأرجح على دافع صغير. عندما مرت الجعة بجوار المستشعر، بدأت المكره في الدوران مثل مروحة محطة الطقس.

سوف يتلقى الكمبيوتر تياراً من الإشارات الكهربائية أثناء تدوير المكره. سيتم تحديد كمية البيرة المتدفقة من خلال تفسير الكمبيوتر للنبضات. سيبدو سهلاً، صحيح؟

في هذه المرحلة، تبدأ المستشعرات في الاهتمام. لم نحسب أبدًا كمية البيرة التي كانت تتدفق عبر المستشعر، كما يمكنك أن ترى ما إذا كنت ستعود وتقرأ شرحنا؛ بدلاً من ذلك، استنتجناه من تيار من النبضات الكهربائية. هذا يشير إلى أننا يجب أن نقرر كيفية تفسيره أولاً.

معايرة أجهزة الاستشعار

سنحتاج إلى استخدام حاوية بسعة حمل معروفة، مثل نصف لتر من الزجاج. سيتعين علينا بعد ذلك ملء الحاوية في ظل ظروف مختلفة لتحديد شكل إشارة النبض الكهربائي. يجب بعد ذلك مراقبة المشغل الذي يدير التدفق في الطرف الآخر عن طريق تشغيله وإيقاف تشغيله.

على سبيل المثال، قد تختلف قراءة صب من منتصف برميل يحتوي على بيرة فقط عن قراءة صب من أول صب من برميل جديد تمامًا، والذي قد يميل إلى الحصول على المزيد من الرغوة. بعد عدة محاولات وكمية كبيرة من البيانات، يمكننا فقط التأكد من أنه يمكننا تحليل البيانات. يمكن أن تعمل مشغلات ومستشعرات (IoT) معًا لأتمتة العمليات مثل ملء الزجاجة.

أهمية المعايرة الدقيقة

يمكن أن تضمن المنهجية قراءة المستشعر بشكل صحيح في جميع الأوقات بعد العثور على هذا الارتباط. هذه عملية معايرة. سيقدم المنتجون ذوو السمعة الطيبة منتجات تمت معايرتها بشكل صحيح ويتضمنون تعليمات حول كيفية إعادة المعايرة للتحقق من دقة المستشعر.

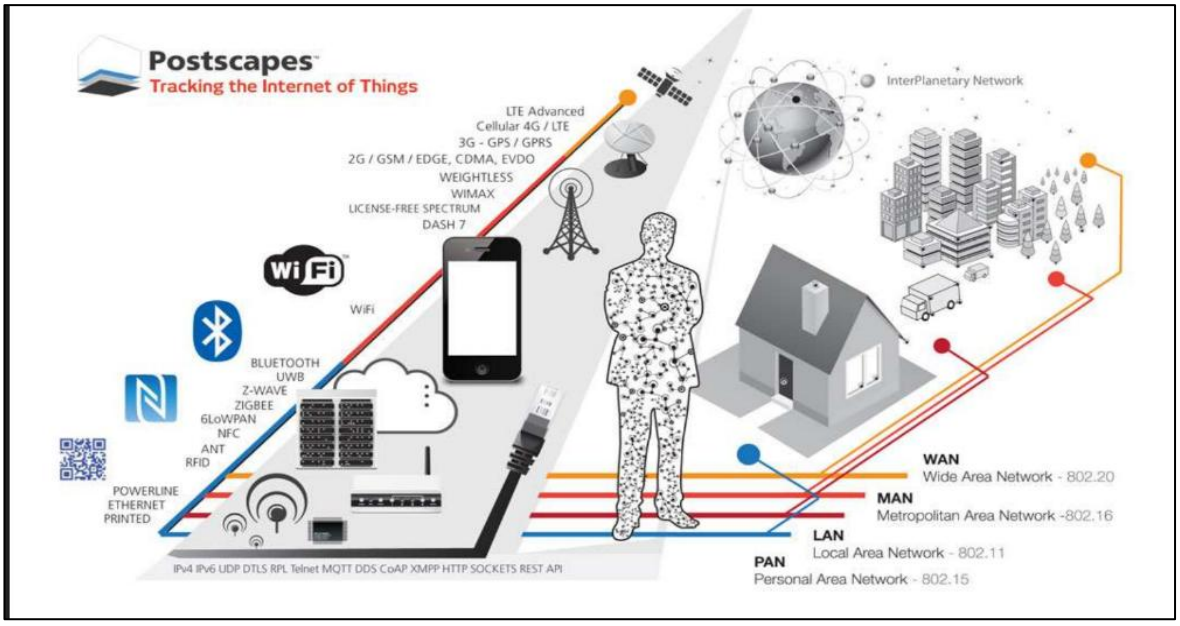
تعد دقة البيانات المستشعرة أمرًا ضروريًا لأنك ستؤسس قرارات مهمة للمهمة على التحليل اللاحق للبيانات، والتي ستكون عديمة الفائدة إذا كانت البيانات غير دقيقة.

تحديات جديدة => تقنيات جديدة

تربط تقنيات اتصال (IoT) بين العديد من الأشياء غير المتجانسة لتقديم خدمات ذكية معينة.

- عادةً، في مواجهة خطوط الاتصال المزعجة والفاقدة، يجب أن تعمل عقد (IoT) بطاقة منخفضة.
- يمكن التمييز بين فئتين رئيسيتين من أجهزة (IoT) وهما:
  - الموارد محدودة: الأجهزة التي تفتقر إلى الموارد اللازمة لدعم TCP / IP؛ على سبيل المثال، الأجهزة والأدوات التي تعتمد على وحدة التحكم الدقيقة.
  - الأجهزة الغنية بالموارد: تلك التي تمتلك الأجهزة والبرامج المطلوبة لدعم مجموعة بروتوكولات TCP / IP.
- التقييس / التشغيل البيني والتكامل:
  - يمكن اعتبار توحيد هندسة (IoT) كأساس لتعزيز المنافسة بين الشركات لإنتاج سلع عالية الجودة.
  - هناك حاجة إلى بروتوكولات جديدة لتوافق الاتصال بين الأشياء غير المتجانسة (الكائنات الحية، المركبات، الهواتف، الأجهزة، البضائع، إلخ).
- التوافر والموثوقية: يجب تطوير الأجهزة لتناسب متطلبات العملاء من حيث التوافر في أي مكان وزمان
- الإدارة والتكوين الذاتي: أمر بالغ الأهمية للتأكد من أن العملاء يتلقون خدمات عالية الجودة بأسعار في متناول الجميع.
- قابلية التوسع: يجب أن تأخذ العديد من البروتوكولات الأساسية في الاعتبار العدد الهائل من العناصر الحريصة على الاتصال بالإنترنت

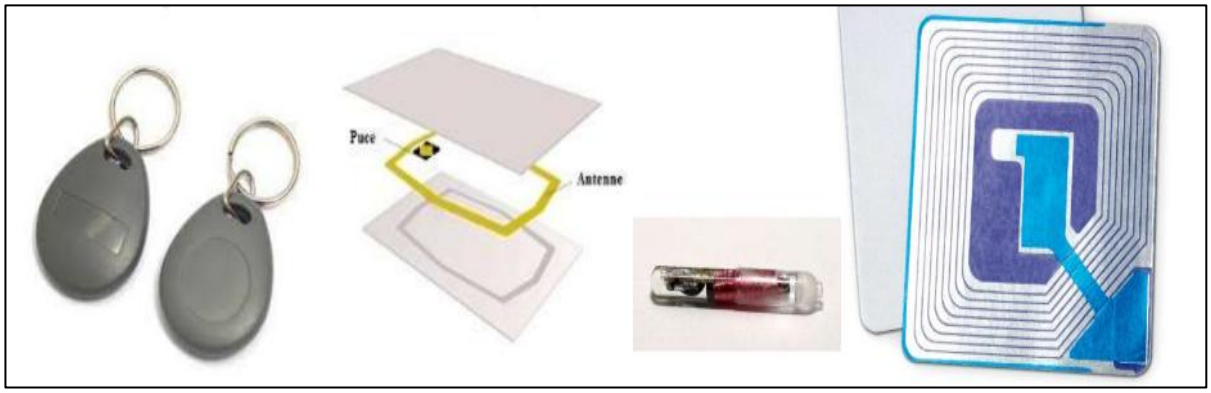
- جودة الخدمة: من المتوقع أن تساهم شبكات (IoT) في إدارة جودة الخدمة من خلال تحسين استخدام الموارد لجميع الأجهزة غير المتجانسة التي تشكل جزءًا من (IoT).
- الأمن والخصوصية: تثير شبكات (IoT) مخاوف أمنية جديدة يجب أخذها في الاعتبار في جميع طبقات (IoT)، بما في ذلك حماية البيانات داخل الأجهزة ذات الموارد المحدودة. نظرًا لأن خصوصية المستهلك حساسة جدًا، فإن الأمان والخصوصية مهمان في كل صناعة في جميع أنحاء العالم.
- استهلاك الطاقة: تعتبر مسألة استهلاك الطاقة نقطة حرجة في شبكات (IoT). عادةً ما تعتمد كفاءة عمل الأشياء الذكية على عمر البطارية.
- الأثر البيئي: سيؤدي العدد الهائل من الأجهزة المتصلة إلى إثارة مخاوف تتعلق بالبيئة والصحة. وبالتالي، أصبحت التكنولوجيا المتجددة أو الخضراء مجال بحث جذاب في تطور (IoT).



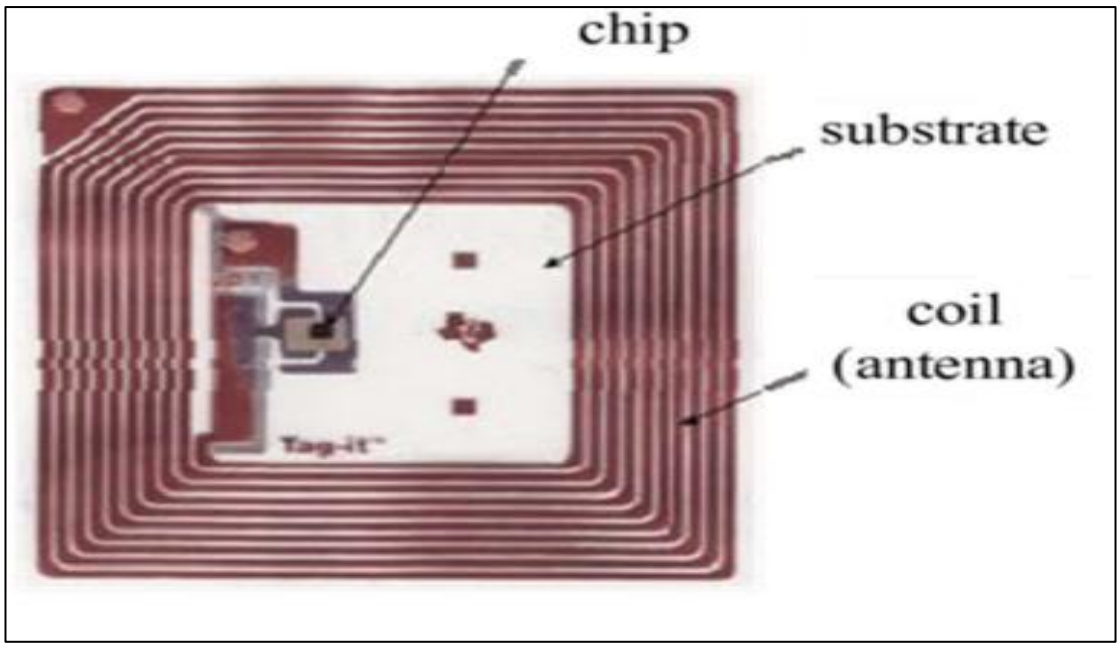
تحديد تردد الراديو RFID

هي تقنية أصبحت عامل تمكين رئيسي ل(IoT). إنه يعمل عن طريق استخدام مجال كهرومغناطيسي لتحديد وتعقب العلامات المرفقة بالكائنات تلقائيًا. يمكن أن تحتوي هذه العلامات على أنواع مختلفة من البيانات، مثل أرقام التعريف أو بيانات

الاستشعار، ويمكن إرفاقها بمجموعة واسعة من الكائنات، من السلع الاستهلاكية إلى المعدات الصناعية. تتكون أنظمة RFID من قارئ يرسل موجات راديو للتواصل مع العلامات والعلامات نفسها، والتي تستجيب لإشارة القارئ عن طريق إرسال بياناته إلى القارئ. أحدثت هذه التكنولوجيا ثورة في إدارة المخزون، ولوجستيات سلسلة التوريد، وتتبع الأصول، من بين تطبيقات أخرى، وهي تستعد للعب دور حاسم في تطوير (IoT).



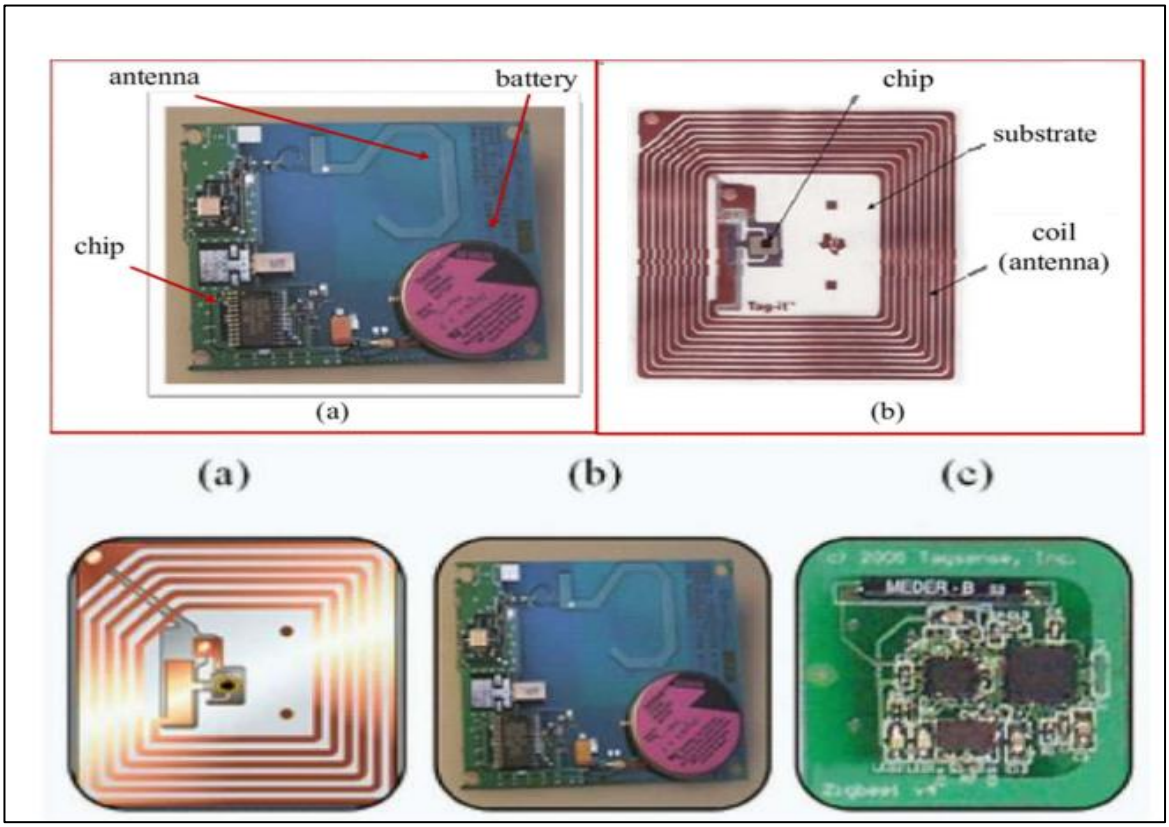
يعد جهاز إرسال واستقبال الإشارات الراديوية أو العلامة وقارئ العلامات هما الجزأين الرئيسيين لتقنية RFID. تتكون العلامة من مكونين رئيسيين: شريحة تحمل المعرف الفريد للكائن وهوائي يسمح للرقاقة بالتواصل باستخدام موجات الراديو مع قارئ العلامات. تستجيب العلامة لمجال تردد الراديو لقارئ العلامات عن طريق عكس موجات الراديو التي ترسل بيانات الكائن إلى القارئ. يقوم القارئ بعد ذلك بتفسير البيانات ومعالجتها حسب متطلبات التطبيق. لقد وجدت هذه التقنية تطبيقات واسعة النطاق في مختلف المجالات، بما في ذلك إدارة المخزون، وتتبع الأصول، ولوجستيات سلسلة التوريد، على سبيل المثال لا الحصر. إن قدرة نظام RFID على توفير معلومات في الوقت الفعلي وأتمتة تتبع الكائنات جعلت منه أحد الأصول القيمة في العديد من الصناعات.



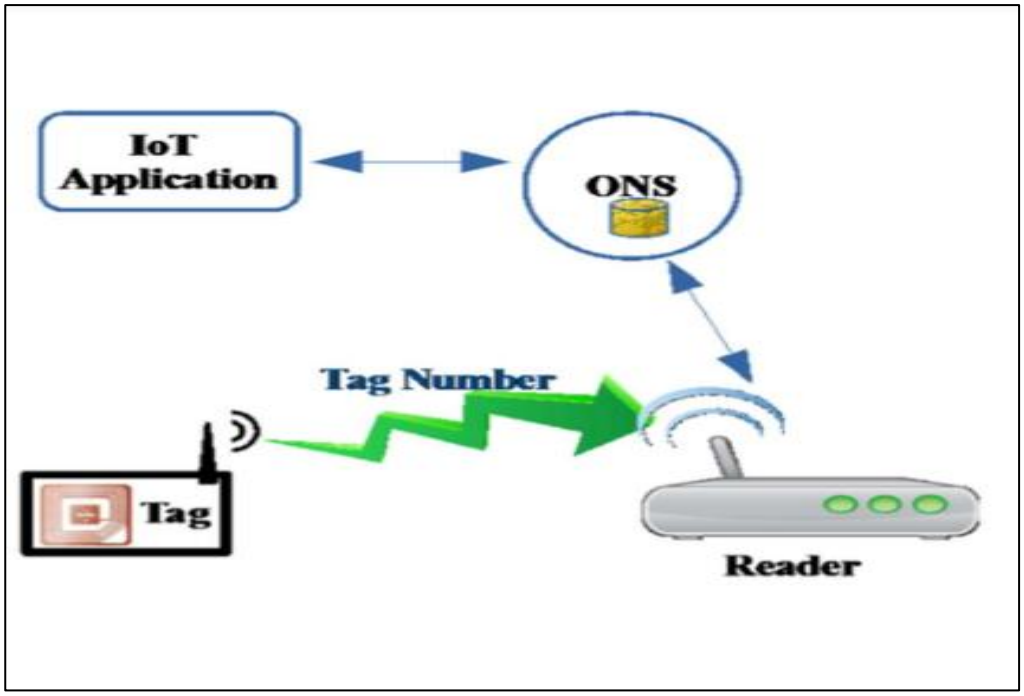
يعمل RFID في واحد من ثلاثة أوضاع: علامة سلبية أو علامة شبه سلبية أو علامة نشطة.

- العلامات السلبية هي أكثر أنواع علامات RFID أساسية واقتصادية. ليس لديهم مصدر طاقة داخلي ويعتمدون على الطاقة المنقولة من قارئ RFID لتشغيل شريحة العلامة وإرسال البيانات مرة أخرى إلى القارئ. العلامات الخاملة لها نطاق قراءة محدود ولا يمكن قراءتها إلا واحدة تلو الأخرى.
- العلامات شبه السلبية، والمعروفة أيضًا باسم العلامات السلبية المدعومة بالبطارية (BAP) لها مصدر طاقة داخلي، عادةً بطارية صغيرة، لتشغيل الشريحة وتمكين العلامة من بث إشارة على مدى أطول من العلامة السلبية. تُستخدم البطارية فقط لنقل الإشارة، ولا تزال العلامة تعتمد على طاقة قارئ RFID لتشغيل الشريحة لتخزين البيانات.
- من ناحية أخرى، تحتوي العلامات النشطة على مصدر طاقة خاص بها، وعادة ما يكون بطارية، لتشغيل شريحة العلامة ونقل البيانات إلى القارئ. تتمتع العلامات النشطة بمدى قراءة أطول ويمكنها نقل البيانات باستمرار، مما يجعلها مثالية لتتبع الكائنات في الوقت الفعلي أو في البيئات القاسية. ومع ذلك، فإن العلامات النشطة

أغلى ثمناً من العلامات السلبية أو شبه السلبية وتتطلب استبدال البطارية بشكل منتظم.

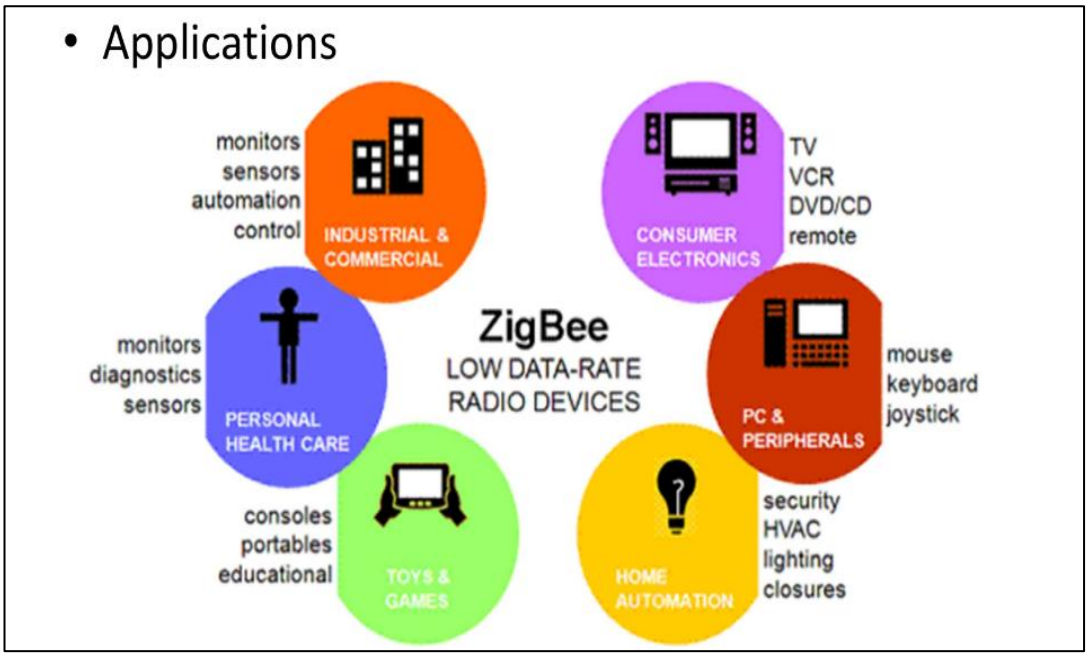


تعمل تقنية تحديد الترددات الراديوية (RFID) عن طريق إرسال رقم التعريف الفريد للعلامة إلى قارئ العلامات باستخدام موجات الراديو. يلتقط القارئ هذا الرقم ويمرره إلى تطبيق كمبيوتر معين يعرف باسم خدمات تسمية الكائنات (ONS). يعد ONS مسؤولاً عن البحث عن التفاصيل المرتبطة بالعلامة من قاعدة البيانات. تخزن قاعدة البيانات هذه المعلومات ذات الصلة بالعلامة، مثل متى وأين تم تصنيعها، وموقعها الحالي، وأي بيانات أخرى ذات صلة. بمجرد أن يسترد ONS تفاصيل العلامة من قاعدة البيانات، فإنه يرسل المعلومات مرة أخرى إلى القارئ، والتي يمكن استخدامها بعد ذلك بواسطة تطبيقات مختلفة لأغراض مختلفة، مثل تتبع المخزون، أو مصادقة المنتجات، أو مراقبة حركة البضائع من خلال سلسلة التوريد. أحدثت تقنية RFID ثورة في طريقة عمل الشركات، حيث وفرت رؤية في الوقت الفعلي لأصولها وتمكين إدارة الموارد بكفاءة وفعالية.



بصرف النظر عن RFID، هناك العديد من تقنيات الاتصالات اللاسلكية الأخرى المستخدمة بشكل شائع في مجال (IoT)، بما في ذلك Zigbee وBluetooth و - LoRa LoRaWAN وMQTT.

Zigbee هي تقنية اتصالات لاسلكية منخفضة الطاقة وقصيرة المدى مصممة خصيصًا لتطبيقات (IoT). يستخدم على نطاق واسع في أتمتة المنزل والإضاءة الذكية والأتمتة الصناعية.



تعتمد شبكة ZigBee على مكدس يتم تنفيذه على أجهزة ZigBee المنطقية. هناك ثلاثة أنواع من الأجهزة المنطقية في شبكة ZigBee المنسق، المعروف أيضًا باسم جهاز الوظيفة الكاملة أو (FFD، والموجه) المعروف أيضًا باسم جهاز الوظيفة الكاملة أو (FFD، والجهاز النهائي) المعروف أيضًا باسم جهاز الوظيفة المنخفضة.

يعد المنسق مكونًا مهمًا في شبكة ZigBee، وهناك دائمًا منسق واحد فقط لكل شبكة. المنسق مسؤول عن بدء الشبكة وصيانتها، وإدارة أمن الشبكة، والتحكم في الاتصال بين الأجهزة المختلفة داخل الشبكة. يعمل كمحور مركزي ويسهل التنسيق العام للشبكة.

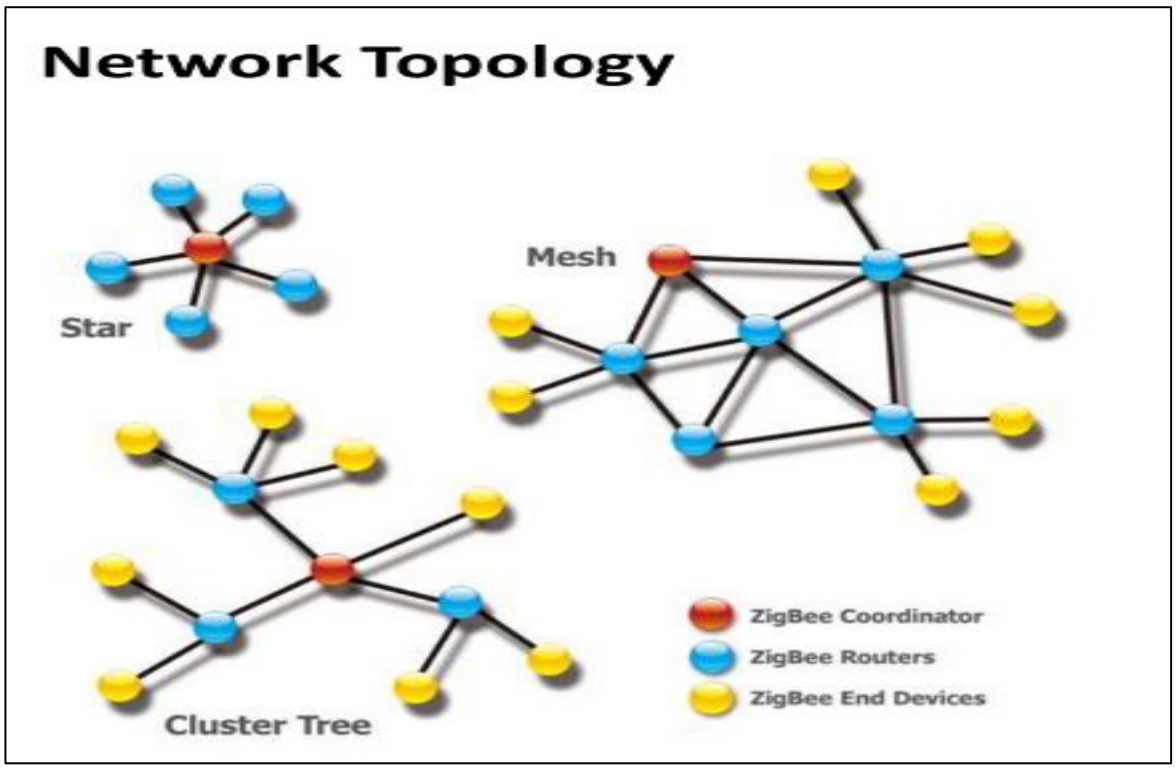
الموجهات هي نوع آخر من الأجهزة المنطقية في شبكة .ZigBee كما أنها تعمل كأجهزة كاملة الوظائف. (FFDs) تلعب أجهزة التوجيه دورًا أساسيًا في توسيع تغطية الشبكة وضمان اتصال موثوق بين الأجهزة. يمكنهم استلام وإعادة توجيه الرسائل من الأجهزة الأخرى، مما يسمح بالاتصال متعدد القفزات داخل الشبكة. تساعد أجهزة التوجيه في بناء بنية تحتية قوية وقابلة للتطوير للشبكة.

الأجهزة الطرفية، من ناحية أخرى، هي أجهزة ذات وظيفة منخفضة .(RFDs) تتمتع هذه الأجهزة بقدرات محدودة مقارنة بالمنسق وأجهزة التوجيه. تُصمم الأجهزة الطرفية عادةً لأداء مهام محددة، مثل جمع البيانات أو التحكم في وظائف معينة. يعتمدون على المنسق أو الموجهات لتسهيل اتصالاتهم داخل الشبكة.

يعتمد عدد أجهزة التوجيه والأجهزة الطرفية في شبكة ZigBee على متطلبات التطبيق المحددة وظروف الموقع الفعلي. يمكن تصميم الشبكة بأعداد متفاوتة من أجهزة التوجيه والأجهزة الطرفية لضمان التغطية المثلى والتواصل الفعال بناءً على احتياجات التطبيق. يعد وضع وتوزيع أجهزة التوجيه والأجهزة الطرفية داخل الشبكة من الاعتبارات الحاسمة لتحقيق اتصال موثوق وقوي.

توفر بنية شبكة ZigBee، مع المنسق والموجهات والأجهزة الطرفية، حلاً مرنًا وقابلًا للتطوير لمختلف التطبيقات التي تتطلب اتصالاً لاسلكيًا منخفض الطاقة. من خلال الاستفادة من المجموعة المناسبة من الأجهزة وتحسين وضعها، يمكن تصميم شبكات

ZigBee لتلبية متطلبات محددة، مما يتيح اتصالاً فعالاً وموثوقًا في مجموعة واسعة من السيناريوهات.



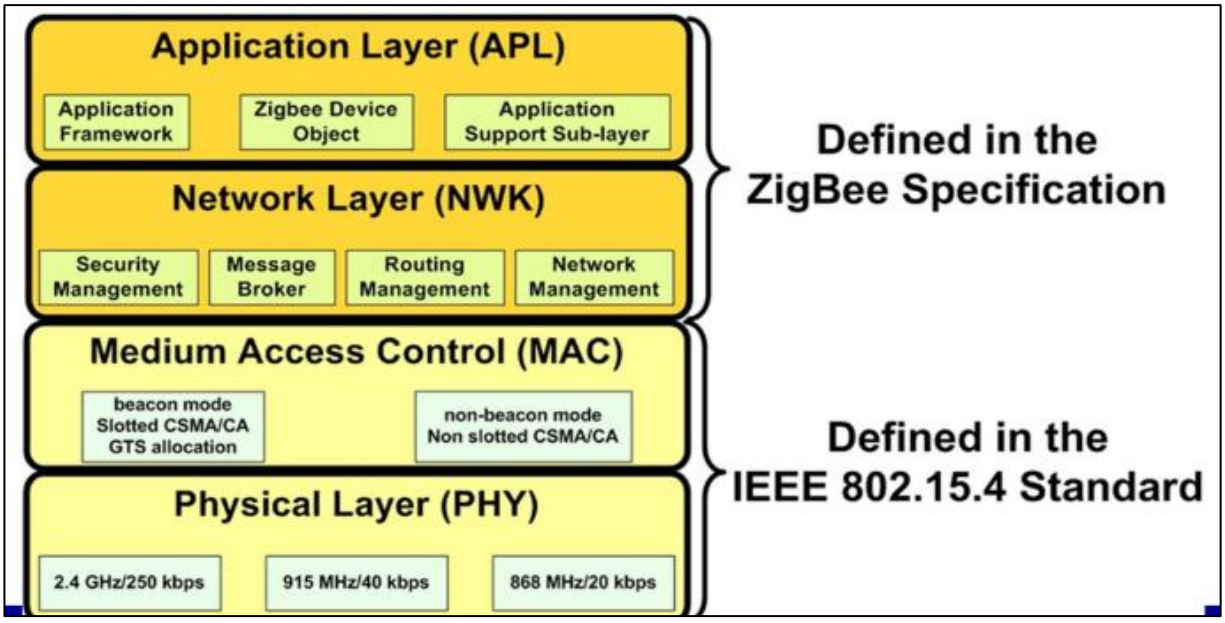
في سياق ZigBee، هناك ثلاثة أنواع رئيسية من الأجهزة المنطقية: المنسق والموجه والجهاز النهائي.

المنسق هو نوع جهاز منطقي ZigBee يلعب دورًا مهمًا في الشبكة. في شبكة ZigBee، يوجد دائمًا منسق واحد فقط. يتحمل هذا الجهاز المسؤولية الفريدة لإنشاء شبكة المنطقة الشخصية اللاسلكية (WPAN) وإدارة عمليات الشبكة. يبدأ الشبكة ويخصص عناوين للأجهزة الأخرى ويتحكم في الاتصال الكلي داخل الشبكة.

جهاز التوجيه هو نوع آخر من الأجهزة المنطقية في شبكات .ZigBee تمتلك أجهزة التوجيه القدرة على توجيه الرسائل من عقدة إلى أخرى، مما يتيح الاتصال متعدد القفزات. يعملون كوسطاء ويساعدون في توسيع تغطية الشبكة عن طريق إعادة توجيه الرسائل بين الأجهزة. تعد أجهزة التوجيه ضرورية لإنشاء بنية تحتية قوية وقابلة للتطوير للشبكة.

الجهاز النهائي هو مصطلح ZigBee يستخدم لوصف الأجهزة التي تفتقر إلى القدرة على التوجيه. يمكن لهذه الأجهزة إرسال واستقبال المعلومات لاستخدامها الخاص فقط. في شبكة شجرة العنقود، يعمل الجهاز النهائي كعقدة طرفية، مما يعني أنه لا يتحمل أي مسؤولية عن توجيه الرسائل إلى الأجهزة الأخرى. في هيكل الشبكة النجمية، تعتبر جميع العقد باستثناء المنسق أجهزة طرفية. من ناحية أخرى، لا تتضمن الشبكة المعشقة الكاملة عادةً أي أجهزة نهائية، على الرغم من أن التصميمات العملية قد تتضمن واحدًا أو أكثر منها بناءً على متطلبات محددة.

باختصار، المنسق مسؤول عن إنشاء شبكة ZigBee، بينما تعمل أجهزة التوجيه على تمكين توجيه الرسائل بين الأجهزة. يمكن للأجهزة الطرفية، بقدراتها المحدودة، الاتصال فقط لأغراضها الخاصة والعمل كعقد طرفية أو أجهزة فردية داخل الشبكة. يتيح الجمع بين أنواع الأجهزة المنطقية هذه إنشاء شبكات ZigBee مرنة وقابلة للتطوير وفعالة تلبي العديد من تطبيقات الخدمات الذكية و(IoT).



تحدد مواصفات ZigBee طبقتين رئيسيتين للمكدس: طبقة الشبكة (NWK) وطبقة إطار عمل التطبيق.

تعد طبقة الشبكة (NWK) مسؤولة عن إدارة الوظائف المتعلقة بالشبكة في شبكة ZigBee. تعالج هذه الطبقة مهام مثل بدء الشبكات والانضمام إليها ومغادرتها واكتشافها. عند إنشاء شبكة ZigBee، يلعب المنسق دورًا حيويًا. يقوم بإجراء مسح للطاقة لتحديد قناة التردد اللاسلكي بأفضل جودة للشبكة الجديدة. بمجرد اختيار القناة، يقوم المنسق بتعيين معرف شبكة منطقي، يُعرف باسم معرف PAN (معرف شبكة المنطقة الشخصية). يتم تطبيق معرف PAN هذا على جميع الأجهزة التي تنضم إلى الشبكة، مما يضمن التنسيق والاتصال داخل الشبكة.

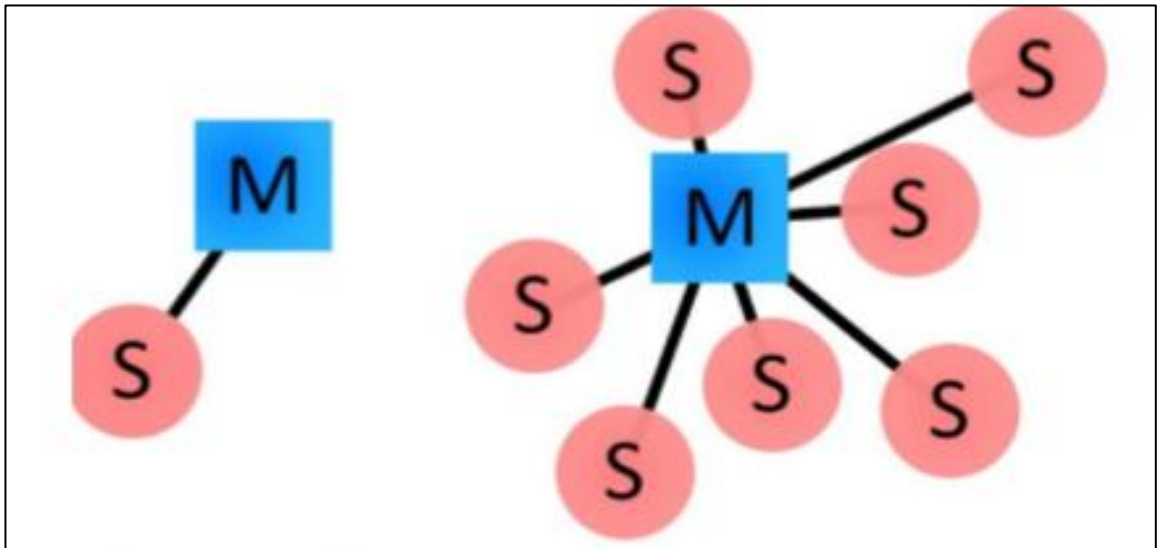
في شبكة ZigBee، من الشائع أن يتم تشغيل المنسقين والموجهات بالتيار الكهربائي، مما يعني أنهم يتلقون الطاقة من مأخذ كهربائي أو مصدر طاقة مستمر. تحتوي هذه الأجهزة على مصدر طاقة أكثر استقرارًا، مما يسمح لها بالتعامل مع تنسيق الشبكة ومهام التوجيه بشكل فعال. من ناحية أخرى، غالبًا ما تعمل الأجهزة الطرفية، مثل أجهزة الاستشعار أو المشغلات، بالبطارية. لديهم موارد طاقة محدودة ومصممة للحفاظ على الطاقة. يمكن للأجهزة الطرفية التي تعمل بالبطارية المشاركة في الشبكة ولكن عادةً ما يكون لها وظائف أقل واستهلاك أقل للطاقة لإطالة عمر بطاريتها.

يتيح استخدام المنسقين والموجهات التي تعمل بالتيار الكهربائي، جنبًا إلى جنب مع الأجهزة الطرفية التي تعمل بالبطارية، لشبكة ZigBee تحقيق التوازن بين إدارة الشبكة الفعالة والحفاظ على الطاقة. يسمح هذا المزيج بنشر أجهزة (IoT) اللاسلكية مع متطلبات طاقة متفاوتة وتحسين الأداء العام للشبكة.

بالمختصر، تتكون ZigBee stack من طبقة الشبكة (NWK) وطبقة إطار عمل التطبيق. تتعامل طبقة NWK مع الوظائف المتعلقة بالشبكة، بما في ذلك إنشاء الشبكة والانضمام إليها والتنسيق. يعد اختيار قناة التردد اللاسلكي وتعيين معرف PAN من المهام الهامة التي يقوم بها المنسق في هذه الطبقة. يضمن التمييز بين المنسقين / أجهزة التوجيه التي تعمل بالتيار الكهربائي والأجهزة الطرفية التي تعمل بالبطارية النشر الفعال والمرن لشبكات ZigBee التي تلبي متطلبات الطاقة المختلفة في تطبيقات (IoT).

ZigBee Network Layer Function	Coordinator	Router	End Device
Establish a ZigBee network	.		
Permit other devices to join or leave the network	.	.	
Assign 16-bit network addresses	.	.	
Discover and record paths for efficient message delivery	.	.	
Discover and record list of one-hop neighbors	.	.	
Route network packets	.	.	
Receive or send network packets	.	.	.
Join or leave the network	.	.	.
Enter sleep mode			.

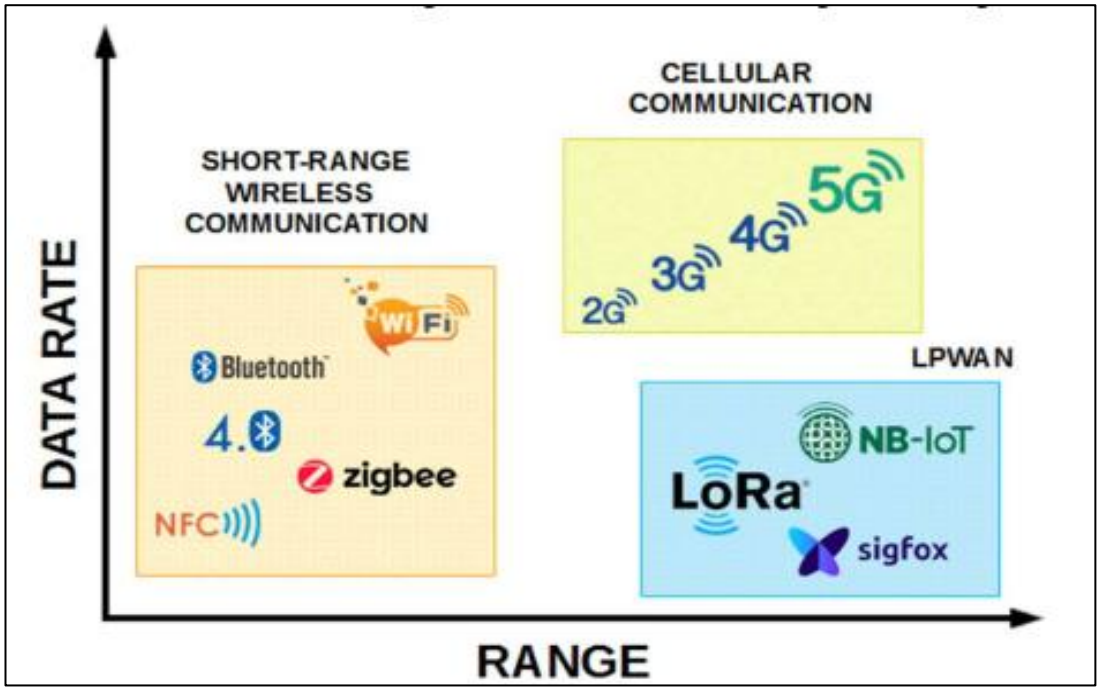
Bluetooth هي تقنية لاسلكية شائعة أخرى تستخدم للاتصال قصير المدى بين الأجهزة. يتم استخدامه على نطاق واسع لتدفق الصوت اللاسلكي وسماعات الرأس اللاسلكية ولوحات المفاتيح والفأرات اللاسلكية. تعمل تقنية البلوتوث في وضعين: السيد والعبد، ويمكن أن تشكل شبكة بيكونيت تتكون مما يصل إلى سبعة من العبيد النشطين.



Examples of Bluetooth master/slave piconet topologies.

LoRa و LoRaWAN هي بروتوكولات اتصال لاسلكية تتيح الاتصال بعيد المدى بين أجهزة (IoT). يستخدمون شبكات واسعة النطاق منخفضة الطاقة (LPWAN) لإرسال

حزم صغيرة من البيانات عبر مسافات طويلة. LoRa هي تقنية الطبقة المادية ، بينما LoRaWAN هو بروتوكول الاتصال الذي يمكّن أجهزة LoRa من الاتصال بالإنترنت.



لبروتوكول LoRaWAN وبنية الشبكة تأثير كبير على جوانب مختلفة من أداء الشبكة. يلعبون دورًا مهمًا في تحديد عمر البطارية للعقد الفردية داخل الشبكة. من خلال تحسين بروتوكولات الاتصال وتنفيذ آليات توفير الطاقة، تهدف LoRaWAN إلى إطالة عمر بطارية الأجهزة، مما يجعلها مناسبة لعمليات النشر والتطبيقات طويلة الأجل التي تتطلب الحد الأدنى من الصيانة.

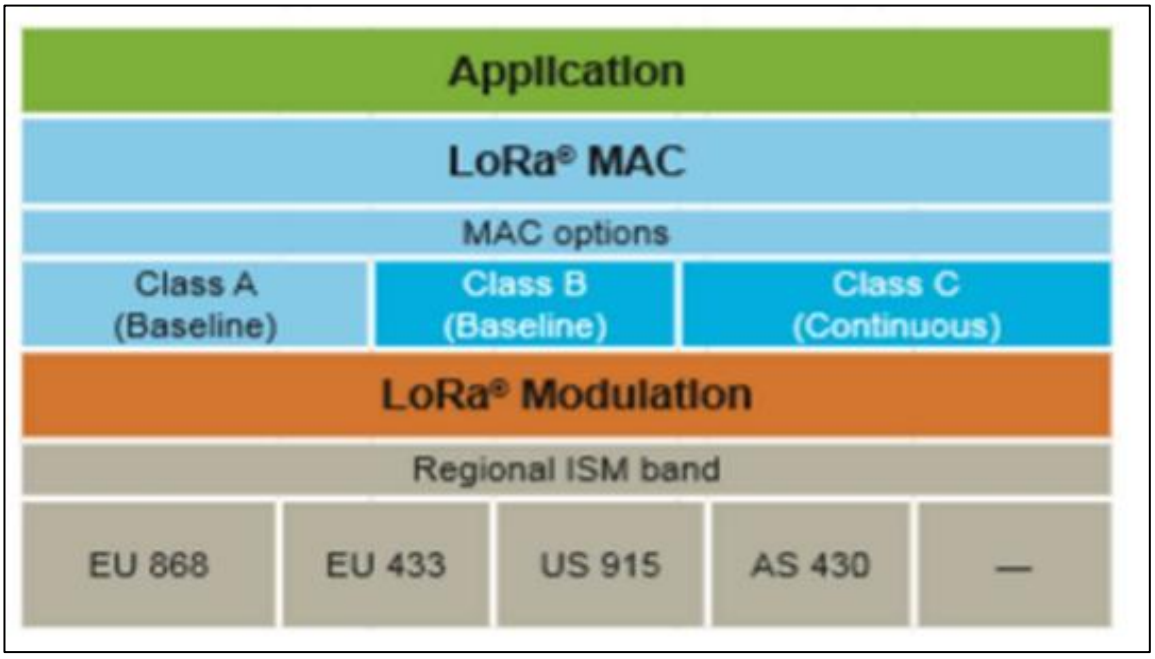
علاوة على ذلك، يؤثر البروتوكول وبنية الشبكة على سعة الشبكة، مما يسمح بالاتصال المتزامن لعدد كبير من الأجهزة. يدعم LoRaWAN عمليات النشر القابلة للتطوير، مع استيعاب كثافة عالية من العقد داخل الشبكة مع الحفاظ على كفاءة الاتصال وتخصيص الموارد.

جودة الخدمة هي اعتبار رئيسي آخر يتأثر ببروتوكول LoRaWAN وبنية الشبكة. يضمن التصميم اتصالًا موثوقًا به حتى في البيئات الصعبة، مع القدرة على التعامل مع التداخل وتوهين الإشارة والعوامل الأخرى التي تؤثر على جودة الارتباط اللاسلكي. يتم تنفيذ آليات جودة الخدمة لتحديد أولويات نقل البيانات الحرجة وتحسين أداء الشبكة.

يعد الأمان جانبًا مهمًا في أي شبكة، وتتضمن LoRaWAN إجراءات أمنية قوية. يتضمن البروتوكول آليات التشفير والمصادقة وحماية التكامل لحماية البيانات المنقولة عبر الشبكة، ومنع الوصول غير المصرح به وضمان خصوصية المعلومات الحساسة.

بالإضافة إلى أنه يتم تحديد تنوع وتنوع التطبيقات التي تخدمها شبكة LoRaWAN بواسطة البروتوكول وبنية الشبكة. تدعم LoRaWAN مجموعة واسعة من تطبيقات (IoT)، بما في ذلك المدن الذكية والزراعة وتتبع الأصول والمراقبة الصناعية. تسمح مرونة البروتوكول بتخصيص معلمات الاتصال ومعدلات البيانات لتلائم متطلبات التطبيق المختلفة.

باختصار، يوفر بروتوكول LoRaWAN، جنبًا إلى جنب مع الطبقة المادية LoRa، حلاً شاملاً للاتصالات طويلة المدى منخفضة الطاقة في شبكات (IoT). يؤثر البروتوكول وبنية الشبكة بشكل كبير على عمر بطارية الأجهزة، وسعة الشبكة، وجودة الخدمة، والأمن، والقدرة على خدمة مجموعة متنوعة من التطبيقات. من خلال تحسين هذه الجوانب، يتيح LoRaWAN اتصالًا موثوقًا وفعالًا عبر مسافات طويلة، مما يدعم نطاقًا واسعًا من عمليات نشر (IoT).

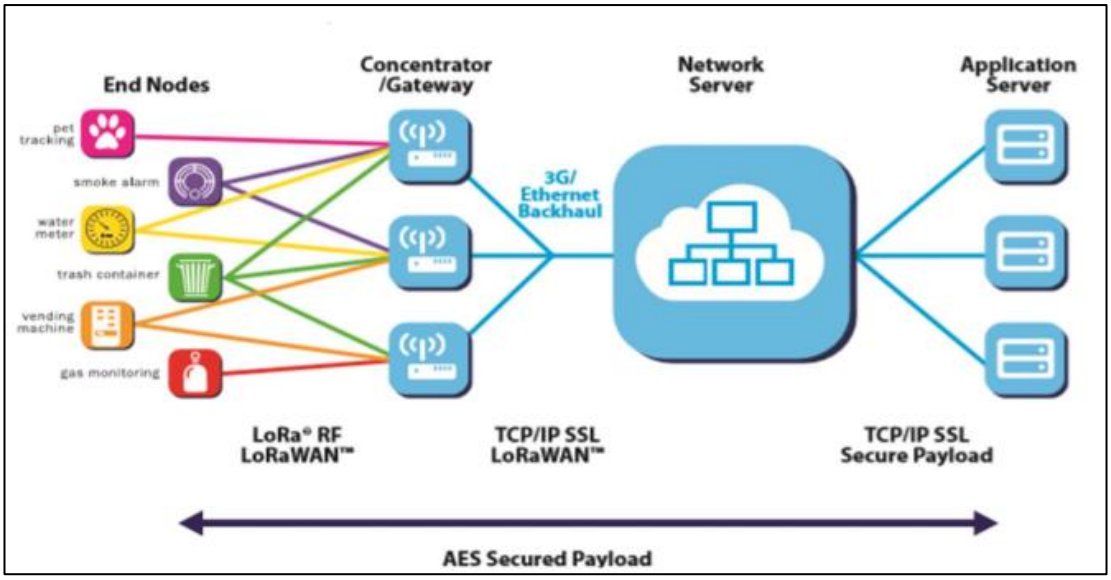


يعتمد اختيار بنية نجمية بعيدة المدى لشبكات LoRaWAN على عدة اعتبارات. في حين أن الهيكل الشبكي يمكن أن يزيد من النطاق، فإنه يقدم أيضًا تعقيدات ومقايضات تجعل العمارة النجمية أكثر ملاءمة في العديد من السيناريوهات.

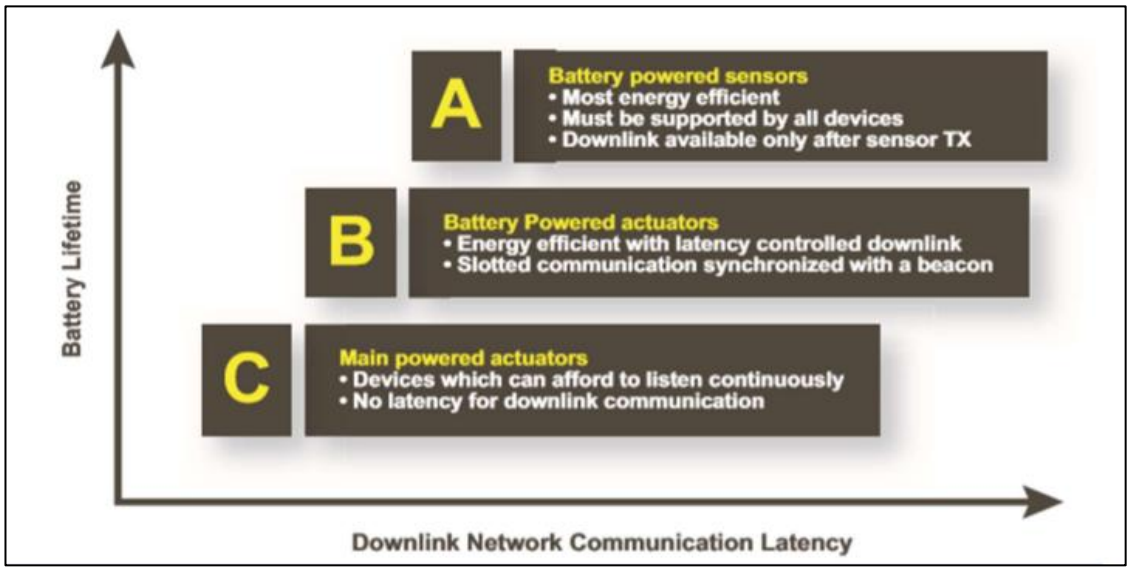
في العمارة النجمية، تتصل جميع الأجهزة الطرفية مباشرة ببوابة مركزية، وتشكل مسار اتصال من قفزة واحدة. توفر هذه البساطة مزايا من حيث سعة الشبكة وعمر البطارية والكفاءة الإجمالية. يحتاج كل جهاز طرفي فقط إلى إرسال البيانات إلى البوابة، مما يقلل عمليات الإرسال غير الضرورية ويقلل من استهلاك الطاقة. هذا مفيد بشكل خاص للأجهزة التي تعمل بالبطاريات، حيث يمكنها توفير الطاقة وتحقيق عمر تشغيلي أطول.

في المقابل، يقدم الهيكل الشبكي قفزات إضافية، حيث تتلقى العقد المعلومات وتعيد توجيهها من العقد الأخرى. بينما يمكن للشبكات المعشقة أن توسع النطاق نظريًا من خلال السماح للعقد الوسيطة بترحيل البيانات، فإن هذا يأتي على حساب زيادة التعقيد وانخفاض سعة الشبكة. يجب أن تؤدي كل عقدة في الشبكة المعشقة وظائف التوجيه، وتستهلك طاقة إضافية، ويحتمل أن تؤدي إلى زمن انتقال في عملية الاتصال. علاوة على ذلك، يمكن أن يؤدي النقل الزائد للمعلومات غير ذات الصلة عن طريق العقد الوسيطة إلى زيادة التأثير على كفاءة الشبكة والأداء العام.

من خلال اعتماد بنية نجمية، تعمل شبكات LoRaWAN على تبسيط مسار الاتصال، مما يتيح استخدامًا أكثر كفاءة للموارد وتعزيز سعة الشبكة الإجمالية. كما أنه يقلل من تعقيد الشبكة، مما يسهل نشرها وإدارتها وصيانتها. يجعل التعقيد المنخفض والاستهلاك الأمثل للطاقة في بنية النجوم مناسبة بشكل خاص لسيناريوهات الاتصالات بعيدة المدى حيث يتم نشر الأجهزة منخفضة الطاقة على مساحة واسعة.



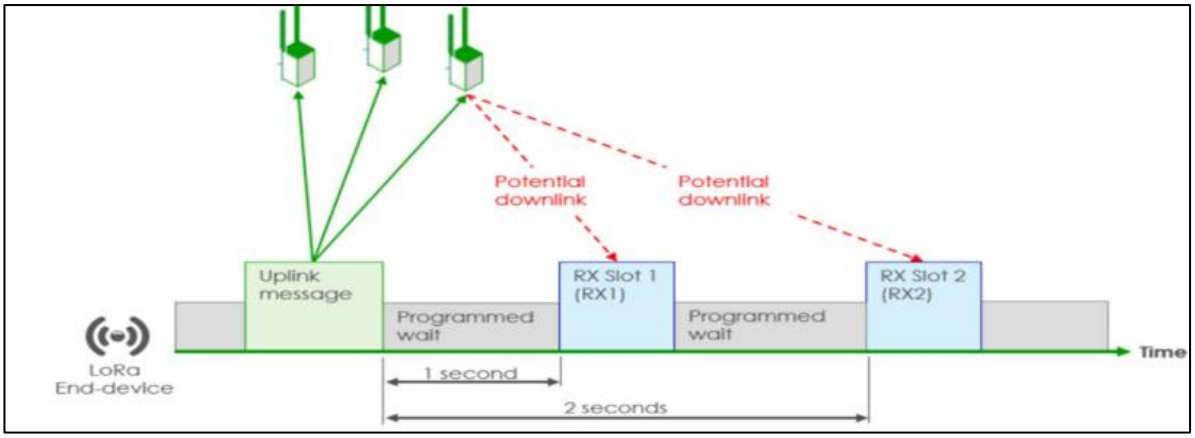
لتحسين ملفات تعريف التطبيقات النهائية المتنوعة، تستخدم LoRaWAN فئات مختلفة من الأجهزة، وهي A وB و C. تعمل فئات الأجهزة هذه على تحقيق التوازن بين زمن انتقال اتصال الوصلة الهابطة للشبكة وعمر البطارية.



الفئة A هي فئة الجهاز الافتراضية في LoRaWAN ، وتستخدم عادةً لأجهزة الاستشعار أو المشغلات التي تعمل بالبطارية. في الفئة أ، يعمل الجهاز في دورة حيث تتبع كل رسالة من رسائل الوصلة الصاعدة فتحتا استقبال لرسائل الوصلة الهابطة. أثناء فتحات الاستقبال هذه، يستمع الجهاز إلى عمليات الإرسال المحتملة للوصلة الهابطة من الشبكة.

بعد رسالة الارتباط الصاعد، يدخل الجهاز في وضع السكون للحفاظ على طاقة البطارية حتى نافذة الاستقبال التالية للوصلة الصاعدة أو الهابطة. تساعد فترة السكون هذه على إطالة عمر بطارية الجهاز. من المهم ملاحظة أن الشبكة يمكنها إرسال رسالة ارتباط فقط عندما يستيقظ الجهاز من وضع السكون. يتم تشغيل حدث التنبيه هذا من خلال حدث على الجهاز، مثل الوصول إلى عداد الوقت أو عتبة جهاز الاستشعار.

توفر فئة الجهاز من الفئة أ توازنًا بين زمن انتقال الاتصال وعمر البطارية. يعطي الأولوية لاتصالات الإرسال، مما يسمح للأجهزة بنقل البيانات بوتيرتها الخاصة مع الحفاظ على الطاقة أثناء فترات السكون. ومع ذلك، يمكن أن يعاني اتصال الوصلة الهابطة من زمن انتقال نظرًا لأنه يعتمد على تنشيط الجهاز وإنشاء فتحات استقبال بعد إرسال الوصلة الصاعدة.



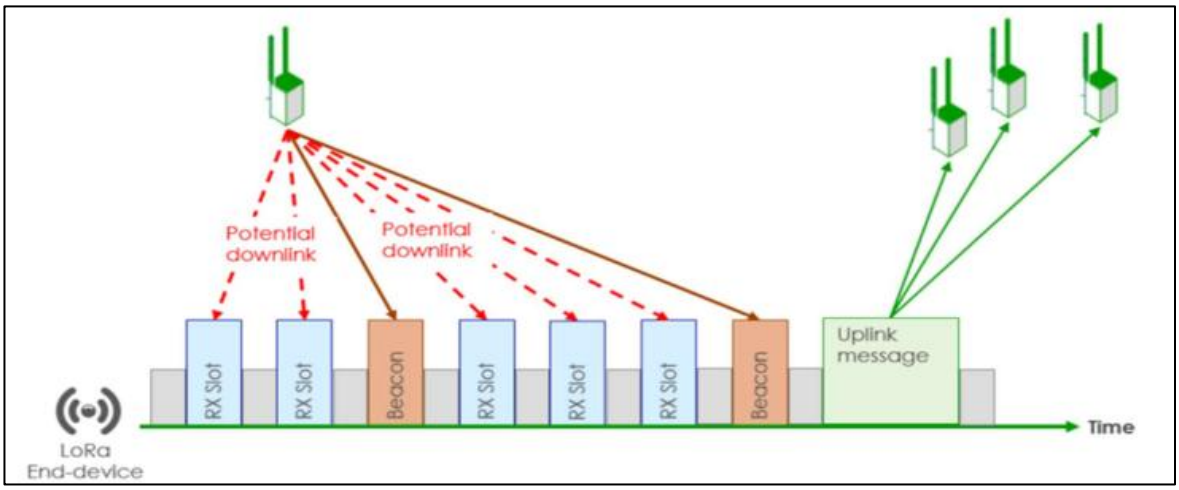
الفئة B، والمعروفة أيضًا باسم فئة Beacon، هي فئة جهاز بديلة في LoRaWAN تعتمد على وظائف الفئة A. بالإضافة إلى نوافذ الاستقبال العشوائية في الفئة A، تفتح أجهزة الفئة B نوافذ استقبال إضافية في المواعيد المحددة.

لتمكين نوافذ الاستلام المجدولة، يتلقى الجهاز النهائي منارة متزامنة مع الوقت من البوابة. يسمح هذا المرشد للجهاز بمحاذاة نافذة الاستلام الخاصة به مع الوقت المجدول الذي تحدده الشبكة. من خلال مزامنة نوافذ الاستلام، يعرف الخادم بدقة متى يستمع الجهاز من الفئة B بنشاط لرسائل الوصلة الهابطة.

توفر إضافة نوافذ الاستلام المجدولة في الفئة B زمن انتقال محسّن للوصلة الهابطة مقارنة بالفئة أ. فهي تسمح بتسليم رسائل الوصلة الهابطة بشكل أكثر قابلية للتنبؤ وفي الوقت المناسب إلى الجهاز. هذا مفيد بشكل خاص للتطبيقات التي تتطلب اتصالات أكثر تكرارا أو حساسة للوقت من الشبكة إلى الجهاز النهائي.

ومع ذلك، من المهم ملاحظة أن نوافذ الاستلام المجدولة في الفئة ب لا تزال تعمل ضمن القيود العامة لاستهلاك طاقة الجهاز وعمر البطارية. سيظل الجهاز يدخل في وضع السكون بين نوافذ الاستقبال للحفاظ على الطاقة.

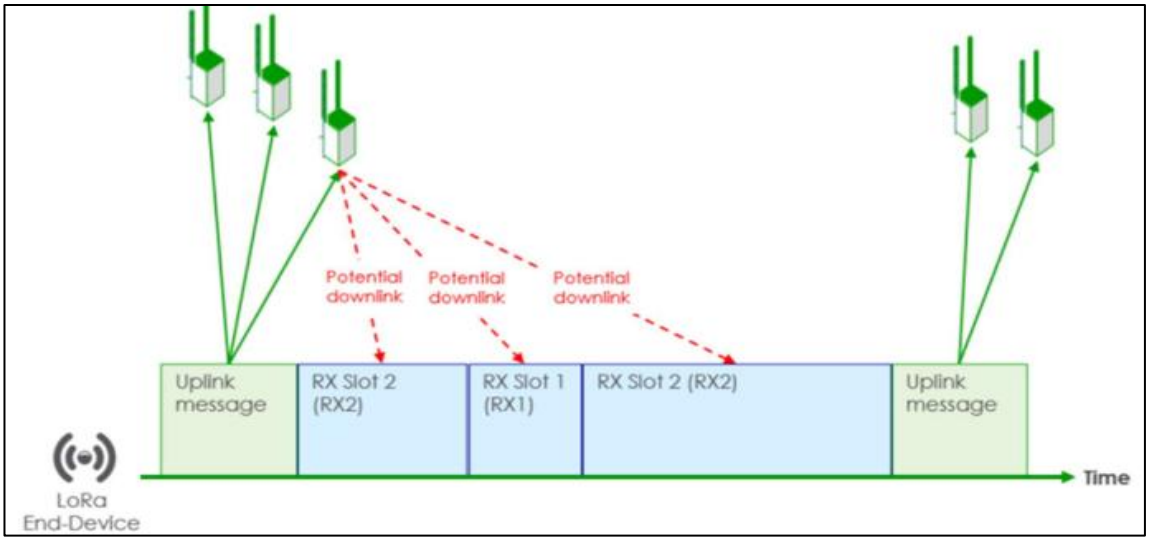
تعتبر الفئة B مناسبة للتطبيقات التي يكون فيها زمن انتقال الوصلة الهابطة عاملاً حاسمًا ويتطلب اتصالًا منتظمًا من الشبكة إلى الجهاز النهائي على فترات زمنية محددة. يوفر توازنًا بين زمن الوصول وكفاءة الطاقة من خلال دمج نوافذ الاستقبال المتزامنة في تشغيل الجهاز.



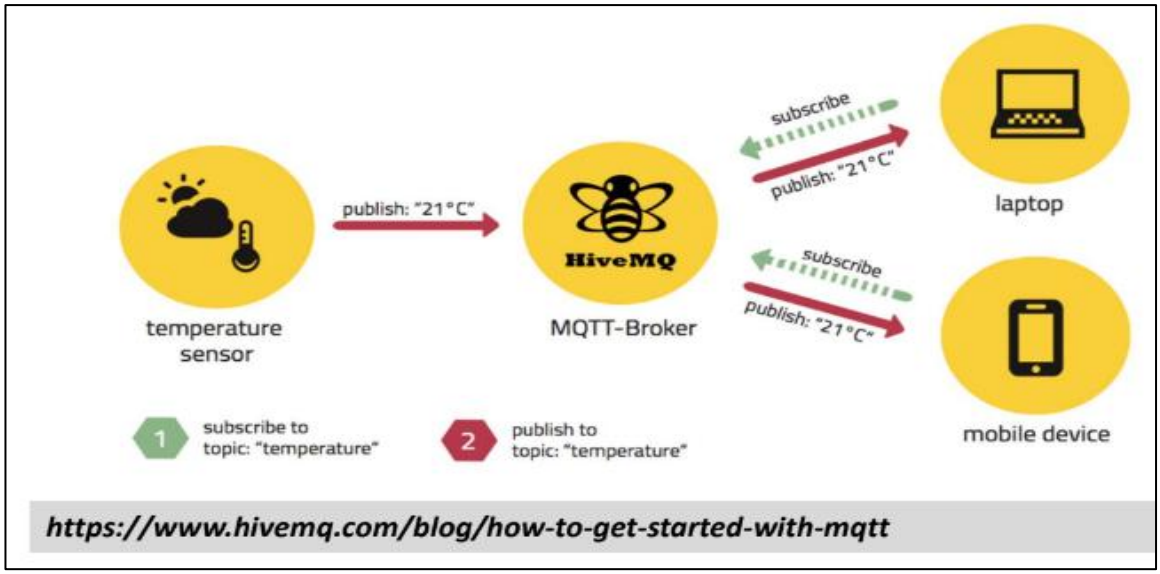
الفئة C هي فئة جهاز أخرى في LoRaWAN ، تُعرف بالفئة المستمرة. على عكس الفئة A والفئة B ، تم تصميم أجهزة الفئة C للاستماع باستمرار لرسائل الوصلة الهابطة ، حتى عندما لا تكون في نافذة الاستلام. يأتي هذا التوافر المستمر لرسائل الوصلة الهابطة على حساب الاستهلاك العالي للطاقة، مما يجعل أجهزة الفئة C مناسبة للسيناريوهات التي يتم فيها تشغيلها بالتيار الكهربائي بدلاً من الاعتماد على طاقة البطارية.

دائمًا ما تكون أجهزة الفئة C نشطة وجاهزة لتلقي رسائل الوصلة الهابطة من الشبكة، مما يوفر اتصالًا بزمن انتقال منخفض للتطبيقات الحساسة للوقت. تسمح إمكانية الاستماع المستمر هذه بالاستجابة الفورية للأوامر أو التحديثات التي ترسلها الشبكة. ومع ذلك، نظرًا لاستهلاك الطاقة المستمر المرتبط بالاستماع المستمر، يتم توصيل أجهزة الفئة C عادةً بمصدر طاقة رئيسي لضمان التشغيل دون انقطاع.

تعتبر فئة الجهاز من الفئة C مناسبة للتطبيقات التي يكون فيها الاتصال في الوقت الفعلي أو القريب من الوصلة الهابطة أمرًا بالغ الأهمية. تُستخدم هذه الأجهزة بشكل شائع في السيناريوهات التي يكون فيها مصدر الطاقة متاحًا بسهولة، مثل مراقبة البنية التحتية أو الأتمتة الصناعية أو تطبيقات المدن الذكية. يتيح التوفر المستمر لرسائل الوصلة الهابطة إجراء اتصال ثنائي الاتجاه فعال وفوري بين الشبكة وأجهزة الفئة C.



MQTT (النقل عن بُعد لوضع الرسائل في قائمة الانتظار) هو بروتوكول مراسلة يُستخدم بشكل شائع لتطبيقات (IoT) لتمكين الاتصال بين الأجهزة والتطبيقات. إنه بروتوكول خفيف الوزن وفعال يمكنه التعامل مع شبكات النطاق الترددي المنخفض والكمون العالي، مما يجعله مثاليًا لتطبيقات (IoT) التي تتطلب استهلاكًا منخفضًا للطاقة واتصالات بيانات في الوقت الفعلي.



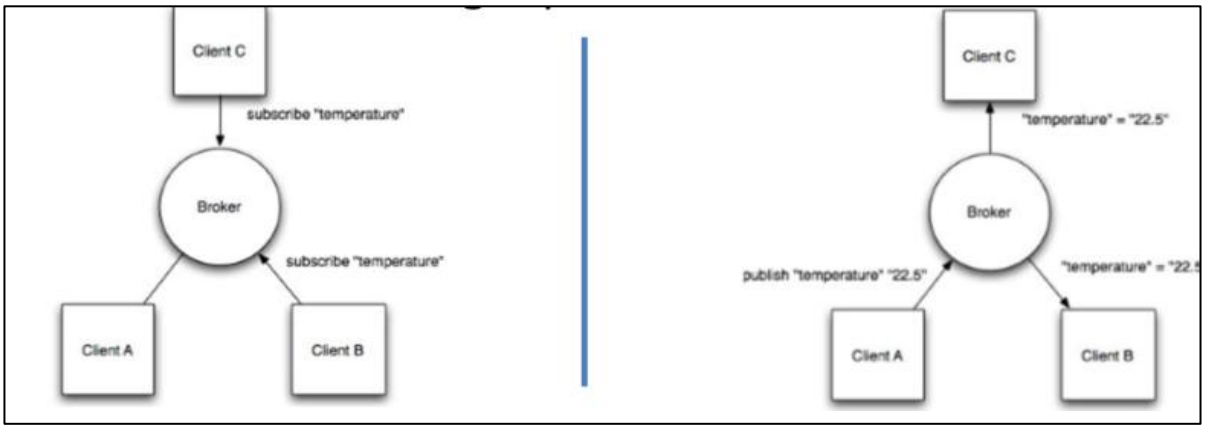
(MQTT) هو بروتوكول مراسلة خفيف الوزن شائع الاستخدام في (IoT) والاتصال من آلة إلى آلة. تتبع نمط رسائل النشر / الاشتراك، والذي يتيح الاتصال المستند إلى الحدث عن طريق دفع الرسائل إلى العملاء.

في نموذج النشر / الاشتراك الخاص بـ MQTT ، هناك مكونان رئيسيان: الناشرون والمشتركون. يتحمل الناشرون مسؤولية إرسال الرسائل إلى موضوع معين، بينما يعبر المشتركون عن اهتمامهم بموضوعات محددة من خلال الاشتراك فيها. يعمل وسيط MQTTكوسيط بين الناشرين والمشتركين، مما يسهل تسليم الرسائل.

عندما يرسل العميل (الناشر) رسالة إلى وسيط MQTT بموضوع معين، يتلقى الوسيط الرسالة ويضمن وصولها إلى جميع العملاء المشتركين (المشتركين) الذين أعربوا عن اهتمامهم بهذا الموضوع. يسمح هذا الفصل بين الناشرين والمشتركين بنموذج اتصال مرن وقابل للتطوير. الناشرون غير مدركين لهوية وعدد المشتركين، ولا يحتاج المشتركون إلى معرفة التفاصيل الخاصة بالناشرين. يدير الوسيط توجيه الرسائل وتسليمها بناءً على اشتراكات الموضوع.

من خلال الاشتراك في موضوع معين، يشير العملاء (المشتركون) إلى اهتمامهم بتلقي الرسائل المتعلقة بهذا الموضوع. عندما يتم نشر رسالة إلى موضوع يطابق اشتراك العميل، يضمن وسيط MQTT تسليم الرسالة إلى العميل. يتيح ذلك تسليم الرسائل بشكل فعال ومستهدف بناءً على اهتمامات واحتياجات المشتركين.

يعد نموذج النشر / الاشتراك في MQTT مناسبًا تمامًا للأنظمة التي تعتمد على الأحداث، حيث يحتاج العملاء إلى تلقي التحديثات أو الإخطارات في الوقت المناسب. يسمح بالاتصال غير المتزامن وفي الوقت الفعلي بين الأجهزة والأنظمة المختلفة بطريقة فعالة وقابلة للتطوير.



MQTTهي بنية تتيح حلولًا قابلة للتطوير بدرجة كبيرة من خلال توفير نموذج اتصال منفصل بين منتجي البيانات ومستهلكي البيانات. في قلب هذه البنية يوجد وسيط MQTT، والذي يعمل كنقطة اتصال مركزية.

وسيط MQTT مسؤول عن تسهيل تبادل الرسائل بين المرسلين (الناشرين) والمستلمين (المشتركين). يقوم عملاء MQTT ، سواء كانوا من منتجي البيانات أو المستهلكين ، بإنشاء اتصال TCP دائم مع الوسيط. يسمح هذا الاتصال المستمر بتسليم الرسائل بشكل فعال وفي الوقت الحقيقي.

تتمثل إحدى المزايا الرئيسية لـ MQTT في قدرتها على التعامل مع اتصال الشبكة المتقطع. إذا انقطع اتصال العميل بالوسيط MQTT ، فيمكن للوسيط تخزين الرسائل المخصصة لهذا العميل مؤقتًا. عندما يعيد العميل الاتصال بالوسيط، يتم تسليم الرسائل المخزنة مؤقتًا إلى العميل. تضمن هذه الميزة تسليم الرسائل بشكل موثوق حتى في المواقف التي يكون فيها اتصال الشبكة غير مستقر.

مثال على وسيط MQTT هو Eclipse Mosquitto ، وهو تطبيق مفتوح المصدر لبروتوكول .MQTT تشتهر Mosquitto بطبيعتها خفيفة الوزن وتوافقها مع العديد من الأجهزة، بدءًا من أجهزة الكمبيوتر ذات اللوحة الواحدة منخفضة الطاقة إلى الخوادم الكاملة. تم ترخيصه بموجب Eclipse Public License (EPL) و Eclipse Distribution License (EDL)، مما يجعله خيارًا شائعًا لتنفيذ الحلول المستندة إلى.MQTT

تتيح الطبيعة المنفصلة لبنية MQTT ودور الوسيط حلولاً مرنة وقابلة للتطوير بدرجة كبيرة. يمكن لمنتجي البيانات والمستهلكين العمل بشكل مستقل، مما يسمح بالإضافة أو الإزالة الديناميكية للأجهزة دون التأثير على النظام ككل. إن قابلية التوسع هذه، جنبًا إلى جنب مع موثوقية تسليم الرسائل وتنوع وسطاء MQTT مثل Eclipse Mosquitto، تجعل MQTT خيارًا شائعًا ل(IoT) وسيناريوهات الاتصال الأخرى في الوقت الفعلي.

في MQTT ، الموضوع عبارة عن سلسلة تستخدم لتصنيف وتنظيم الرسائل ضمن نموذج النشر / الاشتراك. يمكن أن تحتوي الموضوعات على مستويات متعددة من التسلسل الهرمي، مفصولة بشرطة مائلة (/). على سبيل المثال، يمكن أن يكون الموضوع "المنزل / غرفة النوم / درجة الحرارة"، مما يشير إلى بيانات درجة الحرارة في غرفة نوم المنزل.

لتسهيل أنماط الاشتراك المرنة، يدعم MQTT أحرف البدل لاشتراكات الموضوعات. علامة الجمع (+) عبارة عن حرف بدل أحادي المستوى، مما يسمح بقيم عشوائية في مستوى واحد من التسلسل الهرمي. على سبيل المثال، قد يطابق الاشتراك في "المنزل / + / درجة الحرارة" موضوعات مثل "المنزل / غرفة النوم / درجة الحرارة" أو "المنزل / المطبخ / درجة الحرارة"، ولكن ليس "المنزل / غرفة النوم / الرطوبة".

للاشتراك في مستويات متعددة، بما في ذلك جميع مستويات التسلسل الهرمي الأساسية، يوفر MQTT حرف البدل متعدد المستويات (#). على سبيل المثال، قد يطابق الاشتراك في "# / home" مواضيع مثل "المنزل / غرفة النوم / درجة الحرارة" أو "المنزل / غرفة النوم / الرطوبة" أو "المنزل / المطبخ / الإضاءة"، حيث إنه يلتقط جميع الموضوعات التي تبدأ بكلمة "المنزل" وأي مستويات لاحقة.

توفر أحرف البدل هذه مرونة في اشتراكات الموضوعات، مما يسمح للعملاء بتلقي الرسائل من مستويات محددة من التسلسل الهرمي أو حتى عبر مستويات متعددة. يتيح ذلك التصفية الفعالة وتسليم الرسائل بناءً على الاحتياجات المحددة لعملاء.MQTT

يوفر هيكل الموضوع واستخدام أحرف البدل في MQTT آلية قوية لتنظيم الرسائل والاشتراك فيها، مما يسمح بالتحكم الدقيق في استهلاك البيانات في نظام النشر / الاشتراك.

MQTT وHTTP كلاهما بروتوكولات اتصال ولكنهما يخدمان أغراضًا مختلفة ولهما خصائص مميزة. فيما يلي بعض الاختلافات الرئيسية بينهما:

١ .المواصفات MQTT :لها مواصفات قصيرة نسبيًا، تتكون من أنواع الرسائل الأساسية مثلCONNECT و PUBLISH و SUBSCRIBE و UNSUBSCRIBE و .DISCONNECTفي المقابل، تعد مواصفات HTTP أكثر شمولاً وتشمل طرقًا ورموز حالة مختلفة للاتصال بين الخادم والعميل.

٢ .رأس الرسالة وحجم الحزمة: تستخدم MQTT رأس رسالة مضغوطًا، مما ينتج عنه أحجام حزم أصغر. يبلغ الحد الأدنى لحجم رسالة الحزمة في MQTT 2 بايت فقط، مما يجعلها أكثر كفاءة من حيث استخدام النطاق الترددي. من ناحية أخرى، يحتوي HTTPعلى رأس رسالة أكثر أهمية، مما يؤدي إلى أحجام حزم أكبر.

٣ .الإنتاجية وأداء الشبكة: تم تصميم MQTT ليكون خفيف الوزن ومُحسّن لشبكات منخفضة الطاقة وعرض النطاق الترددي المنخفض. في بعض بيئات الشبكة، مثل شبكات الجيل الثالث، وجد أن MQTT لديها إنتاجية أعلى بكثير مقارنة ببروتوكول .HTTPأظهرت القياسات أن MQTT أسرع بما يصل إلى ٩٣ مرة من HTTP في شبكات الجيل الثالث، ويرجع ذلك أساسًا إلى تنسيق الرسالة الفعال وتقليل النفقات العامة.

٤ .نموذج الاتصال: تتبع MQTT نموذج اتصال دائم، حيث يقوم العملاء بإنشاء وصيانة اتصالات طويلة الأمد مع الوسيط. يقلل هذا الأسلوب من النفقات العامة لإنشاء اتصال جديد لكل رسالة ويتيح الاتصال في الوقت الفعلي والمدفوع بالأحداث. في

المقابل، يتبع HTTP نموذج استجابة الطلب، حيث يبدأ العملاء طلبًا إلى الخادم لكل تفاعل، مما يؤدي إلى زيادة الحمل والكمون المحتمل.

٥. حالات الاستخدام: يتم استخدام MQTT بشكل شائع في سيناريوهات (IoT) والاتصال من آلة إلى آلة، حيث يكون النطاق الترددي المنخفض، وانخفاض استهلاك الطاقة، والرسائل في الوقت الفعلي أو شبه الحقيقي أمرًا بالغ الأهمية. إنه مناسب تمامًا للتطبيقات مثل المراقبة عن بُعد والقياس عن بُعد والتشغيل الآلي للمنزل. من ناحية أخرى، يستخدم HTTP على نطاق واسع للتطبيقات المستندة إلى الويب، حيث يعد نموذج الطلب والاستجابة والوظائف الغنية التي توفرها طرق HTTP (GET و POST و PUT و DELETE وما إلى ذلك) ضرورية.

باختصار، لدى MQTT وHTTP مبادئ تصميم مختلفة وتستهدف حالات استخدام مختلفة. تتفوق MQTT في سيناريوهات النطاق الترددي المنخفض والطاقة المنخفضة، مما يوفر رسائل خفيفة الوزن مع استخدام فعال للشبكة. HTTP ، بمواصفاته الشاملة ، أكثر تنوعًا ويستخدم على نطاق واسع لمختلف التطبيقات المستندة إلى الويب. يعتمد الاختيار بين MQTT وHTTP على المتطلبات المحددة للتطبيق، بما في ذلك عوامل مثل حجم الرسالة وظروف الشبكة والاحتياجات في الوقت الفعلي وقيود استهلاك الطاقة.

مستوى جودة الخدمة (QoS) في بروتوكولات المراسلة، مثل MQTT، هو اتفاق بين مرسل الرسالة ومتلقيها يحدد مستوى الضمان لتسليم الرسالة. هناك ثلاثة مستويات لجودة الخدمة متوفرة في MQTT، يقدم كل منها مستويات مختلفة من الموثوقية وضمان التسليم.

QoS 0 ، والمعروف أيضًا باسم "مرة واحدة على الأكثر" ، هو أدنى مستوى من جودة الخدمة المتوفرة في .MQTT إنه يوفر نهج تسليم بأفضل جهد دون أي ضمان لتسليم الرسائل. فيQoS 0 ، لا يقر مستلم الرسالة باستلامها، ولا يقوم المرسل بتخزين الرسالة أو إعادة إرسالها.

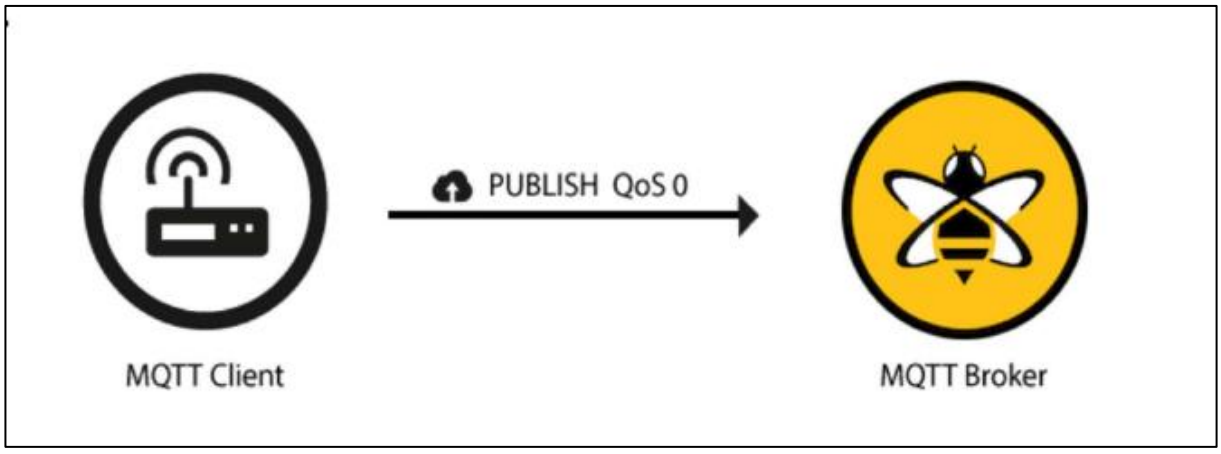
معQoS 0 ، يتم التعامل مع الرسالة بشكل أساسي على أنها عملية "Fire and forget".بمجرد أن ينشر المرسل الرسالة، يتم إرسالها إلى المستلمين المقصودين، ولكن

لا يتم اتخاذ أي إجراءات أخرى لضمان نجاح تسليمها أو إقرارها. إذا فشلت الرسالة في الوصول إلى وجهتها أو فقدت أثناء الإرسال، فلن يتم إعادة إرسالها.

غالبًا ما تتم مقارنة QoS 0 ببروتوكول TCP (بروتوكول التحكم في الإرسال) الأساسي، وهو بروتوكول طبقة النقل الذي يستخدمه .MQTT مثل TCP ، تعمل QoS 0 على أساس أفضل جهد، دون أي آليات موثوقية واضحة.

بينما توفر QoS 0 أقل ضمان لتسليم الرسائل، إلا أنها لا تزال مفيدة في السيناريوهات التي يكون فيها فقدان الرسائل العرضي أو عدم التسليم مقبولاً. إنه يوفر أقل مقدار من النفقات العامة والكمون مقارنة بمستويات جودة الخدمة الأعلى، مما يجعله مناسبًا للتطبيقات التي يتم فيها إعطاء الأولوية لبيانات الوقت الفعلي أو شبه الحقيقي على التسليم المضمون.

ومع ذلك، من المهم ملاحظة أنه يجب استخدام QoS 0 بحذر في المواقف التي تكون فيها موثوقية الرسالة وضمان التسليم أمرًا بالغ الأهمية. في مثل هذه الحالات، يجب مراعاة مستويات جودة الخدمة الأعلى، مثل QoS 1 أو QoS 2، لضمان المستوى المطلوب من الموثوقية وتأكيد تسليم الرسالة.



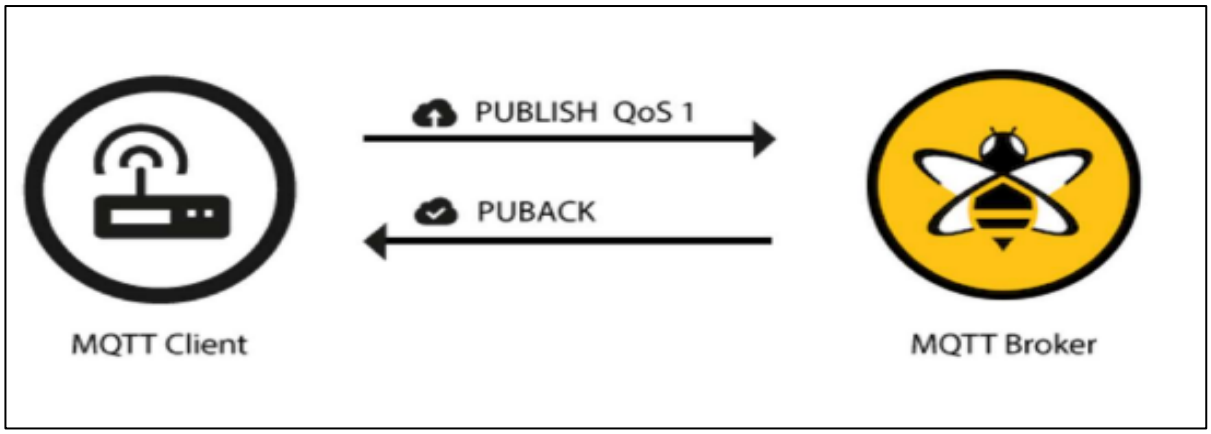
QoS 1 ، المعروف أيضًا باسم "مرة واحدة على الأقل" ، هو مستوى أعلى من جودة الخدمة في MQTT يضمن تسليم الرسالة إلى المستلم مرة واحدة على الأقل. باستخدام QoS 1، يقوم مرسل الرسالة بتخزين الرسالة حتى يتلقى حزمة PUBACK (نشر إقرار) من جهاز الاستقبال، مما يشير إلى استلام الرسالة بنجاح.

عندما يتم نشر رسالة باستخدام1 QoS ، يحتفظ المرسل بنسخة من الرسالة حتى يتلقى حزمة .PUBACK إذا لم يستلم المرسل PUBACK خلال إطار زمني محدد، فإنه يفترض أن الرسالة لم يتم تسليمها بنجاح ويعيد إرسالها. تضمن هذه الآلية تسليم الرسالة إلى المتلقي، حتى لو تطلبت عدة محاولات.

نظرًا لإمكانية تسليم الرسائل المتعددة، فمن الضروري للتطبيقات التعامل مع التكرارات المحتملة ومنع الآثار الجانبية غير المقصودة. على سبيل المثال، قد يحتاج التطبيق المستلم إلى إزالة تكرار الرسائل أو تنفيذ عمليات غير فعالة لضمان بقاء معالجة الرسائل متسقة.

توفر QoS 1 مستوى أعلى من الموثوقية مقارنة بـ0 QoS ، لأنها تضمن تسليم رسالة واحدة على الأقل إلى جهاز الاستقبال. ومع ذلك، فإنه لا يضمن تسليم الرسالة مرة واحدة فقط. هذا يعني أنه في بعض السيناريوهات، قد يتلقى المتلقي رسائل مكررة، ويحتاج التطبيق المستلم إلى التعامل معها وفقًا لذلك.

تعد QoS 1 مناسبة للتطبيقات التي تكون فيها موثوقية تسليم الرسائل مهمة، ويمكن معالجة الرسائل المكررة في بعض الأحيان دون آثار ضارة. إنه يحقق توازنًا بين الموثوقية والكفاءة، مما يوفر مستوى أعلى من الضمان مقارنة بـ QoS 0 مع تقليل النفقات العامة المرتبطة بأعلى مستوى QoS، QoS 2.



QoS 2 هو أعلى مستوى من جودة الخدمة في MQTT ، ويقدم أقوى ضمان لتسليم الرسائل. مع QoS 2، يتلقى المستلمون المقصودون كل رسالة مرة واحدة فقط.

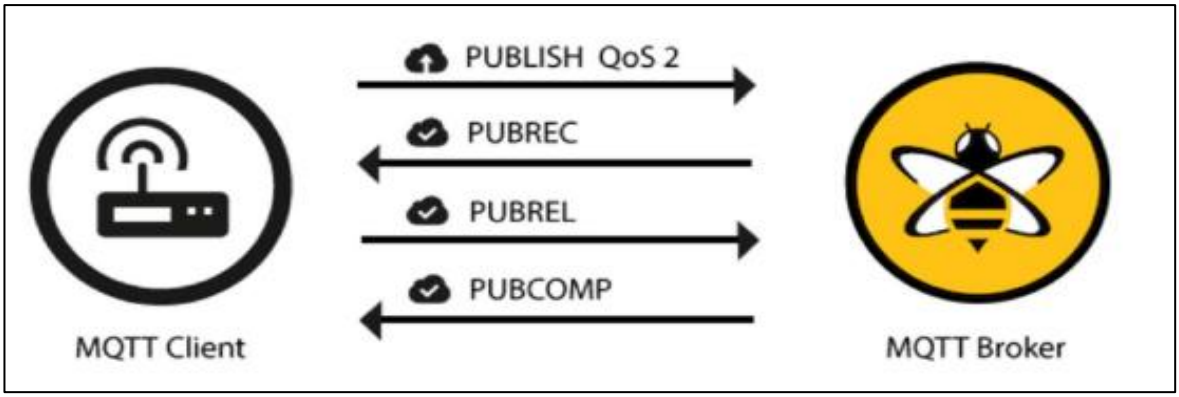
توفر QoS 2 مستوى الخدمة الأكثر أمانًا والأكثر موثوقية ولكنه أيضًا الأبطأ بسبب التكاليف الإضافية المطلوبة لضمان تسليم الرسائل. يتم ضمان التسليم بمجرد تحقيقه من خلال تبادل تأكيد الاتصال المكون من أربعة أجزاء، والذي يتكون من تدفقي طلب / استجابة على الأقل، بين المرسل والمستقبل.

عندما يتم نشر رسالة باستخدام QoS 2، ينخرط المرسل والمستقبل في عملية منسقة لضمان تسليم الرسالة بنجاح. يتضمن ذلك استخدام معرّف الحزمة، الذي يعينه المرسل ويدرج في رسالة النشر الأصلية. حزم تبادل المرسل والمستقبل PUBREC (تم استلام النشر) و PUBREL (نشر الإصدار) لتأكيد التقدم في تسليم الرسالة والإقرار به. أخيرًا، يتلقى المرسل حزمة PUBCOMP (اكتمال النشر) من جهاز الاستقبال، مما يشير إلى التسليم الناجح واستكمال تبادل الرسائل.

تضمن هذه المصافحة المكونة من أربعة أجزاء والتنسيق من خلال معرفات الحزمة تسليم كل رسالة بشكل موثوق به مرة واحدة فقط، حتى في حالة وجود مشكلات أو أعطال محتملة في الشبكة.

تعد QoS 2 مناسبة للتطبيقات التي يكون فيها تكامل الرسالة والدقة بمجرد التسليم أمرًا بالغ الأهمية، مثل المعاملات المالية أو تحديثات النظام الهامة أو المواقف التي لا يُقبل فيها التكرارات أو فقد الرسائل. ومع ذلك، من المهم ملاحظة أن زيادة الموثوقية والضمان المقدم من QoS 2 يأتي على حساب تكاليف الشبكة الإضافية وزيادة زمن الوصول مقارنة بمستويات جودة الخدمة المنخفضة.

تقدم QoS 2 أعلى مستوى من ضمان تسليم الرسائل في MQTT، مما يضمن استلام كل رسالة مرة واحدة بالضبط من قبل المستلمين المقصودين من خلال عملية منسقة وموثوقة.



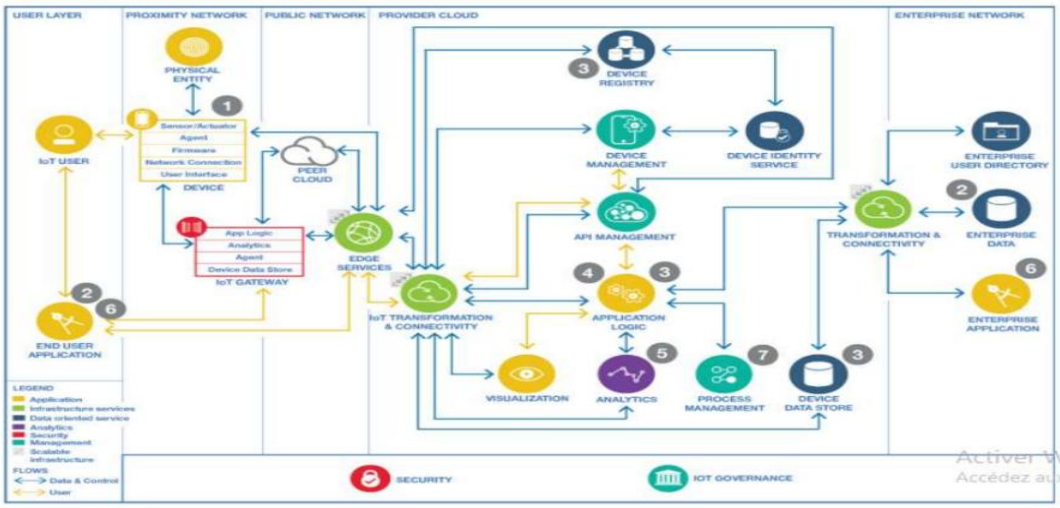
منصة (IoT)

تتيح تقنية متعددة الطبقات تسمى منصة (IoT) توفير وإدارة وأتمتة الأجهزة المتصلة داخل النظام البيئي ل(IoT). إنه بمثابة برمجيات وسيطة، ينشئ اتصالات بين الأجهزة البعيدة وتطبيقات المستخدم أو الأدوات الأخرى ويتحكم في جميع الاتصالات بين طبقات الأجهزة والتطبيق. بالإضافة إلى ضمان قابلية التوسع والتوافق عبر الأجهزة، توفر منصة (IoT) للمطورين مجموعة من الميزات الجاهزة للاستخدام التي تسرع بشكل كبير تطوير التطبيقات للأجهزة المتصلة. بشكل أساسي، تقوم منصة (IoT) بتوصيل أجهزة متنوعة بالسحابة من خلال خيارات اتصال مرنة وآليات أمان على مستوى المؤسسات وإمكانيات معالجة بيانات واسعة. من خلال تقديم خدمات مشتركة للتطبيقات ودمج الحوسبة غير المتجانسة وأجهزة الاتصال، تدعم منصة (IoT) إمكانية التشغيل البيني ضمن التطبيقات والخدمات المتنوعة التي تعمل على هذه الأجهزة.

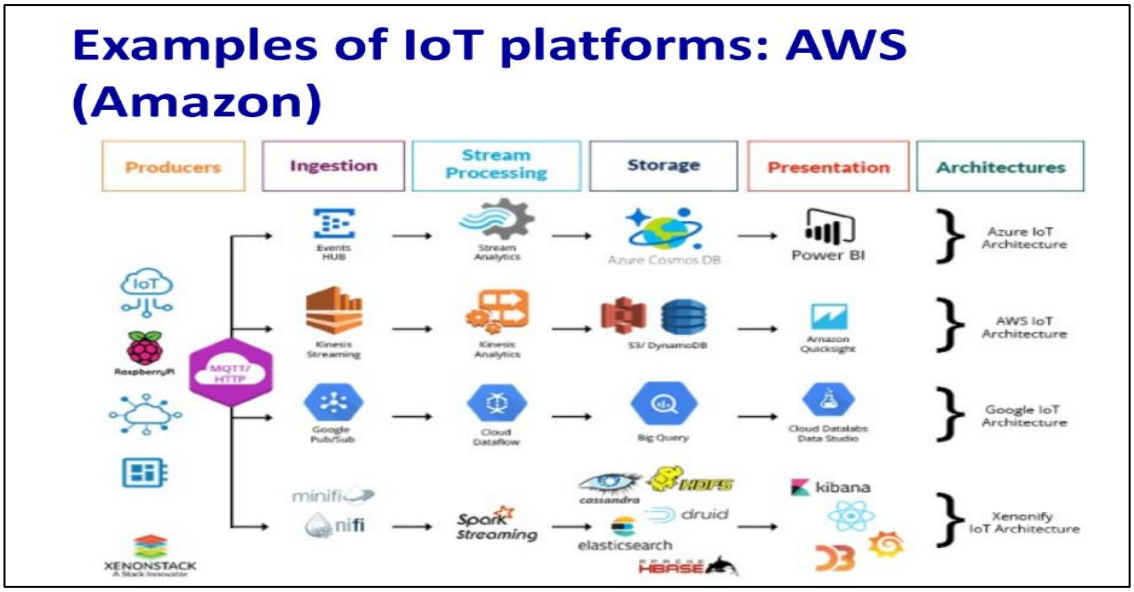
Examples of IoT platforms

Google Cloud Platform
salesforce
amazon web services™
Bosch IoT Suite
SAP
KAA
Particle
Iot4beginners
Microsoft Azure
IBM Watson
cisco IoT
ThingWorx
A PTC Business
ORACLE

Examples of IoT platforms: IBM Watson



Activer Win
Accédez aux pa



في بنية منصة (IoT)، هناك ثماني وحدات بناء مهمة تساهم في وظيفتها وفعاليتها:

١ .الاتصال والتطبيع: يركز هذا العنصر الأساسي على الجمع بين مختلف البروتوكولات وتنسيقات البيانات في واجهة برمجية موحدة. يضمن التدفق السلس والدقيق للبيانات والتفاعل مع جميع الأجهزة المتصلة. من خلال تطبيع البروتوكولات والصيغ المختلفة، تتيح المنصة الاتصال الفعال وقابلية التشغيل البيني بين الأجهزة.

٢ .إدارة الجهاز: إدارة الجهاز هي المسؤولة عن الإشراف على الأداء السليم للأجهزة المتصلة. إنه يتولى مهام مثل مراقبة حالة الجهاز وإدارة تحديثات البرامج وضمان التشغيل السلس للتطبيقات التي تعمل على الأجهزة أو بوابات الحافة. يضمن هذا العنصر الأساسي صيانة الأجهزة والتحكم فيها بشكل فعال داخل منصة (.IoT)

٣ .قاعدة البيانات: يوفر مكون قاعدة البيانات لمنصة (IoT) مساحة تخزين قابلة للتطوير لبيانات الجهاز. إنه يتعامل مع تحديات الحجم والتنوع والسرعة والصدق المرتبطة ببيانات (IoT). يمكن أن تكون قاعدة البيانات مستندة إلى السحابة، مما يتيح التخزين الفعال، والاسترجاع، وتحليل البيانات التي تم إنشاؤها بواسطة الأجهزة المتصلة.

٤. المعالجة وإدارة الإجراءات: تتيح هذه اللبنة الأساسية معالجة البيانات وإدارة الإجراءات بناءً على قواعد ومشغلات محددة. إنه يجلب بيانات المستشعر إلى الحياة من خلال تطبيق منطق إجراء الحدث المستند إلى القواعد. من خلال تحليل البيانات وتفسيرها في الوقت الفعلي، يمكن للنظام الأساسي تنفيذ إجراءات ذكية وأتمتة الاستجابات بناءً على قواعد وحدود محددة مسبقًا.

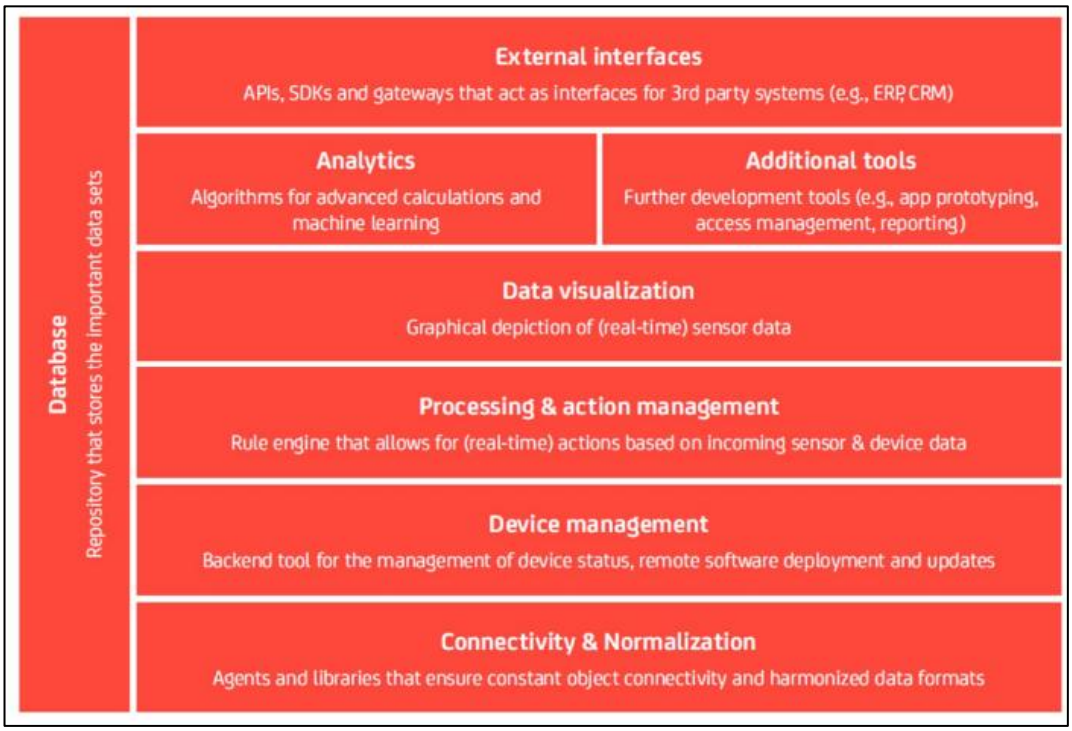
٥ .التحليلات والرؤى: تتضمن التحليلات والرؤى تطبيق تقنيات تحليلات متقدمة على بيانات (IoT) التي تم جمعها. تسمح هذه الكتلة البرمجية الإنشائية باستخراج رؤى واتجاهات وأنماط ذات مغزى من البيانات التي تم إنشاؤها بواسطة الأجهزة المتصلة. إنه يمكّن المؤسسات من اتخاذ قرارات تعتمد على البيانات، وتحسين العمليات، واكتساب ذكاء أعمال ذي قيمة.

٦ .الأمن والخصوصية: يعتبر الأمان والخصوصية من الاعتبارات الهامة في منصة (IoT). تشتمل لبنة البناء هذه على تدابير وبروتوكولات لضمان سرية البيانات وسلامتها وتوافرها. يتضمن المصادقة والتحكم في الوصول وتشفير البيانات وبروتوكولات الاتصال الآمن لحماية أجهزة (IoT) والبيانات التي تولدها.

.التصور وواجهة المستخدم: يركز عنصر التصور وواجهة المستخدم على توفير واجهات سهلة الاستخدام للتفاعل مع منصة (IoT). إنه يمكّن المستخدمين من تصور بيانات الجهاز ومراقبة الأداء في الوقت الفعلي والتحكم في الأجهزة من خلال لوحات معلومات بديهية وتمثيلات رسومية وواجهات سهلة الاستخدام.

٨. التكامل وAPIs: التكامل وAPIs (واجهات برمجة التطبيقات) تسهل التكامل السلس مع الأنظمة والتطبيقات والخدمات الخارجية. يتيح هذا العنصر الأساسي تبادل البيانات وقابلية التشغيل البيني مع أنظمة الجهات الخارجية أو الخدمات السحابية أو الأنظمة الأساسية الأخرى. يسمح لمنصة (IoT) بالاستفادة من الوظائف الخارجية وتوسيع قدراتها من خلال التكامل.

من خلال دمج هذه اللبنات المعمارية الثمانية، توفر منصة (IoT) من طرف إلى طرف حلاً شاملاً وقويًا للاتصال والإدارة والمعالجة والتحليل واستخلاص القيمة من بيانات (IoT). إنه يمكّن المؤسسات من تسخير الإمكانات الكاملة لتقنيات (IoT) ودفع الابتكار في مختلف الصناعات والتطبيقات.



هناك العديد من لغات البرمجة المستخدمة بشكل شائع في تطوير (IoT)، ولكل منها نقاط قوتها ومدى ملاءمتها للجوانب المختلفة لتطبيقات (IoT). فيما يلي بعض من أفضل لغات البرمجة المستخدمة بشكل متكرر في (IoT):

١ :C / C ++. تستخدم C و C ++ على نطاق واسع في الأنظمة المضمنة وتطوير (IoT) نظرًا لقدراتها منخفضة المستوى وكفاءتها والوصول المباشر إلى الأجهزة. غالبًا ما يتم استخدامها لتطوير البرامج الثابتة، وبرامج تشغيل الأجهزة، والبيئات محدودة الموارد حيث يكون الأداء واستخدام الذاكرة أمرًا بالغ الأهمية.

٢ Python: Python. هي لغة برمجة متعددة الاستخدامات وشائعة معروفة ببساطتها وقابليتها للقراءة. يستخدم على نطاق واسع في (IoT) لتحليلات البيانات والبرمجة النصية والنماذج الأولية السريعة. مكتبات وأطر Python الواسعة، مثل

PySerialوDjango، تجعلها مناسبة لتطوير تطبيقات (IoT) ومعالجة البيانات وواجهات الويب.

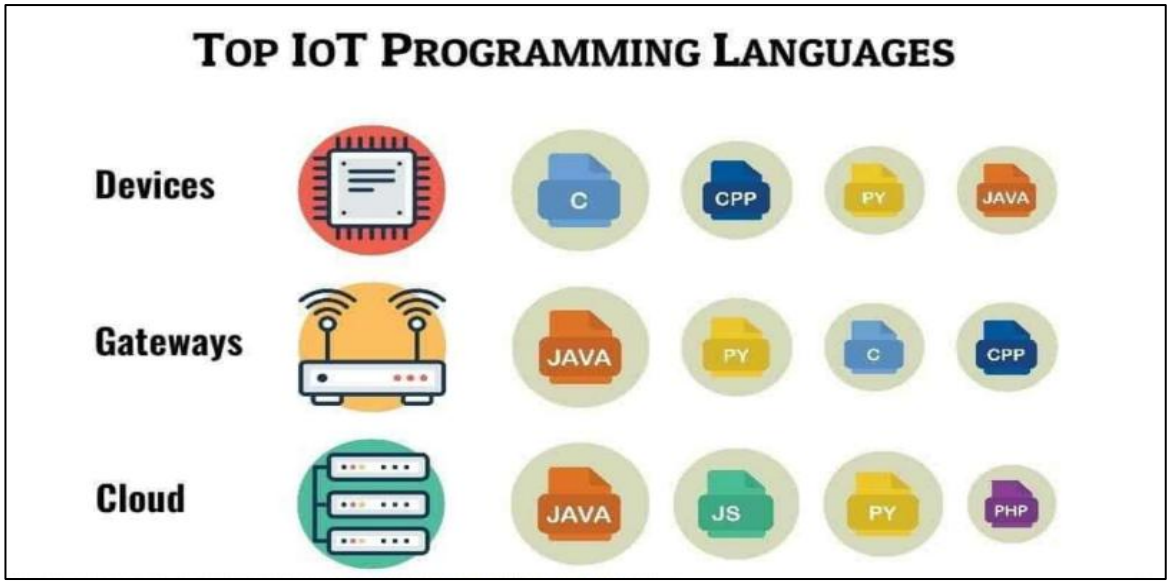
٣ Java: Java .هي لغة قوية ومستقلة عن النظام الأساسي مع نظام بيئي كبير من المكتبات والأطر. يتم استخدامه بشكل شائع في بوابات (IoT)، والخدمات الخلفية، وتطبيقات (IoT) على مستوى المؤسسة. تجعل موثوقية Java وقابليتها للتوسع والتوافق خيارًا مفضلاً لبناء أنظمة (IoT) التي تتطلب معالجة موزعة وقابلية للتشغيل البيني.

٤ :JavaScript .تُستخدم JavaScript بشكل أساسي لتطبيقات (IoT) المستندة إلى الويب، حيث إنها اللغة المفضلة لتطوير الويب الأمامي. مع ظهور Node.js ، تُستخدم JavaScriptأيضًا للتطوير من جانب الخادم، مما يجعلها مناسبة لبناء منصات (IoT) ولوحات المعلومات المستندة إلى الويب والتواصل في الوقت الفعلي بين الأجهزة والخوادم.

٥ .الصدأ: يكتسب Rust شعبية في مجال (IoT) نظرًا لتأكيده على أمان الذاكرة والتزامن والأداء. إنها مناسبة لتطوير مكونات البرامج منخفضة المستوى والبرامج الثابتة والبرمجة على مستوى النظام حيث تكون السلامة والكفاءة أمرًا بالغ الأهمية.

٦. Go: Go ، المعروفة أيضًا باسم Golang ، هي لغة برمجة حديثة تم تطويرها بواسطة Google. تشتهر ببساطتها وكفاءتها ودعمها المدمج للبرمجة المتزامنة. يعد Go مناسبًا تمامًا لتطوير تطبيقات (IoT) التي تتطلب شبكات عالية الأداء ومعالجة متوازية وتدفق البيانات في الوقت الفعلي.

من المهم ملاحظة أن اختيار لغة البرمجة في تطوير (IoT) يعتمد على عوامل مختلفة مثل المتطلبات المحددة للمشروع، وقيود الأجهزة، والبنية التحتية الحالية، ومعرفة المطور، ودعم المجتمع. في النهاية، يتضمن اختيار لغة البرمجة الصحيحة مراعاة احتياجات تطبيق (IoT) والاستفادة من نقاط القوة في اللغة لتحقيق الوظائف والأداء وقابلية التوسع المطلوبة.



بالإضافة إلى لغة البرمجة، هناك العديد من المعايير المهمة الأخرى التي تميز منصات (IoT) عن بعضها البعض. تتضمن هذه المعايير قابلية التوسع، والتخصيص، وسهولة الاستخدام، والتحكم في التعليمات البرمجية، والتكامل مع برامج الطرف الثالث، وخيارات النشر، ومستوى أمان البيانات. فيما يلي بعض الاعتبارات الرئيسية لمنصة (IoT) الفعالة:

١. **قابلية التوسع** :(Cloud Native) يجب أن تكون منصة (IoT) المتقدمة قادرة على التوسع بسلاسة عبر عدد كبير من نقاط النهاية. يجب أن يدعم قابلية التوسع المرنة، مما يسمح للمنصة بمعالجة عبء العمل المتزايد واستيعاب اتصال الجهاز المتزايد. تضمن إمكانات موازنة التحميل داخل النظام الأساسي الأداء الأمثل لمجموعة الخادم، مما يتيح المعالجة الفعالة لحركة مرور البيانات.

٢. **قابلية التخصيص**: التخصيص أمر بالغ الأهمية لسرعة ومرونة تسليم حلول (IoT). يجب أن توفر منصة (IoT) خيارات قابلة للتخصيص، مثل واجهات برمجة التطبيقات للتكامل المرن، والمكونات غير المترابطة، والوصول الشفاف إلى التعليمات البرمجية المصدر. يتيح ذلك للمطورين تصميم النظام الأساسي وفقًا لمتطلبات المشروع المحددة ودمجه بسلاسة مع الأنظمة الحالية.

٣. **الأمان**: يعد أمن البيانات جانبًا مهمًا في أي منصة ل(IoT). يجب أن تتضمن تدابير أمنية قوية لحماية البيانات الحساسة. يتضمن ذلك تشفير البيانات سواء أثناء

النقل أو غير ذلك، وإدارة الهوية الشاملة، ومصادقة الجهاز، وإدارة حقوق وصول المستخدم، والالتزام ببروتوكولات الأمان القياسية في الصناعة. يجب أن يوفر النظام الأساسي أيضًا خيارات نشر مرنة، مثل البنية التحتية السحابية الخاصة، لضمان المعالجة الآمنة للبيانات الحساسة.

٤. **سهولة الاستخدام**: يجب أن تكون منصة (IoT) سهلة الاستخدام وبديهية، مما يسهل على المطورين والمسؤولين والمستخدمين النهائيين التفاعل مع النظام الأساسي وإدارته. تساهم واجهة المستخدم المصممة جيدًا والوثائق الواضحة وموارد الدعم التي يمكن الوصول إليها في سهولة استخدام النظام الأساسي واعتماده.

٥. **التحكم في التعليمات البرمجية**: يجب أن توفر المنصة للمطورين القدرة على التحكم في الكود وتخصيصه وفقًا لمتطلبات محددة. يتضمن ذلك ميزات مثل SDKs (مجموعات تطوير البرامج) وواجهات برمجة التطبيقات (واجهات برمجة التطبيقات) والوصول إلى التعليمات البرمجية المصدر لتمكين التحكم الدقيق والتخصيص.

٦. **التكامل مع برامج الطرف الثالث**: يجب أن تسهل منصة (IoT) الفعالة التكامل السلس مع برامج وخدمات وأدوات الطرف الثالث. يتيح ذلك الاستفادة من الأنظمة الحالية وتوسيع قدرات حل (IoT) من خلال التكامل مع التطبيقات الخارجية أو منصات تحليل البيانات أو الخدمات السحابية.

٧. **خيارات النشر**: يجب أن توفر المنصة مرونة في خيارات النشر لتلبية متطلبات وتفضيلات البنية التحتية المختلفة. يجب أن يدعم النشر في أماكن العمل، أو في السحابة، أو في البيئات المختلطة، مما يسمح للمؤسسات باختيار نموذج النشر الأنسب بناءً على احتياجاتها الخاصة ومتطلبات الامتثال وأهداف قابلية التوسع.

بالنظر إلى هذه المعايير وتقييم منصات (IoT) استنادًا إلى قابليتها للتوسع والتخصيص والأمان وسهولة الاستخدام والتحكم في الكود وقدرات التكامل وخيارات النشر، ستساعد المؤسسات على اختيار منصة (IoT) الأكثر ملاءمة لحالات ومتطلبات الاستخدام الخاصة بها.

التطبيق

في القسم التالي، سنقوم بتصنيف تطبيقات مختلفة ل(IoT)، بما في ذلك الاكثر شيوعاً.

المدن الذكية

ما هي؟

تُستخدم أجهزة (IoT) مثل أجهزة الاستشعار المتصلة والأضواء والعدادات في المدن الذكية لجمع البيانات وتحليلها. تُستخدم البيانات التي تم جمعها لتحسين المرافق العامة والبنية التحتية والخدمات، من بين أشياء أخرى. وبهذه الطريقة، تقدم المدن الذكية لسكانها أسلوب حياة أكثر كفاءة وجودة أعلى. فيما يلي الطرق التي تحقق بها المدن الذكية هذه الأهداف.

تقنيات المدينة الذكية

تُستخدم تكنولوجيا المعلومات والاتصالات (ICT) في المدن الذكية لتحسين الفعالية التشغيلية، ومشاركة المعرفة مع عامة الناس، ومستوى الخدمات العامة ورفاهية المواطنين. ترتبط المدن الذكية عبر مجموعة متنوعة من البرامج والاتصالات وشبكات الواجهة. نظرًا لأنه يجعل مشاركة البيانات والاتصال بين الأجهزة أسهل، فإن (IoT) هي واحدة من التقنيات التي تستخدمها المدن الذكية أكثر من غيرها. الذكاء الاصطناعي (AI)، وخدمات الحوسبة السحابية، والتعلم الآلي، والاتصال من آلة إلى آلة، وواجهات برمجة التطبيقات(APIs) ، والشبكات الشبكية مثل Wi-SUN ، ولوحات المعلومات هي بعض التقنيات الشائعة الأخرى المستخدمة في المدن الذكية.

تُستخدم هذه التقنيات في المدن الذكية الأوروبية لتعزيز إدارة البيئة الحضرية والإنتاجية. قد تستخدم المدن، على سبيل المثال، أجهزة (IoT) لجمع البيانات في الوقت الفعلي من أجهزة الاستشعار والعدادات لتحديد الأنماط وتتبع استخدام الطاقة وتحسين تدفق حركة المرور. يمكن لروبوتات الدردشة التي تستخدم الذكاء الاصطناعي تحسين مستوى خدمات المواطنين، بينما يمكن لخدمات الحوسبة السحابية تخزين

كميات هائلة من البيانات والتعامل معها. يمكن تحليل مجموعات البيانات بواسطة خوارزميات التعلم الآلي لتحديد مناطق التحسين المحتملة، ويمكن لواجهات برمجة التطبيقات توصيل أنظمة مختلفة للسماح بمشاركة البيانات عبر المدينة.

تستخدم المدن الذكية الحلول التقنية لإدارة وتحسين الخدمات والبنية التحتية الحضرية بهدف تحسين نوعية الحياة لمواطنيها.

(IoT) في المدن الذكية

ترتبط (IoT) والمدن الذكية ببعضها البعض لأن فكرة (IoT) تركز بشكل كبير على تكامل تقنيات (IoT). يمكن جمع البيانات حول جوانب مختلفة من حياة السكان باستخدام أجهزة (IoT) مثل أجهزة الاستشعار والكاميرات. كل شيء في المدن السلكية متصل بالشبكات، بما في ذلك المركبات والهياكل والأجهزة المنزلية، فضلاً عن المستشعرات وتقنية الشبكة الذكية التي تتيح توزيع الطاقة وتكامل مصادر الطاقة. يتم تعزيز تكامل الأجهزة الذكية بشكل أكبر من خلال أنظمة الإدارة المطورة.

قد يتفاعل سكان المدن الذكية مع بيئتهم من خلال منازلهم المتصلة، والسيارات المتصلة، والهواتف الذكية. توفر هذه الأدوات للمستخدمين القدرة على تتبع استخدامهم للطاقة، والحصول على معلومات حركة المرور، والإبلاغ عن المشكلات المتعلقة بالسلامة العامة، من بين أشياء أخرى. يستفيد السكان من اقتران الجهاز والبيانات، مما يساعد أيضًا على تقليل النفقات وزيادة الاستدامة. قد تعمل المدن الذكية على تحسين خدماتها وتقليل هدر الطاقة من خلال تقييم البيانات التي تم جمعها بواسطة أجهزة (IoT).

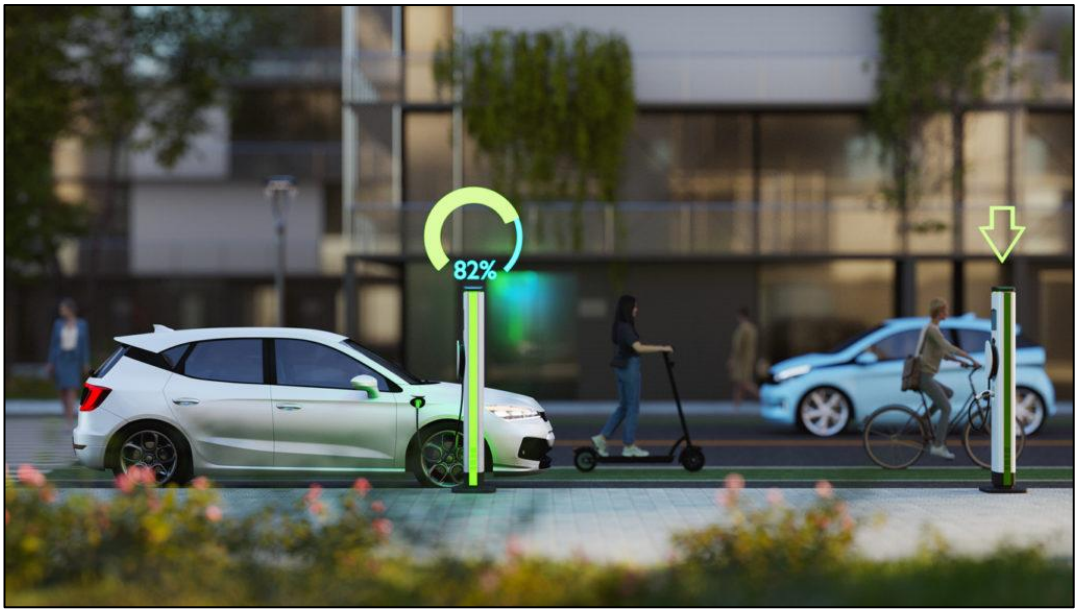
تعتمد المدن الذكية بشكل كبير على تقنية (IoT) لأنها توفر الإطار المطلوب للاتصال وإدارة البيانات الفعالة. يعمل دمج أجهزة (IoT) في المدن الذكية على تحسين نوعية الحياة للمواطنين مع تقليل النفقات والتأثيرات البيئية أيضًا.

المدن الذكية والاستدامة

يمكن للمجتمعات توزيع الطاقة بشكل أكثر فعالية، وجمع القمامة بسرعة أكبر، وتقليل حركة المرور، وتحسين جودة الهواء بفضل تقنية (IoT). على سبيل المثال، يمكن لأجهزة الاستشعار الموضوعة على علب القمامة مراقبة مدى امتلائها، مما يتيح جدولة أكثر كفاءة للتخلص من القمامة. يمكن أيضًا ضبط توقيت وإيقاع إشارات المرور في الوقت الفعلي اعتمادًا على المعلومات الواردة من أجهزة الاستشعار والسيارات المتحركة، مما يمكن أن يساعد في تقليل الازدحام المروري.

قد تزيد المدن الذكية من جودة الهواء من خلال مراقبة الملوثات في الوقت الفعلي وتحديد مصادر التلوث المحتملة من خلال استخدام أجهزة (IoT). على سبيل المثال، يمكن وضع أجهزة الاستشعار في مكانها عند التقاطعات التي بها الكثير من حركة المرور للعثور على تركيزات عالية من أكاسيد النيتروجين التي تنتجها المركبات المتحركة. بعد ذلك، باستخدام هذه المعلومات، يمكن وضع سياسات لتقليل حركة المرور وتحسين جودة الهواء.

أنظمة وقوف السيارات الذكية هي مثال آخر على تقنية (IoT) في المدن الذكية. يمكن للسائقين تحديد أماكن وقوف السيارات المفتوحة بسهولة بفضل المستشعرات الموضوعة في أماكن وقوف السيارات التي يمكنها تحديد ما إذا كانت هناك مساحة مشغولة أو متوفرة بسرعة. هذا يقلل من الازدحام المروري وانبعاثات الكربون الناتجة عن دوران السيارات بحثًا عن أماكن وقوف السيارات.



أحد العوامل المهمة في تطوير فكرة المدن الذكية هو الاستدامة البيئية. تستخدم المدن الذكية حلول التنقل الموفرة للطاقة، مثل السيارات الكهربائية (EV) وبرامج مشاركة الدراجات، لتحقيق ذلك. تساهم خيارات السفر الخضراء هذه بشكل كبير في خفض انبعاثات الكربون وتحسين جودة الهواء.

تجمع هذه الأجهزة البيانات التي يتم الاحتفاظ بها على الخوادم أو في السحابة، حيث يمكن تحليلها لتعزيز إنتاجية كل من القطاعين العام والخاص، وتحسين نوعية حياة المواطن، وتوفير مكاسب مالية. على سبيل المثال، يمكن استخدام البيانات من المركبات الكهربائية لتحسين محطات الشحن، بينما يمكن استخدام البيانات من أنظمة مشاركة الدراجات لتحديد أكثر المناطق ازدحامًا لمحطات الدراجات وأكثر طرق ركوب الدراجات شيوعًا. وبالتالي، قد يصبح نظام النقل أكثر فعالية بشكل عام، مما سيوفر المال ويكون له تأثير سلبي أقل على البيئة.

الاستدامة عنصر أساسي في فكرة المدن الذكية. قد تعمل المدن الذكية على خفض انبعاثات الكربون وتحسين جودة الهواء وتوفير مزايا اقتصادية من خلال دمج مصادر الطاقة وأنظمة النقل المستدامة. ستستمر جودة الحياة للمقيمين في التحسن نتيجة لتحليل البيانات التي تم الحصول عليها من هذه الأجهزة لتعظيم فعالية القطاعين العام والتجاري.

التحديات في المدن الذكية

تتمثل إحدى إستراتيجيات رفع مستويات المعيشة الحضرية في إنشاء مدن ذكية. تتمتع المدن الذكية بالقدرة على التأثير على مستقبل الحياة الحضرية من خلال تحسين جودة حياة المواطنين وتقليل التأثير البيئي وتحسين عمليات المدينة.

لكن تطوير المدينة الذكية لا يخلو من الصعوبات. أكبر المخاوف هي مشكلات الخصوصية والأمان، خاصة عند جمع كميات هائلة من البيانات وتحليلها. نظرًا للنفقات الكبيرة التي ينطوي عليها نشر تكنولوجيا المدن الذكية وصيانتها، لا تمتلك جميع المدن الوسائل المالية للاستثمار في هذه المشاريع.

يمثل مطلب الاتفاقيات الحكومية لتعزيز المشاركة الواسعة للمواطنين صعوبة أخرى. يجب أن يتعاون القطاع الحكومي وقطاع الأعمال مع السكان المحليين حتى يكون للمدن الذكية تأثير مفيد على المجتمع.

علاوة على ذلك، فإن الاتصال الناجح والتعاون عبر مئات الآلاف أو ربما الملايين من الأجهزة المرتبطة يجعل تكامل أجهزة (IoT) تحديًا كبيرًا. لتوفير تبادل سلس للبيانات بين الأجهزة مع الحفاظ في نفس الوقت على الخصوصية والأمان، يلزم وجود بنية تحتية قوية وآمنة.

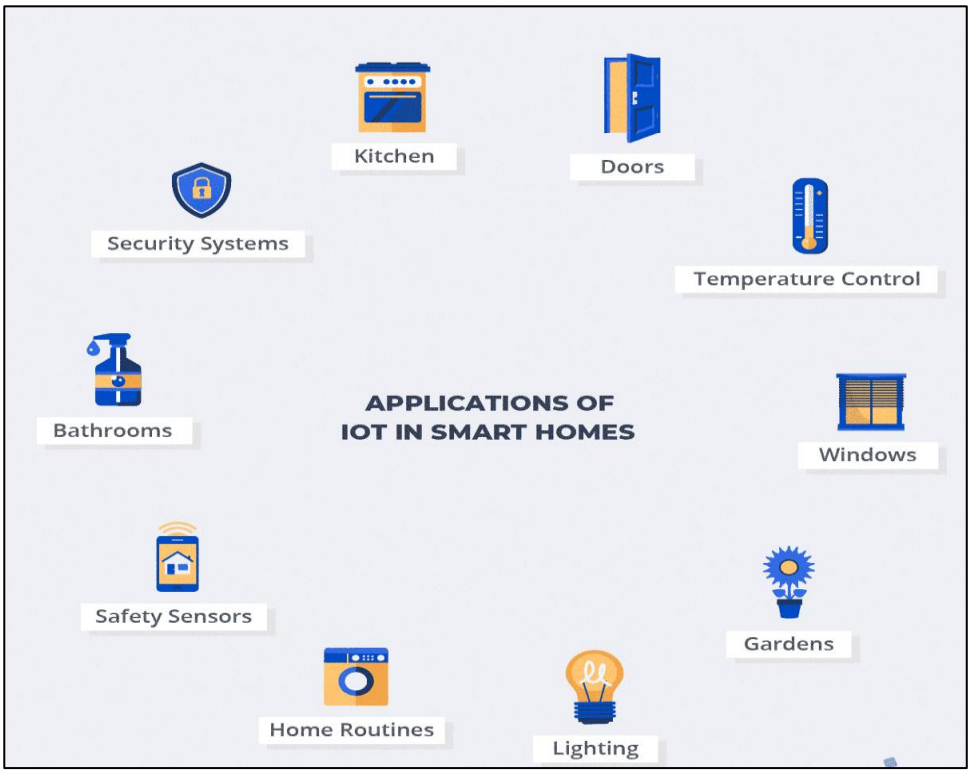
على الرغم من أن إنشاء المدن الذكية لديه القدرة على تغيير الحياة الحضرية، إلا أن هناك عقبات يجب التغلب عليها. من أجل التنفيذ الفعال لمبادرات المدن الذكية، يجب التغلب على عدد من التحديات الرئيسية، بما في ذلك حدود الميزانية، وقضايا الخصوصية والأمن، والحاجة إلى مشاركة جماعية للمواطنين، والتنسيق بين القطاعين العام والتجاري.

المنازل الذكية

تتمتع مستشعرات (IoT) الذكية بالقدرة على تعلم تفضيلات الإنسان، بما في ذلك أذواقنا الموسيقية ودرجة الحرارة المفضلة وإعدادات الإضاءة والروتين اليومي، مثل عندما نستيقظ ونأكل ونذهب إلى الفراش. أصبح رويتننا اليومي أكثر بساطة من خلال الأدوات الذكية مثل المقابس والأضواء وأنظمة الأمان. تتم إدارة هذه الأجهزة بسهولة

بواسطة تطبيقات الهواتف الذكية، مما يسمح لنا بمراقبة أمن المنزل حتى أثناء وجودنا بعيدًا. أحد الاستخدامات الرئيسية لتقنية (IoT) هو أتمتة المنزل الذكي، والذي يتيح التحكم السلس والتكامل في أجهزتنا المنزلية.

تطبيقات (IoT) في المنازل الذكية



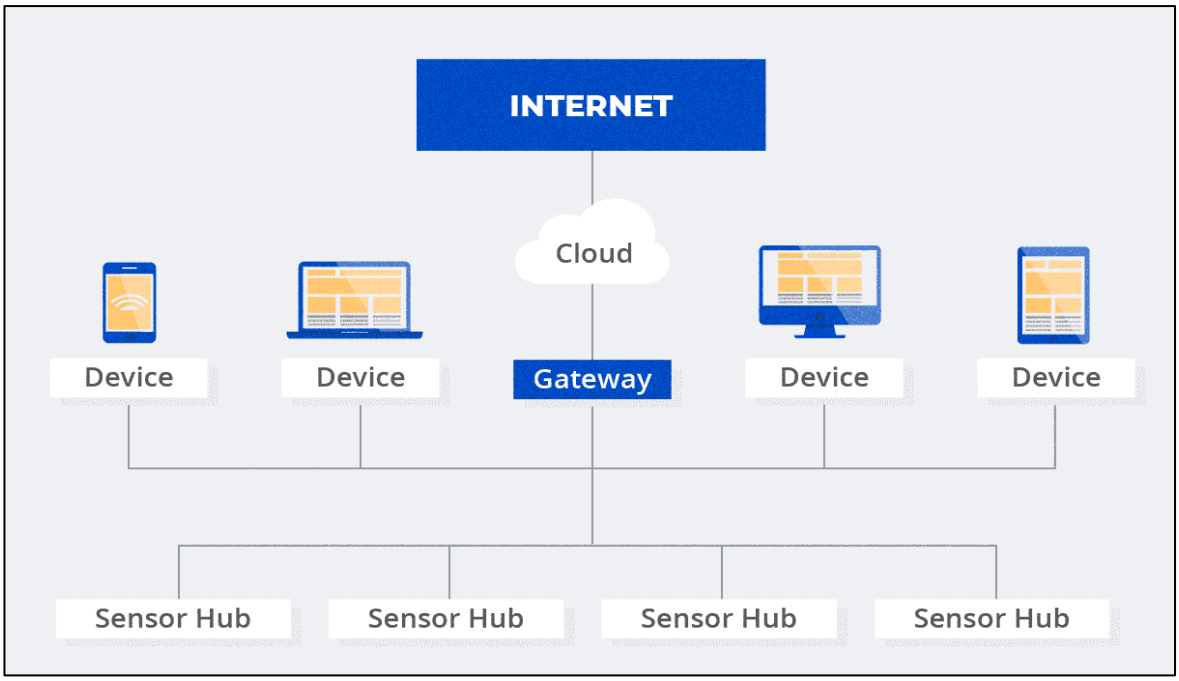
تم تغيير الطريقة التي نعيش بها في منازلنا من خلال أتمتة المنزل الذكي. باستخدام تقنية (IoT) ، يمكن توصيل الأجهزة المنزلية المختلفة معًا وإدارتها بواسطة الهواتف الذكية والأجهزة المتصلة الأخرى. نتج عن ذلك العديد من المزايا، بما في ذلك زيادة الراحة والأمان وكفاءة الطاقة.

على سبيل المثال، قد يتم تغيير إضاءة المنزل تلقائيًا بناءً على تفضيلات المستخدم، ويمكن للنظام إطفاء الأنوار عندما يغادر المستخدم المنزل للحفاظ على الطاقة. أصبح الروتين اليومي في الحمام أكثر إمتاعًا وعمليًا من خلال ابتكارات (IoT) مثل المرايا الذكية وأدوات التحكم في الدش. قد تقدم المستشعرات الذكية توصيات بشأن الوصفات وتحسب القيمة الغذائية وتراقب مستويات الدخان وأول أكسيد الكربون في المطبخ لضمان السلامة.

عند مغادرة المنزل، تقوم أنظمة الأمان الذكية بإغلاق الأبواب وإغلاق المصاريع وإيقاف الأجهزة الإلكترونية لتوفير راحة البال للمستخدمين. يمكن تحديد المخاطر المحتملة بواسطة مستشعرات السلامة، والتي يمكنها بعد ذلك إخطار المستهلكين عبر هواتفهم المحمولة. قد تستخدم الأبواب الذكية التعرف على الوجه لفتح المنزل، ويمكن لأتمتة التحكم في درجة الحرارة تغيير درجة حرارة المنزل لتتناسب مع تفضيلات المستخدم والأنشطة الحالية.

تشمل المزايا العديدة لأتمتة المنزل الذكي تحسين الراحة والأمان واقتصاد الطاقة. يمكن للمستخدمين إدارة عناصر مختلفة من منازلهم باستخدام تقنيات الذكاء الاصطناعي والتعلم الآلي، ويمكنهم حتى استخدام هواتفهم الذكية لمراقبة حالة نظام التشغيل الآلي الخاص بهم من أي مكان.

كيف يعمل نظام الأتمتة القائم على (IoT)



الإعداد الأساسي

يحتوي نظام أتمتة (IoT) على بنية متطورة تتكون من خوادم بعيدة تحتوي على أجهزة استشعار. قد تتحكم هذه الخوادم في وقت واحد في العديد من أجهزة الاستشعار

وتقع في السحابة. تستخدم مستشعرات (IoT) بروتوكولات اتصال مختلفة، بما في ذلك Bluetoothو ZigBee و Wi-Fi وZ-Wave.

وحدة التحكم، التي يشار إليها أحيانًا باسم المحور أو البوابة، هي أدمغة النظام. يستخدم Ethernet للاتصال بالشبكة المنزلية ويعمل كمحور مركزي للتحكم في المستشعرات. من أجل ربط جميع الأجهزة وتمكين بناء تسلسلات الإجراءات المطلوبة، تقوم البوابة بعد ذلك بنقل هذه البيانات إلى السحابة.

يجعل هذا الاتصال من الأسهل على العملاء إدارة منازلهم وتشغيلها تلقائيًا لأنهم يستطيعون رؤية أجهزة (IoT) والتحكم فيها عن بُعد عبر أحد التطبيقات. بشكل عام، يوفر نظام أتمتة (IoT) طريقة سلسة وفعالة للتحكم في الأجهزة المنزلية وتحسين جودة الحياة لعملائها.

الاتصال السحابي

تقوم السحابة بتخزين وإدارة بيانات جهاز (IoT)، مما يجعلها متاحة من أي مكان متصل بالإنترنت. نتيجة لذلك، يمكن للعملاء إصدار أوامر إلى أجهزة (IoT) الخاصة بهم من أي مكان في العالم.

يتلقى المحور أمرًا وينقله إلى المستشعرات، مما يتسبب في قيامهم بالإجراء المحدد. يقوم المركز بعد ذلك بتحديث حالة الجهاز لمنح المستخدم البيانات ذات الصلة. هذا يجعل من الممكن التحكم في أجهزة (IoT) بسهولة وفعالية من أي مكان.

المر اقبة في الوقت الحقيقي والتنبيهات

قد يقوم مستخدمو نظام أتمتة (IoT) بترتيب الأنشطة التي تم تشغيلها وتتبع التعديلات الدورية للجدول الزمني بفضل اتصال المحور المستند إلى الإنترنت بالشبكة السحابية. عند إدخال أمر ما، ترسله الشبكة السحابية إلى المحور وتنقله هناك. ثم يتم إرسال الأمر عن طريق المحور إلى المستشعر المناسب، لبدء العملية.

يتم إبلاغ المستخدم فورًا بحالة النظام المعدلة بعد انتهاء النشاط. يوفر ذلك راحة البال والإدارة الفعالة لأجهزة (IoT) من خلال ضمان عدم الإبلاغ عن أي تعديلات على أجهزتها الذكية.

التكامل (IFTTT)

من خلاله، يمكنك إنشاء سلسلة من الأنشطة. سيتم اتخاذ الإجراء فقط في حالة استيفاء الشروط المطلوبة. على سبيل المثال، سيتم إغلاق النوافذ تلقائيًا لحماية الممتلكات الخاصة بك إذا اكتشفت المستشعرات المطر أو الثلج.



أجهزة استشعار (IoT) لأتمتة المنزل

يمكن أن يؤدي استخدام مستشعرات (IoT) إلى تحسين جودة حياتنا وسلامة المنزل بشكل كبير. على سبيل المثال، قد تُعلم أجهزة التحكم الذكية في الحركة المستخدمين عبر التطبيق إذا اقترب شخص ما أو حيوان من ممتلكاتك، مما يزيد من مستوى الأمان.

يمكن للمستخدمين التأكد من إغلاق جميع النوافذ والأبواب في الليل أو أثناء حالات الطقس المحددة مثل المطر أو العواصف باستخدام أدوات التحكم الذكية. يمكن أيضًا

استخدام أدوات التحكم لتغيير الإضاءة والرطوبة ودرجة الحرارة لتناسب أذواق الشخص.

تحمي أجهزة التحكم في الدخان المنازل من مخاطر الحريق، بينما تساعد أجهزة الكشف عن أول أكسيد الكربون في تجنب التسمم من هذا الغاز الخطير. تعمل هذه المستشعرات وأدوات التحكم على زيادة أمن المنزل وتوفر للمالكين مزيدًا من راحة البال.

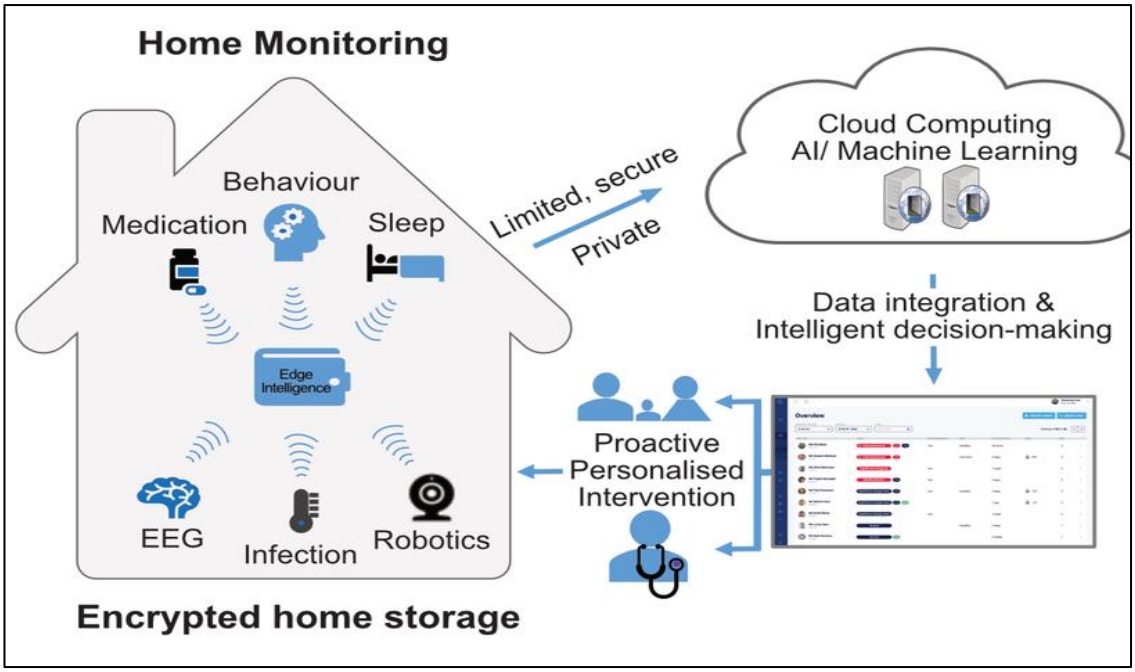
(IoT) في الرعاية الصحية

يوضح مصطلح (IoMT) الشبكة المكونة من المعدات والأجهزة والبرامج الطبية المتصلة بالشبكة والمرتبطة بتكنولوجيا المعلومات الخاصة بالرعاية الصحية. تسمح قدرة المعدات الطبية على الاتصال لاسلكيًا وعن بعد عبر الإنترنت بفضل هذه التقنية، التي يشار إليها أحيانًا باسم (IoT) في صناعة الرعاية الصحية، بإجراء تحليل سريع ومرن للبيانات الطبية مع ضمان الأمان.

يركز IoMT بشكل أساسي على الرعاية الصحية والتطبيقات الطبية، لكن (IoT) الأكبر يشمل جميع الأجهزة المتصلة بالإنترنت، بما في ذلك معدات التصنيع، وأجهزة المسح الضوئي للأمن السيبراني البيومترية، ومعدات الزراعة المستقلة. بالمقارنة مع أنظمة (IoT) الأخرى، تتطلب IoMT بنية أمنية أكثر جوهرية وشمولية بسبب الطبيعة الحساسة لبيانات الرعاية الصحية والقواعد الصارمة المتعلقة بها.

IoMT في المنزل

أدت القدرة على توفير البيانات الطبية لممارسي الرعاية الصحية من المنزل بفضل تقنية (IoT) (IoMT) إلى تغيير الرعاية الصحية. IoMT في المنزل هو اسم هذا. تعد مراقبة المريض عن بُعد (RPM) أحد أهم استخدامات (IoT) داخل المنزل. تمكّن RPM المرضى الذين خرجوا مؤخرًا من المستشفى من استخدام المعدات الطبية لإرسال البيانات إلى أطبائهم، مثل ضغط الدم أو تشبع الأكسجين. يتيح ذلك للمهنيين الطبيين تحديد أي مشاكل قبل أن تتفاقم وقد يقلل من عدد حالات إعادة الإدخال إلى المستشفى.



من التطبيقات المهمة الأخرى لتقنية IoMT الرعاية الصحية عن بُعد، والتي تقدم للمرضى العلاج الطبي عن بُعد. يمكن للمرضى الذين تم إطلاق سراحهم مؤخرًا التواصل مع أطبائهم تقريبًا بسبب الصعوبات البسيطة بفضل التكنولوجيا. الرعاية المستمرة خارج بيئة المريض ممكنة باستخدام أجهزة (IoT) (IoMT) والرعاية الصحية عن بُعد. أحد الأمثلة على ذلك هو أنظمة الاستجابة الشخصية للطوارئ (PERS). في حالة الطوارئ، مثل السقوط أو النوبة القلبية، يمكن لهذه الأدوات الاتصال على الفور للحصول على المساعدة. يمكن أن تكون PERS مفيدة بشكل خاص للأفراد الضعفاء، مثل المواطنين الأكبر سنًا الذين يرغبون في العيش بحرية دون تعريض سلامتهم للخطر.

IoMT على الجسد

يشار إلى المعدات الطبية القابلة للارتداء والتي يمكن توصيلها بأنظمة المراقبة البعيدة باسم IoMT على الجسم. أجهزة IoMT على الجسم، على عكس IoMT في المنزل، يتم ارتداؤها خارج المنزل وقد تتعقب صحة مرتديها أثناء ممارسة أنشطتهم المعتادة.

قد تقيس أجهزة IoMT الخاصة بالعميل على الجسم المعلمات الصحية للاستخدام الشخصي والمشاركة مع ممارسي الرعاية الصحية. يمكن الوصول إليها بسهولة من خلال التكنولوجيا القابلة للارتداء. يمكن أن تعمل هذه الأدوات كمؤشرات مبكرة على

المشكلات الطبية التي يحتمل أن تكون خطرة. على سبيل المثال، قد تحدد Apple Watchدقات القلب غير الطبيعية.

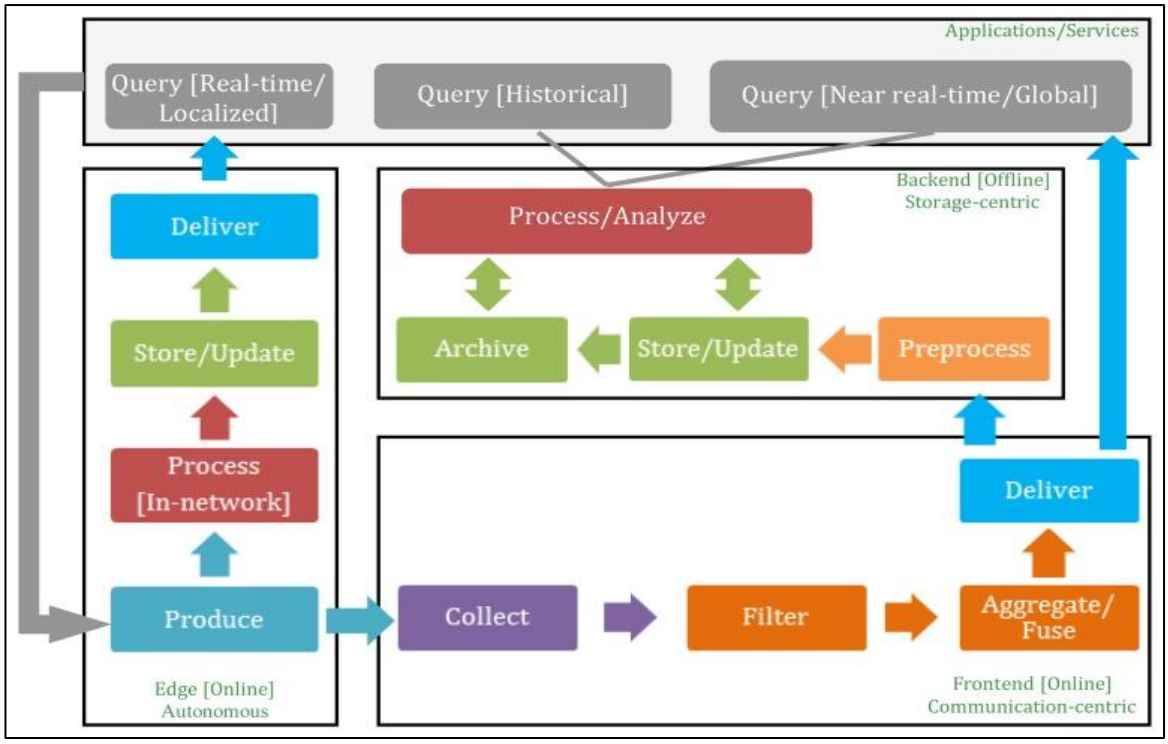
تُستخدم أنظمة IoMT السريرية على الجسم بشكل متكرر في إعدادات الرعاية الصحية وتوفر نطاقًا أكبر من خيارات المستشعرات. على سبيل المثال، يمكن لمرضى السكري ارتداء مستشعرات الجلوكوز لإخطارهم بالتغيرات في مستويات السكر في الدم. من أجل ضمان العلاج السريع والدقيق، قد تقوم العديد من هذه الأجهزة أيضًا بنقل البيانات مباشرة إلى أطباء المريض.

الإدارة والتحليل للبيانات (IoT)

لم تعد حلول إدارة البيانات التقليدية كافية في عالم (IoT) للتعامل مع الأحجام الهائلة من البيانات التي تنتجها الأجهزة المرتبطة. يجب أن تكون حلول إدارة بيانات (IoT) قادرة على تخزين البيانات عبر الإنترنت وتسجيلها وتدقيقها وتلخيصها لتحليلها دون اتصال بالإنترنت. وهذا يستلزم نهجًا جديدًا لإدارة البيانات، وهو نهج يتجاوز إدارة المعاملات والتخزين دون اتصال بالإنترنت ليشمل الاتصال عبر الإنترنت والعمليات المزدوجة.

دورة حياة (IoT)

يمكن تقسيم تدفق بيانات نظام (IoT) إلى مراحل مختلفة، بدءًا من توليد البيانات وانتهاءً بتحليلها. قبل الإرسال، يتم إنشاء البيانات، ثم تجميعها، ربما بالترشيح والتحضير. ثم يتم أرشفة البيانات المرسلة والاحتفاظ بها لاستخدامها لاحقًا. تتضمن الخطوات الأخيرة للعملية تحليل البيانات والاستعلام. في حين أن بعض هذه المراحل تركز على الاتصال والإنترنت، إلا أن البعض الآخر غير متصل بالإنترنت ويحتاج إلى الكثير من طاقة المعالجة والتخزين.



بينما تتعامل إجراءات الأرشفة مع بيانات للقراءة فقط، تضمن أنشطة التخزين إمكانية الوصول المستمر إلى البيانات للتحديثات على المدى الطويل. بالنسبة للخدمات المحلية وفي الوقت الفعلي، يتم إنشاء البيانات ومعالجتها وتخزينها محليًا داخل بعض شبكات أنظمة (IoT). يشير هذا إلى أن الوحدات المستقلة، التي يشار إليها باسم "الحواف"، قد تتضمن كلاً من مكونات معالجة البيانات وتخزينها دون الحاجة إلى إرسال معلومات إلى محاور النظام المركزية. يتم وصف كل مكون من مكونات عمر بيانات (IoT) في الفقرات التالية.

في الأنظمة التي تستخدم الكثير من البيانات، يعد الاستعلام خطوة حاسمة للوصول إلى البيانات واسترجاعها. لأسباب تتعلق بالمراقبة الزمنية أو للحصول على منظور معين للبيانات المخزنة في النظام، يمكن استخدام الاستعلامات في سياق (IoT). يتم استخدام النوع الأول بشكل متكرر لطلبات الحصول على بيانات محلية في الوقت الفعلي، بينما يتم استخدام الأحدث في وجهات النظر الدولية للبيانات والدراسة المتعمقة للاتجاهات والأنماط.

يشكل الاستشعار ونقل البيانات بواسطة "الأشياء" داخل النظام إنتاج البيانات في (IoT). ثم يتم إرسال المعلومات كرد على الاستفسارات التي تطلب البيانات من أجهزة

الاستشعار والأجهزة الذكية، والتي يتم إبلاغها بشكل دوري للأطراف المهتمة من خلال نموذج الاشتراك / الإخطار، ودفع الشبكة إلى نقاط التجميع، وفي النهاية إلى خوادم قواعد البيانات. غالبًا ما تكون المعلومات مختومة بالطابع الجغرافي والوقت. يمكن أن تظهر كأزواج قيمة مفتاح مباشرة أو كمعلومات صوتية أو صور أو فيديو أكثر تعقيدًا. اعتمادًا على الاستخدام، قد يتغير تعقيد البيانات.

في (IoT)، قد يتم جمع البيانات بواسطة أجهزة الاستشعار والأدوات الذكية التي إما تخزنها لفترة زمنية معينة أو تبلغ عنها لمكونات التحكم. قد يتم جمع البيانات في نقاط تركيز الشبكة أو البوابات، حيث يتم بعد ذلك ترشيحها ومعالجتها، وفي بعض الأحيان دمجها في أشكال صغيرة للإرسال الفعال. يتم استخدام تقنيات الاتصال اللاسلكي مثل Zigbeeو Wi-Fi والخلية بواسطة العناصر لنقل البيانات إلى محطات التجميع.

نظرًا لمعدلات تدفق البيانات المتزايدة والنطاق الترددي المقيد في (IoT)، فقد يكون إرسال جميع البيانات الأولية في الوقت الفعلي أمرًا مكلفًا للغاية. يتم استخدام تقنيات التجميع والدمج، التي تستخدم إجراءات التلخيص والجمع في الوقت الفعلي لتقليل كمية البيانات التي يجب حفظها ونقلها، لحل هذه المشكلة.

قد يلزم تسليم نتائج تصفية البيانات وتجميعها ومعالجتها في (IoT) إلى أعلى النظام، إما كردود نهائية أو للتخزين والتحليل المتعمق. قد تحدث هذه المعالجة في مواقع التركيز أو الوحدات الافتراضية المستقلة داخل الشبكة. يمكن استخدام اتصالات النطاق العريض السلكية أو اللاسلكية لنقل البيانات إلى مستودعات البيانات الدائمة.

سيتم استخدام البيانات من مصادر عديدة ذات أنواع وهياكل متنوعة في (IoT). قبل أن تلتزم البيانات بالتخزين، قد تكون المعالجة المسبقة ضرورية لإدارة البيانات المفقودة، والقضاء على التكرار، ودمج البيانات من عدة مصادر في مخطط واحد. في التنقيب عن البيانات، يشار إلى هذا الإعداد باسم تنظيف البيانات. لا يستلزم تكامل المخطط إجبار جميع البيانات على مخطط علائقي صارم، بل يستلزم تحديدًا أكثر عمومية لكيفية الوصول إلى البيانات باستمرار دون الحاجة إلى ضبط الوصول إلى تنسيقات البيانات المحددة لكل مصدر. يمكن تطبيق الاحتمالات على مستويات مختلفة

في المخطط على عناصر بيانات (IoT) في هذه المرحلة لمعالجة أي غموض قد يكون موجودًا في البيانات أو لمعالجة نقص الثقة الذي قد يكون موجودًا في مصادر البيانات.

تستلزم مرحلة التخزين / أرشفة التحديث في دورة حياة بيانات (IoT) إدارة فعالة للبيانات وتخزينها، فضلاً عن التحديثات المستمرة مع البيانات الحديثة عندما تصبح متاحة. تتم أرشفة البيانات غير المطلوبة على الفور لعمليات النظام المستمرة للتخزين دون اتصال طويل المدى. يُعرف استخدام هياكل التخزين التي يمكن أن تتكيف مع أنواع البيانات المختلفة ومعدلات جمع البيانات بالتخزين المركزي. الخيار الشائع هو أنظمة إدارة قواعد البيانات العلائقية، التي ترتب البيانات في هيكل جدول مع علاقات وبيانات وصفية راسخة لاسترجاعها بسرعة في المستقبل. نظرًا لأنها توفر تخزينًا هائلاً للبيانات دون الاعتماد على البنية العلائقية أو متطلبات الاتساق الصارمة الشائعة في أنظمة قواعد البيانات العلائقية، أصبحت متاجر NoSQL ذات القيمة الرئيسية أكثر شيوعًا. التخزين اللامركزي هو خيار لأنظمة (IoT) المستقلة، حيث تحتفظ بالبيانات بالقرب من المصادر بدلاً من إرسالها إلى أعلى التسلسل الهرمي. ومع ذلك، مقارنة بنموذج التخزين المركزي، لا تزال سعة التخزين مقيدة بسبب القدرات المحدودة لهذه الكائنات.

تتم عمليات الاسترداد والتحليل على البيانات المخزنة بشكل مستمر أثناء مرحلة المعالجة / التحليل من دورة حياة بيانات (IoT) لاكتساب رؤى حول البيانات السابقة، أو التنبؤ بالاتجاهات المستقبلية، أو العثور على الحالات الشاذة في البيانات التي قد تحتاج إلى استفسار أو إجراء إضافي. قبل إجراء عمليات مهمة، قد تكون المعالجة المسبقة الخاصة بالمهمة ضرورية لتصفية البيانات وتنظيفها. في الأنظمة الفرعية المستقلة ل(IoT) التي تحتفظ بالمعالجة والتخزين في الشبكة بدلاً من طلب التخزين الدائم للبيانات، يمكن تنفيذ المعالجة داخل الشبكة استجابةً للطلبات المحلية أو في الوقت الفعلي.

بالنظر إلى الشكل، يمكن أن يأخذ تدفق البيانات في (IoT) واحدًا من ثلاث مسارات: مسار للأنظمة المستقلة داخل (IoT) ينتقل من الاستعلام إلى الإنتاج إلى المعالجة داخل الشبكة ثم التسليم، وهو مسار يبدأ من الإنتاج ويستمر إلى التجميع والتصفية / التجميع / الاندماج، وينتهي بتسليم البيانات لبدء الاستعلامات (التي قد تكون عالمية أو

قريبة من الوقت الفعلي)، وأخيرًا، المسار الذي يمتد من الإنتاج إلى التجميع الإضافي، بما في ذلك المعالجة المسبقة وتخزين البيانات الدائم والأرشفة والمعالجة والتحليل المتعمقان.

بالنظر إلى دورة حياة البيانات هذه، هناك حاجة إلى حلول إدارة البيانات التي تتجاوز القدرات الحالية لإدارة البيانات التقليدية.

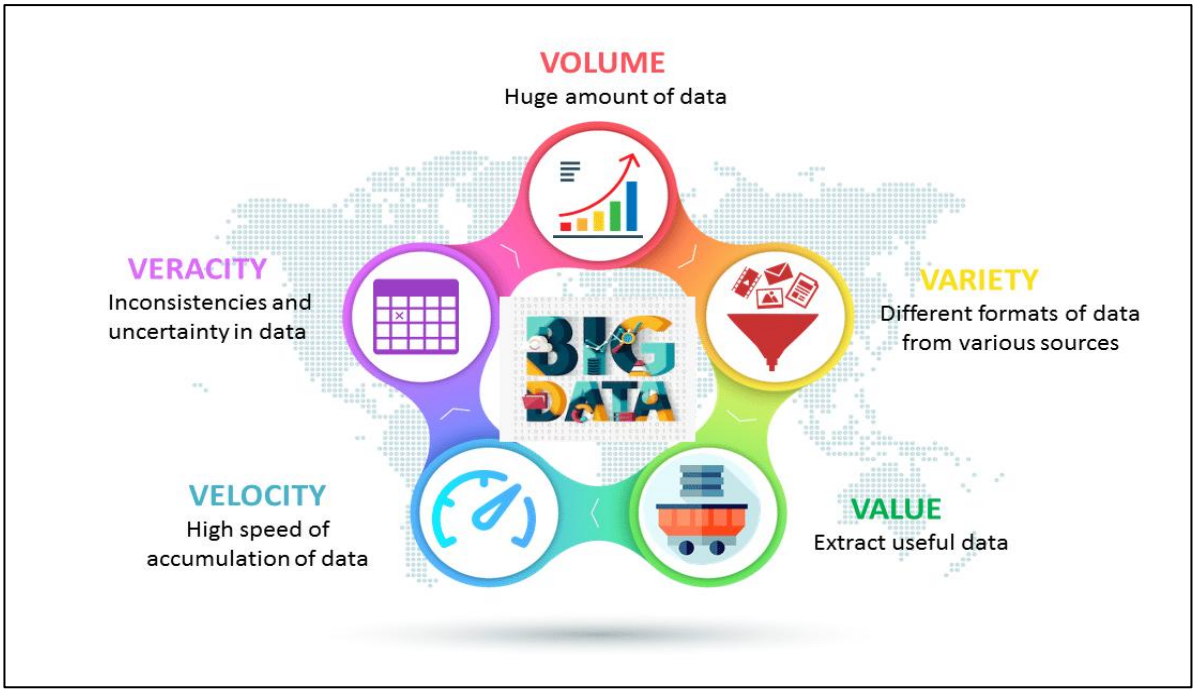
(IoT) والبيانات الكبيرة

ما هي البيانات الكبيرة؟

هو المصطلح المستخدم لوصف تجميع كميات هائلة من المعلومات من عدة مصادر، مثل النقرات على وسائل التواصل الاجتماعي والمعاملات المالية وغير ذلك. تم إنتاج أكثر من ٣٥٢ تريليون غيغابايت من البيانات، أو ٤٤ زيتابايت، في العامين الماضيين وحدهما في الكون الرقمي. يتم إنشاء ما يقدر بنحو ١,١٤٥ تريليون غيغابايت من البيانات كل يوم. نتيجة لذلك، تقوم الشركات والمؤسسات الأخرى بفرز كميات هائلة من البيانات لاكتشاف المعلومات الثاقبة التي قد توجه الخيارات الحاسمة.

تستخدم المنظمات مجموعة متنوعة من التقنيات، بما في ذلك برامج النمذجة والذكاء الاصطناعي مثل التعلم الآلي، لتقييم مثل هذه المعلومات الضخمة. يمكن لهذه الدراسات التنبؤ بالنتائج وتقديم المشورة وتوجيه الخيارات الحاسمة. من أجل التوصية بالأفلام ذات الصلة للعرض المستقبلي، على سبيل المثال، تجمع خدمات بث الفيديو مثل Netflix و Amazon Prime معلومات حول عادات البث لدى العملاء. يتم تخصيص إعلانات الويب لكل مستخدم بناءً على سجل البحث واستخدام الارتباط من قبل المتاجر عبر الإنترنت.

تم التعرف على العوامل الأربعة - الحجم، والتنوع، والسرعة، والصدق - من قبل علماء البيانات في شركة IBM باعتبارها أهم أربعة عوامل لفهم فكرة البيانات الضخمة.



يصف الحجم الأحجام الهائلة من البيانات التي يتم جمعها من خلال أجهزة الاستشعار والمعاملات عبر الإنترنت ووسائل التواصل الاجتماعي، ولكن لا يمكن التعامل معها أو تخزينها بطريقة تقليدية. هناك حاجة لأطر تحليلات البيانات مثل Amazon S3 أو Hadoop أو Spark للتخزين الموزع وتجميع ٤٦٣ إكسابايت من البيانات التي سيتم إنتاجها يوميًا بحلول عام ٢٠٢٥.

يشير التنوع إلى مجموعة واسعة من أنواع البيانات التي يتم جمعها، بما في ذلك أنواع البيانات غير المهيكلة مثل الصور الفوتوغرافية ومقاطع الفيديو التي يصعب تنظيمها في أطر عمل تقليدية. قد يتم تسخير هذه البيانات غير المهيكلة بواسطة أدوات تحليل قوية ودمجها مع مصادر بيانات أكثر بساطة لتقديم رؤى إضافية.

يشار إلى السرعة التي تتدفق بها البيانات إلى الخوادم بالسرعة. ستكون معالجة هذه البيانات مهمة ضخمة في عام ٢٠٢٠ مع ١,٧ ميغابايت من البيانات التي يتم إنشاؤها كل ثانية من مليارات عمليات البحث على Google ، وساعات من الأفلام المنشورة على YouTube، والتغريدات كل يوم.

الصدق هو مصطلح يستخدم لوصف صحة وأمانة جزء معين من البيانات، بما في ذلك موثوقية مصدر البيانات. تخسر الولايات المتحدة ٣,١ تريليون دولار سنويًا بسبب

رداءة جودة البيانات، مما يجعل من الضروري تقليل الازدواجية والقضاء على التحيز ومعالجة البيانات بطريقة منطقية للتطبيق المحدد أو قطاع الصناعة. حتى لو كان الذكاء الاصطناعي يتطور، فإن المحللين البشريين والأساليب الإحصائية التقليدية لا تزال مفيدة لتحديد صحة البيانات.

(IoT) والبيانات الكبيرة

يتكون المحيط الهائل من البيانات الضخمة من العديد من مصادر البيانات المختلفة، بما في ذلك بيانات (IoT). المجموعة الهائلة من أجهزة الاستشعار والأدوات والأجهزة الأخرى المترابطة والمتصلة ب(IoT) - والتي تقدر بنحو ٣٥,٨٢ مليار جهاز على مستوى العالم - تزيد بشكل كبير من كمية البيانات التي يتم جمعها. (IoT) له استخدامات عديدة في مجموعة متنوعة من الصناعات، بما في ذلك أتمتة التصنيع، والأجهزة الذكية للمستهلكين، والزراعة. يمكن أيضًا استخدام مستشعرات (IoT) لإدارة الأسطول ومراقبة الصحة عن بُعد وأغراض أخرى.

لكن قيمة البيانات التي تنتجها أجهزة (IoT) تعتمد على الاستنتاجات التي يمكن استخلاصها منها. تم إنشاء المنصات والتطبيقات والمنتجات الأخرى بواسطة موفري حلول (IoT) مثل Soracom و Balena لمساعدة الشركات والمؤسسات على إدارة أجهزة (IoT) الخاصة بهم وتغذية البيانات بأمان إلى الخدمات السحابية لتحليلها. تساعد هذه الحلول الشركات في الحصول على معلومات ثاقبة من الأحجام الهائلة من البيانات التي تنتجها أجهزة (IoT).

تتميزولكنها تكميلية

على الرغم من حقيقة أن كلاً من البيانات الضخمة و(IoT) يستلزم جمع كميات هائلة من البيانات، فإن أهدافها وطرقها تختلف بعدة طرق. من خلال الجمع بين جمع البيانات والتحليلات، فإن أحد الأهداف الرئيسية ل(IoT) هو السماح باتخاذ القرار في الوقت الفعلي. قد تقوم شركة التجارة الإلكترونية، على سبيل المثال، بمراقبة سلوك العميل بمرور الوقت واستخدام هذه المعلومات لتوفير محتوى وإعلانات مخصصة. في

المقابل، يجب على السيارات المستقلة الحصول بسرعة على المعلومات ومعالجتها من أجل الاستجابة بسرعة للظروف الخطرة المحتملة.

بينما تعتمد العديد من أجهزة (IoT) على الخوادم البعيدة التي يمكن الوصول إليها من خلال السحابة، تتبنى الصناعات الأخرى معالجة البيانات المتطورة لتقليل زمن الوصول من خلال السماح للأجهزة بمعالجة بعض البيانات محليًا. قد تستمر تقنيات البيانات الضخمة في المساعدة في بعض مهام (IoT)، مثل استخدام التحليلات التنبؤية للتنبؤ بمشكلات المعدات الوشيكة ومنع فترات التوقف الباهظة.

البيانات الضخمة و(IoT) لها مصادر بيانات مختلفة. الهدف الأساسي لتحليلات البيانات الضخمة هو التنبؤ بالسلوك والعثور على الأنماط أو الاتجاهات من خلال التركيز على القرارات البشرية. من ناحية أخرى، يمكن لأجهزة (IoT) أن تتعلم من البيانات التي ينشئها المستخدم، ولكنها تعتمد أيضًا إلى حد كبير على البيانات التي تم إنشاؤها بواسطة الآلة لتحقيق الأهداف الموجهة نحو الماكينة مثل تحسين أداء المعدات، وإجراء الصيانة التنبؤية، وتتبع الأصول.

الأمان والخصوصية في (IoT)



المخاطر الأمنية والتحديات

تشير (IoT) إلى الشبكة المترابطة للأجهزة المادية والمركبات والأجهزة المنزلية وغيرها من الأشياء المضمنة مع أجهزة الاستشعار والبرامج والاتصال. تتواصل هذه الأجهزة مع بعضها البعض ومع الإنترنت، مما ينتج عنه كميات هائلة من البيانات التي يمكن تحليلها واستخدامها لتحسين الكفاءة والإنتاجية والراحة. ومع ذلك، مع زيادة عدد الأجهزة المتصلة، تزداد أيضًا احتمالية المخاطر والتحديات الأمنية.

نقاط ضعف الجهاز

أحد المخاطر الأمنية الرئيسية ل(IoT) هو عدم وجود تدابير أمنية مناسبة في أجهزة (IoT). تم تصميم العديد من هذه الأجهزة دون اعتبار الأمان ميزة رئيسية، ونتيجة لذلك، يمكن أن تكون عرضة لهجمات مثل البرامج الضارة أو انتهاكات البيانات أو الوصول غير المصرح به. يمكن للمتسللين استغلال نقاط الضعف هذه للوصول إلى البيانات الحساسة أو للتحكم في الأجهزة، مما قد يتسبب في ضرر جسدي أو ضرر.

سلامة البيانات وسريتها

تنشئ أجهزة (IoT) كميات كبيرة من البيانات التي يتم إرسالها عبر الشبكات وتخزينها في الخوادم السحابية. يمكن اعتراض هذه البيانات أو التلاعب بها أو تسريبها، مما قد يؤدي إلى انتهاكات الخصوصية أو اتخاذ قرارات غير صحيحة. على سبيل المثال، يمكن اختراق منظم الحرارة الذكي، ويمكن أن تتغير درجة الحرارة، مما يؤدي إلى الشعور بعدم الراحة أو حتى الأذى الجسدي. وبالمثل، يمكن اختراق كاميرا أمنية واستخدام اللقطات لأغراض شائنة.

قنوات الاتصال غير الآمنة

غالبًا ما تتواصل أجهزة (IoT) عبر قنوات غير آمنة، مثل Wi-Fi أو Bluetooth، مما يجعلها عرضة للتنصت أو هجمات الرجل في الوسط. على سبيل المثال، يمكن للمتسلل اعتراض البيانات المنقولة بين ساعة ذكية وهاتف ذكي، وسرقة معلومات حساسة مثل أرقام بطاقات الائتمان أو بيانات اعتماد تسجيل الدخول. بالإضافة إلى ذلك، تحتوي

العديد من أجهزة (IoT) على أسماء مستخدمين وكلمات مرور افتراضية يسهل تخمينها، مما يجعلها عرضة لهجمات القوة الغاشمة.

فقدان المعيار القياسي

التحدي الكبير الآخر الذي يواجه أمن (IoT) هو عدم وجود معايير أمان عالمية لأجهزة (IoT). يمكن أن يؤدي هذا النقص في التوحيد القياسي إلى ممارسات أمنية غير متسقة، مما يجعل من الصعب على الشركات المصنعة والمستهلكين التأكد من أن أجهزتهم آمنة. بالإضافة إلى ذلك، غالبًا ما تكون هناك مشكلات في التوافق بين أجهزة (IoT) المختلفة، مما قد يجعل إنشاء إطار أمان شامل أمرًا صعبًا.

مخاوف الخصوصية

أثار انتشار أجهزة (IoT) مخاوف كبيرة بشأن الخصوصية فيما يتعلق بجمع البيانات وتخزينها واستخدامها. بعض مخاوف الخصوصية الرئيسية في (IoT) هي:

جمع البيانات المجتاحة

تجمع أجهزة (IoT) كميات هائلة من البيانات، غالبًا بدون موافقة أو معرفة صريحة من المستخدم. على سبيل المثال، قد يجمع التلفزيون الذكي معلومات حول العروض أو الأفلام التي يشاهدها المستخدم، بينما قد يقوم منظم الحرارة الذكي بجمع البيانات حول تفضيلات درجة حرارة المستخدم. يمكن أن يؤدي هذا النوع من جمع البيانات إلى انتهاكات محتملة للخصوصية ويمكن أن يكون مقلقًا بشكل خاص عندما لا يكون المستخدمون على دراية بالبيانات التي يتم جمعها.

تجميع البيانات وتنميطها

يمكن أن يؤدي الجمع بين البيانات من أجهزة (IoT) المختلفة إلى ملفات تعريف مفصلة للمستخدم، والتي يمكن استخدامها للتسويق الغازي أو حتى المراقبة. على سبيل المثال، يمكن دمج البيانات التي تم جمعها من ساعة ذكية وجهاز تلفزيون ذكي ومكبر صوت ذكي لإنشاء ملف تعريف مفصل لعادات المستخدم وتفضيلاته. يمكن أن يكون

هذا النوع من التنميط مقلقًا بشكل خاص عندما لا يكون المستخدمون على دراية بمدى البيانات التي يتم جمعها أو كيفية استخدامها.

الخرق في البيانات

يمكن أن يؤدي الوصول غير المصرح به إلى بيانات جهاز (IoT) إلى الكشف عن معلومات حساسة، مثل البيانات الشخصية أو بيانات الموقع أو المعلومات المالية. على سبيل المثال، قد يؤدي خرق البيانات في شركة لأمن المنازل إلى الكشف عن لقطات فيديو من الكاميرات الأمنية للعملاء. يمكن أن يكون هذا النوع من خرق البيانات مقلقًا بشكل خاص عندما يعتمد المستخدمون على أجهزة (IoT) من أجل سلامتهم وأمنهم.

التحكم غير الكافي للمستخدم

قد لا يمتلك المستخدمون تحكمًا كافيًا في كيفية جمع بيانات (IoT) الخاصة بهم وتخزينها واستخدامها، مما يؤدي إلى انتهاكات محتملة للخصوصية. على سبيل المثال، قد يقوم المتحدث الذكي بتسجيل المحادثات دون معرفة المستخدم أو موافقته، مما يؤدي إلى انتهاكات محتملة للخصوصية. قد لا يتمكن المستخدمون أيضًا من حذف البيانات التي تم جمعها، أو قد لا يتحكمون في كيفية مشاركة بياناتهم مع شركات خارجية.

الحلول الخاصة بالأمن و أفضل الممارسات

يعد تنفيذ الحلول الأمنية وأفضل الممارسات أمرًا بالغ الأهمية لمعالجة مخاوف الخصوصية وأمان (IoT). بعض الحلول وأفضل الممارسات التي يمكن تنفيذها هي:

التصميم الآمن للجهاز

يجب تصميم أجهزة (IoT) مع مراعاة الأمان، بما في ذلك تنفيذ آليات مصادقة وتشفير قوية. يجب على مصنعي الأجهزة إجراء تقييمات واختبارات أمنية شاملة أثناء مرحلة التصميم لتحديد ومعالجة الثغرات الأمنية المحتملة.

التحديثات المنتظمة وإدارة الترميم

يجب أن تتلقى أجهزة (IoT) تحديثات برامج منتظمة وتصحيحات أمان للحماية من الثغرات الأمنية المعروفة. تساعد التحديثات المنتظمة في ضمان حماية الأجهزة من أحدث التهديدات، ويمكن لتصحيحات الأمان إصلاح الثغرات الأمنية التي تم تحديدها.

تجزئة الشبكة

يجب عزل أجهزة (IoT) عن الشبكات والأجهزة الأخرى، مما يحد من أسطح الهجوم المحتملة. يمكن أن يساعد تقسيم الشبكة في منع الوصول غير المصرح به إلى المعلومات الحساسة وتقليل تأثير خرق الأمان.

التقليص من البيانات وإخفاء الهوية

يمكن أن يساعد الحد من جمع البيانات وتخزينها، وكذلك إخفاء هوية البيانات، في حماية خصوصية المستخدم. يتضمن تقليل البيانات فقط جمع البيانات الضرورية للغرض المقصود من الجهاز، بينما يتضمن إخفاء الهوية إزالة معلومات التعريف الشخصية من مجموعات البيانات لحماية خصوصية المستخدم.

تشمل حلول الأمان الأخرى وأفضل الممارسات التي يمكن تنفيذها ما يلي:

- تنفيذ آليات المصادقة متعددة العوامل
- استخدام جدران الحماية لتقييد الوصول إلى أجهزة (IoT)
- تنفيذ أنظمة كشف ومنع التسلل
- إجراء عمليات تدقيق وتقييم أمنية منتظمة

الأطر والمعايير الأمنية لـ (IoT)

هناك العديد من أطر ومعايير أمان (IoT) التي تم تطويرها من قبل العديد من المنظمات لتوجيه تطوير وتنفيذ أجهزة وأنظمة (IoT) الآمنة. فيما يلي بعض الأمثلة على أطر ومعايير أمان (IoT) البارزة:

- برنامج NIST للأمن السيبراني ل(IoT): طور المعهد الوطني للمعايير والتكنولوجيا (NIST) برنامج الأمن السيبراني لبرنامج (IoT) الذي يوفر إرشادات وأفضل الممارسات لتأمين أجهزة وأنظمة (IoT). يشتمل البرنامج على إطار عمل لتحسين الأمن السيبراني للبنية التحتية الحيوية، بالإضافة إلى منشورات حول تأمين أجهزة (IoT).
- سلسلة معايير :ISA / IEC 62443 قامت الجمعية الدولية للأتمتة (ISA) واللجنة الكهرو تقنية الدولية (IEC) بتطوير سلسلة معايير ISA / IEC 62443 للأتمتة الصناعية وأنظمة التحكم. توفر هذه المعايير إرشادات لتأمين أنظمة التحكم الصناعية وقد تم تبنيها على نطاق واسع في مختلف الصناعات.
- مشروع :OWASP Internet of Things يحتوي مشروع أمان تطبيق الويب المفتوح (OWASP) على مشروع (IoT) الذي يوفر إرشادات حول أمان (IoT)، بما في ذلك نمذجة التهديدات واختبار الأمان ومبادئ تصميم الأمان.
- إطار عمل أمان الإنترنت الصناعي التابع لاتحاد الإنترنت الصناعي (IIC): طورت IIC إطار أمان الإنترنت الصناعي (IISF)، والذي يوفر إرشادات لتأمين أنظمة (IoT) الصناعية. يتضمن إطار العمل أفضل الممارسات والمبادئ التوجيهية والبنية المرجعية لتأمين أجهزة وأنظمة (IoT) في البيئات الصناعية.

يمكن أن يساعد تنفيذ أطر ومعايير أمان (IoT) هذه في ضمان تطوير أجهزة وأنظمة (IoT) وتنفيذها بشكل آمن، مما يقلل من مخاطر تهديدات الأمن السيبراني ويحمي خصوصية المستخدم. ومع ذلك، من المهم ملاحظة أن هذه الأطر والمعايير ليست حلاً واحدًا يناسب الجميع ويجب تخصيصها وتكييفها مع حالات وبيئات استخدام (IoT) المحددة.

التشفير في (IoT)

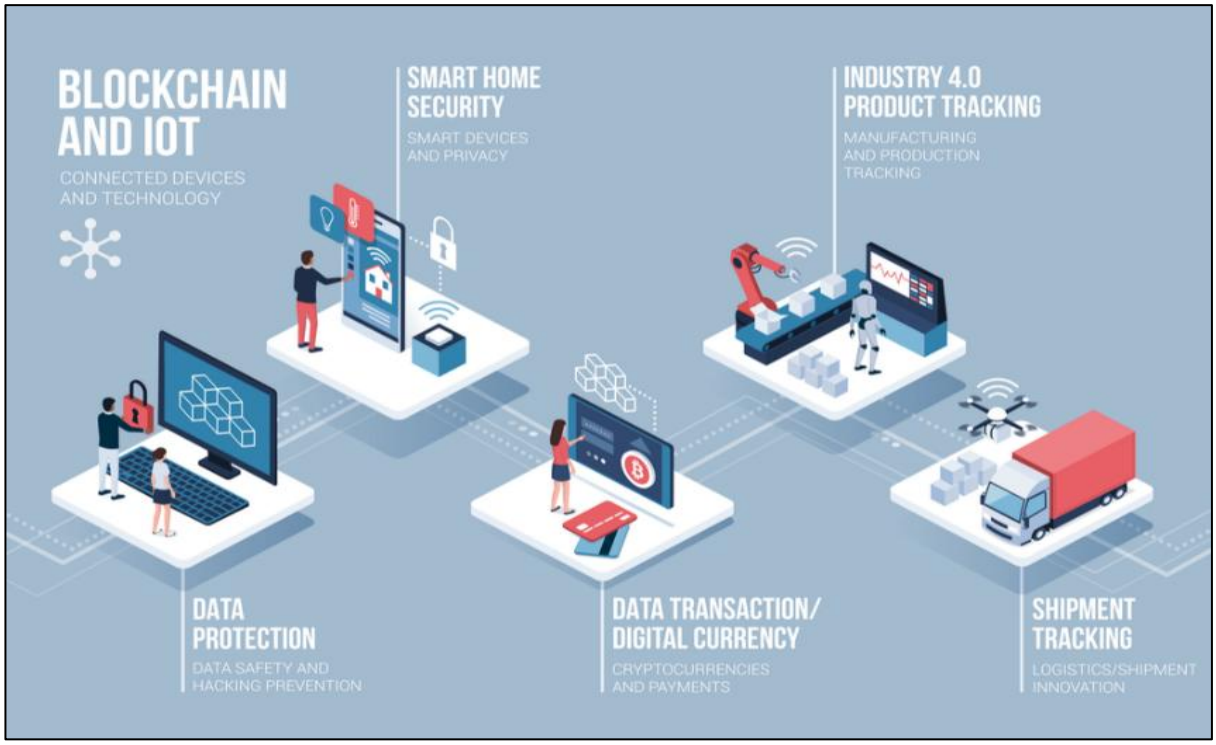
يلعب التشفير دورًا حيويًا في ضمان أمان أجهزة وأنظمة (IoT). يوفر آليات لتأمين البيانات أثناء الإرسال، والتحقق من صحة البيانات، وضمان سلامة البيانات. يعد

استخدام التشفير ضروريًا لحماية البيانات الحساسة مثل المعلومات الشخصية والبيانات المالية وغيرها من المعلومات السرية من التهديدات الإلكترونية.

هناك العديد من تقنيات التشفير المستخدمة في (IoT)، بما في ذلك التشفير المتماثل وغير المتماثل ووظائف التجزئة وإدارة المفاتيح. يتضمن التشفير المتماثل استخدام مفتاح مشترك واحد لكل من تشفير وفك تشفير البيانات أثناء الإرسال. يستخدم التشفير غير المتماثل زوجًا من المفاتيح بين القطاعين العام والخاص للتبادل الآمن للمفاتيح والتوقيعات الرقمية. تُستخدم وظائف التجزئة لضمان تكامل البيانات وإنشاء التوقيعات الرقمية. إدارة المفاتيح هي عملية إنشاء مفاتيح التشفير وتخزينها وتوزيعها بأمان.

يوفر استخدام التشفير في (IoT) العديد من الفوائد، بما في ذلك الحماية من التنصت والعبث والتهديدات الإلكترونية الأخرى. من خلال ضمان سرية البيانات وسلامتها ومصداقيتها، تساعد تقنيات التشفير في الحفاظ على الثقة في أجهزة وأنظمة (IoT). من المهم تنفيذ تقنيات التشفير المناسبة وأفضل الممارسات لضمان أمان أجهزة وأنظمة (IoT).

نظام (Blockchain) لحفظ الأمن في (IoT)



يعد أمان (IoT) مشكلة مهمة يجب معالجتها لضمان التشغيل الآمن والموثوق للأجهزة والأنظمة المتصلة. أدى انتشار أجهزة (IoT) وترابطها إلى ظهور مخاطر وتحديات أمنية جديدة، مثل الوصول غير المصرح به، وانتهاكات البيانات، وانتهاكات الخصوصية. يمكن أن تكون تقنية Blockchain حلاً واعدًا لهذه المشكلات من خلال توفير نظام أساسي لامركزي وشفاف ومقاوم للعبث لتخزين البيانات والاتصال.

تتمثل إحدى الفوائد الرئيسية لـ blockchain لأمان (IoT) في تأمين هوية الجهاز والمصادقة. يمكن استخدام Blockchain لتخزين هويات الجهاز بشكل آمن وتمكين المصادقة الآمنة بين الأجهزة، مما يجعل من الصعب على المهاجمين انتحال هويات الجهاز أو التلاعب بها. من خلال الاستفادة من تقنيات التشفير والإجماع الموزع، يمكن أن توفر blockchain طريقة آمنة وموثوقة لتأسيس الثقة بين أجهزة (IoT).

هناك مجال آخر يمكن أن تساعد فيه blockchain في تحسين أمان (IoT) وهو تكامل البيانات ومصدرها. يمكن أن تضمن Blockchain سلامة البيانات ومصدرها من خلال تسجيل تاريخ غير قابل للتغيير لمعاملات البيانات. من خلال تخزين البيانات على

منصة لا مركزية ومقاومة للعبث، يمكن لـ blockchain توفير سجل شفاف وقابل للتدقيق لمعاملات البيانات، مما يسهل اكتشاف ومنع الوصول غير المصرح به أو التلاعب بالبيانات.

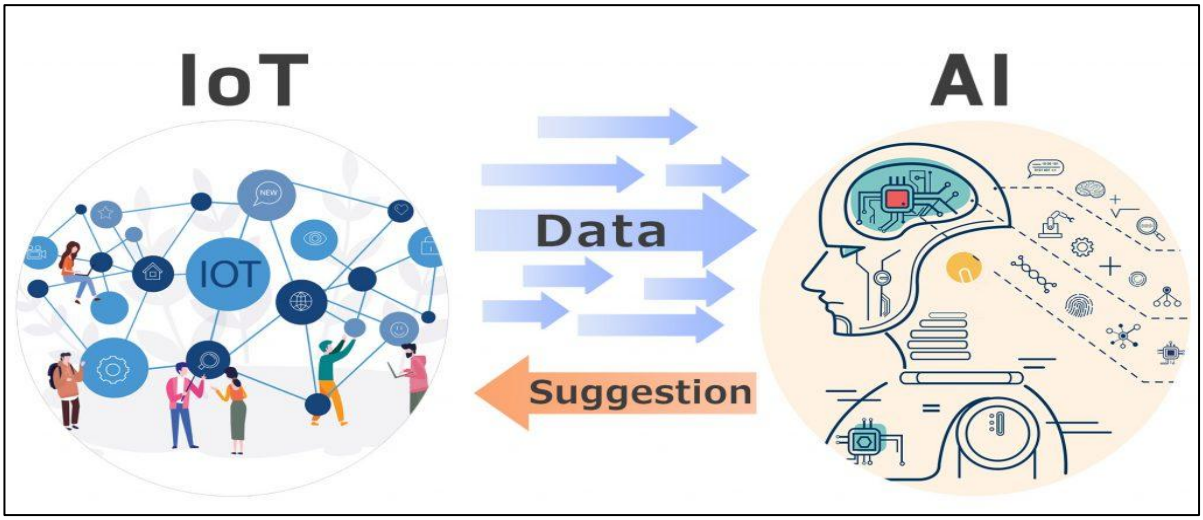
بالإضافة إلى ذلك، يمكن للعقود الذكية القائمة على blockchain تسهيل عمليات اتخاذ القرار المؤتمتة في أنظمة (IoT)، مما يقلل الحاجة إلى التدخل البشري والأخطاء المحتملة. يمكن أن تساعد العقود الذكية في أتمتة المهام مثل تحليل البيانات وتخصيص الموارد واتخاذ القرار، مما يجعل أنظمة (IoT) أكثر كفاءة وموثوقية.

يمكن أن توفر Blockchain أيضًا حل تخزين بيانات لامركزي، مما يجعل من الصعب على المهاجمين اختراق البيانات من خلال نقطة فشل واحدة. من خلال توزيع البيانات عبر شبكة من العقد، يمكن أن توفر blockchain بنية تحتية لتخزين البيانات أكثر قوة ومرونة وأقل عرضة للهجمات.

يعد التحكم في الوصول ومشاركة البيانات من المجالات الأخرى حيث يمكن أن تساعد blockchain في تحسين أمان (IoT). من خلال الاستفادة من تقنيات التشفير والعقود الذكية، وتتيح تمكين التحكم في الوصول الآمن ومشاركة البيانات بين أجهزة (IoT) والمستخدمين. يمكن أن تساعد أيضًا في الحفاظ على خصوصية المستخدم من خلال تمكين المعاملات المجهولة ومشاركة البيانات دون الكشف عن هوية الأطراف المعنية.

في الختام، تتمتع تقنية blockchain بإمكانية إحداث ثورة في أمان (IoT) من خلال توفير نظام أساسي لامركزي وشفاف ومقاوم للعبث لتخزين البيانات والاتصال. من خلال معالجة المخاطر والتحديات الأمنية، وتنفيذ أفضل الممارسات، والاستفادة من التقنيات مثل التشفير وblockchain، يمكننا إنشاء نظام بيئي (IoT) أكثر أمانًا وجدارة بالثقة.

نظام (IoT) والذكاء الاصطناعي



إن (IoT) عبارة عن شبكة من الأجهزة المادية والمركبات والأجهزة المنزلية والعناصر الأخرى المضمنة في الإلكترونيات والبرامج وأجهزة الاستشعار واتصال الشبكة، مما يسمح لهذه الكائنات بجمع البيانات وتبادلها. يولد النظام البيئي ل(IoT) كميات هائلة من البيانات كل يوم، ويمكن استخدام هذه البيانات لاكتساب رؤى، وتحسين العمليات، وتحسين قدرات اتخاذ القرار.

ومع ذلك، يمكن أن تكون معالجة هذه البيانات وتحليلها مهمة صعبة، خاصةً عندما تكون البيانات غير منظمة ومتنوعة ومتغيرة باستمرار. هذا هو المكان الذي يأتي فيه الذكاء الاصطناعي. يمكن للذكاء الاصطناعي أن يساعد أجهزة (IoT) في معالجة وتحليل واتخاذ القرارات بناءً على البيانات التي تجمعها في الوقت الفعلي.

تمكّن خوارزميات الذكاء الاصطناعي أجهزة (IoT) من التعلم من البيانات التي تجمعها وتكييف سلوكها وفقًا لذلك. على سبيل المثال، يمكن لمنظم الحرارة الذكي التعرف على تفضيلات مستخدميه وضبط إعدادات درجة الحرارة تلقائيًا. يؤدي هذا إلى تحسين كفاءة الطاقة وتوفير التكاليف.

وبالمثل، يمكن لخوارزميات الذكاء الاصطناعي تحسين العمليات الصناعية من خلال التنبؤ باحتياجات الصيانة، واكتشاف الحالات الشاذة، وتحديد الأعطال المحتملة قبل حدوثها. يؤدي هذا إلى تقليل وقت التوقف عن العمل وتحسين الإنتاجية وزيادة السلامة.

حالة استخدام أخرى للذكاء الاصطناعي في (IoT) هي المدن الذكية. يمكن أن تساعد خوارزميات الذكاء الاصطناعي في إدارة تدفق حركة المرور وتحسين إدارة النفايات وتقليل استهلاك الطاقة في المباني العامة. يؤدي هذا إلى تحسين نوعية الحياة للسكان وتقليل التأثير البيئي.

في الختام، يعد الذكاء الاصطناعي مكونًا مهمًا في النظام البيئي ل(IoT). إنه يمكّن الأجهزة من معالجة كميات هائلة من البيانات، واستخراج رؤى ذات مغزى، واتخاذ القرارات في الوقت الفعلي. من خلال الاستفادة من خوارزميات الذكاء الاصطناعي، يمكن أن تصبح أنظمة (IoT) أكثر كفاءة وتكيفًا وذكاءً، مما يؤدي إلى توفير التكاليف وتحسين الإنتاجية وتحسين قدرات اتخاذ القرار.

التعلم الآلي في (IoT)

التعلم الآلي (ML) هو مجموعة فرعية من الذكاء الاصطناعي (AI) تتضمن تدريب خوارزميات للتعرف على الأنماط وإجراء تنبؤات بناءً على البيانات. يمكن استخدام خوارزميات ML للتحليل والتعلم من كميات هائلة من البيانات التي تم جمعها بواسطة أجهزة (IoT). يساعد استخدام ML في أنظمة (IoT) في إجراء تنبؤات وتحديد الأنماط وتحسين أداء الجهاز.

الصيانة التنبؤية هي أحد التطبيقات الأساسية لتعلم الآلة في (IoT). تتضمن الصيانة التنبؤية استخدام البيانات التي تم جمعها بواسطة أجهزة الاستشعار وأجهزة (IoT) الأخرى للتنبؤ بالوقت الذي ستكون فيه الصيانة مطلوبة قبل حدوث العطل. يمكن تدريب خوارزميات ML على التعرف على الأنماط في البيانات التي تشير إلى احتمال فشل الجهاز. يسمح هذا بإجراء الصيانة الوقائية قبل حدوث العطل، مما يقلل من وقت التوقف عن العمل ويحسن الكفاءة.

يعد اكتشاف الشذوذ تطبيقًا آخر لتعلم الآلة في (IoT). يتضمن اكتشاف الشذوذ استخدام خوارزميات ML لتحديد أنماط البيانات التي تنحرف عن القاعدة. على سبيل المثال، قد تتم برمجة جهاز (IoT) لمراقبة درجة حرارة الجهاز في المصنع. إذا ارتفعت درجة الحرارة فجأة، فقد يطلق الجهاز تنبيهًا للإشارة إلى احتمال وجود مشكلة في الجهاز. يمكن

تدريب خوارزميات ML على التعرف على هذه الحالات الشاذة وتقديم رؤى حول ما قد يسببها.

التنبؤ بالطلب هو تطبيق آخر لتعلم الآلة في (IoT). من خلال تحليل البيانات التي تم جمعها بواسطة أجهزة (IoT) ، يمكن استخدام خوارزميات ML للتنبؤ بالطلب المستقبلي على المنتجات والخدمات. يمكن استخدام هذه المعلومات لتحسين إدارة الإنتاج والمخزون، مما يضمن توفر المنتجات المناسبة بالكميات المناسبة في الوقت المناسب.

يمكن أن يؤدي استخدام ML في أنظمة (IoT) إلى تحسين الكفاءة وتقليل وقت التوقف عن العمل وتحسين قدرات اتخاذ القرار. يمكن أن تساعد خوارزميات ML المؤسسات على التنبؤ بالوقت الذي ستكون فيه الصيانة مطلوبة، وتحديد الحالات الشاذة في البيانات، وتوقع الطلب على المنتجات والخدمات. مع نشر المزيد من أجهزة (IoT)، من المرجح أن يصبح استخدام ML في (IoT) ذا أهمية متزايدة.

التعلم العميق (DL) في (IoT)

التعلم العميق هو مجموعة فرعية من ML التي تستخدم الشبكات العصبية لتقليد عملية صنع القرار في الدماغ البشري. تتكون نماذج التعلم العميق من طبقات متعددة من الخلايا العصبية المترابطة التي تعمل معًا لمعالجة البيانات وتحليلها. تتعلم النماذج من مجموعات البيانات الكبيرة وتحسن دقتها بمزيد من البيانات.

تولد أجهزة (IoT) كميات كبيرة من البيانات من مصادر مختلفة، بما في ذلك أجهزة الاستشعار والكاميرات ومصادر أخرى. يمكن استخدام هذه البيانات لتطوير وتدريب نماذج التعلم العميق لمجموعة واسعة من تطبيقات (IoT). يمكن أن يكون التعلم العميق فعالاً بشكل خاص في التعامل مع التعقيدات والفروق الدقيقة لهذه البيانات.

على سبيل المثال، في سياق (IoT)، يمكن استخدام تقنيات التعلم العميق للتعرف على الصور، وهو أمر مفيد في اكتشاف وتحديد الكائنات والأشخاص والحيوانات في تدفقات الفيديو في الوقت الفعلي. يمكن أيضًا استخدام التعلم العميق لمعالجة اللغة الطبيعية (NLP)، والتي يمكن أن تساعد في معالجة وتحليل البيانات النصية التي تم

إنشاؤها بواسطة أجهزة (IoT) مثل المساعدين الأذكياء وروبوتات المحادثة وقنوات الاتصال الأخرى.

يعد التعرف على الكلام مجالًا آخر يمكن أن يكون فيه التعلم العميق مفيدًا في تطبيقات (IoT). ينشئ المساعدون الصوتيون ومكبرات الصوت الذكية والأجهزة الأخرى التي يتم تنشيطها صوتيًا قدرًا هائلاً من البيانات الصوتية، والتي يمكن تحليلها ومعالجتها باستخدام نماذج التعلم العميق لتحسين دقة التعرف على الكلام.

باختصار، يمكن أن يتيح الجمع بين (IoT) والتعلم العميق إنشاء أنظمة ذكية يمكنها معالجة كميات هائلة من البيانات الناتجة عن الأجهزة المتصلة. من خلال الاستفادة من تقنيات التعلم العميق، يمكن لأنظمة (IoT) أن تعزز قدرتها على التعرف على الأنماط وتحديد الحالات الشاذة والتنبؤات، مما يتيح اتخاذ قرارات أفضل وتحسين الكفاءة والفعالية الكلية لتطبيقات (IoT).

تطبيقات (IoT) التي تعمل بالذكاء الاصطناعي

تعمل تطبيقات (IoT) التي تعمل بالذكاء الاصطناعي على تحويل العديد من الصناعات من خلال الاستفادة من قوة الذكاء الاصطناعي وتوصيل (IoT). هذه التطبيقات لديها القدرة على إحداث ثورة في طريقة عمل الشركات، مما يجعلها أكثر كفاءة وفعالية من حيث التكلفة واستدامة. فيما يلي بعض الأمثلة على تطبيقات (IoT) التي تعتمد على الذكاء الاصطناعي:

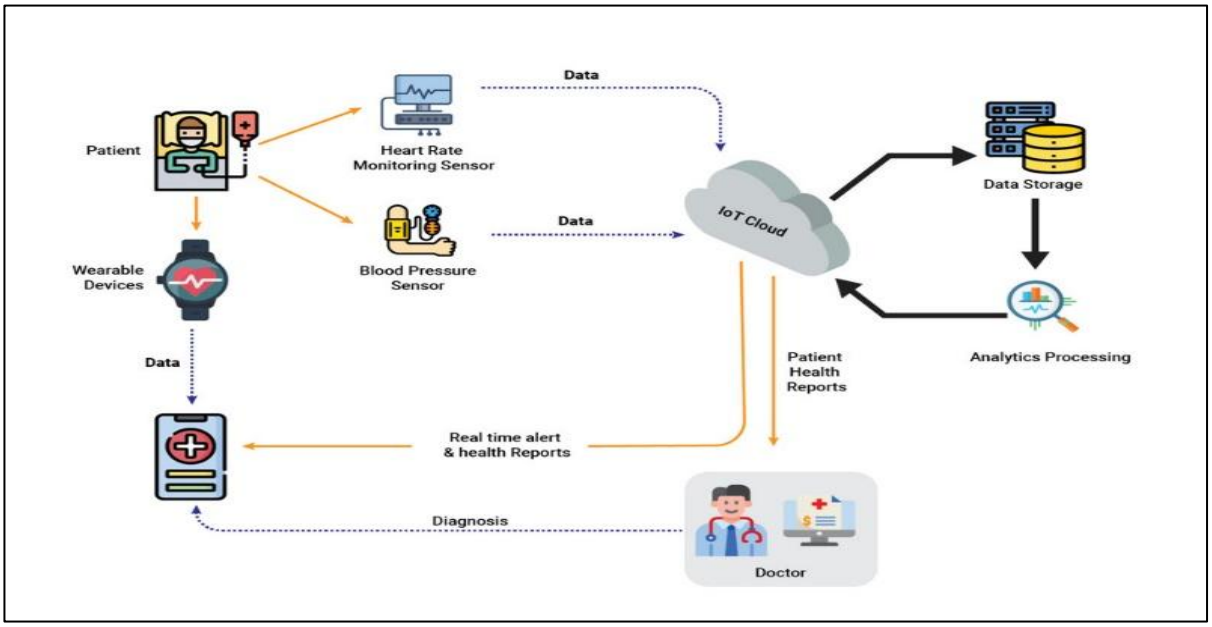
المنازل الذكية

يمكن لخوارزميات الذكاء الاصطناعي تحسين استهلاك الطاقة من خلال التحكم في أنظمة الإضاءة والتدفئة والتبريد بناءً على أنماط الإشغال والاستخدام. على سبيل المثال، يمكن لمنظم الحرارة الذكي معرفة تفضيلات صاحب المنزل وضبط درجة الحرارة وفقًا لذلك، مما يقلل من استهلاك الطاقة والتكاليف. بالإضافة إلى ذلك، يمكن لأنظمة الأمن المنزلي التي تعمل بالذكاء الاصطناعي استخدام البيانات من أجهزة (IoT) مثل الكاميرات وأجهزة استشعار الحركة لاكتشاف ومنع الاختراقات المحتملة.



القطاع الصحي

يمكن لأجهزة (IoT) التي تعمل بالذكاء الاصطناعي مراقبة العلامات الحيوية للمرضى والتنبؤ بالمشكلات الصحية المحتملة، مما يتيح التدخل المبكر والرعاية الشخصية. على سبيل المثال، يمكن للأجهزة القابلة للارتداء مثل الساعات الذكية وأجهزة تتبع اللياقة البدنية جمع البيانات وتحليلها مثل معدل ضربات القلب وأنماط النوم ومستويات النشاط البدني. يمكن استخدام هذه البيانات لمراقبة الحالات المزمنة مثل مرض السكري أو أمراض القلب، واكتشاف المشكلات الصحية المحتملة، وتنبيه المهنيين الطبيين للتدخل قبل تفاقم الحالة.

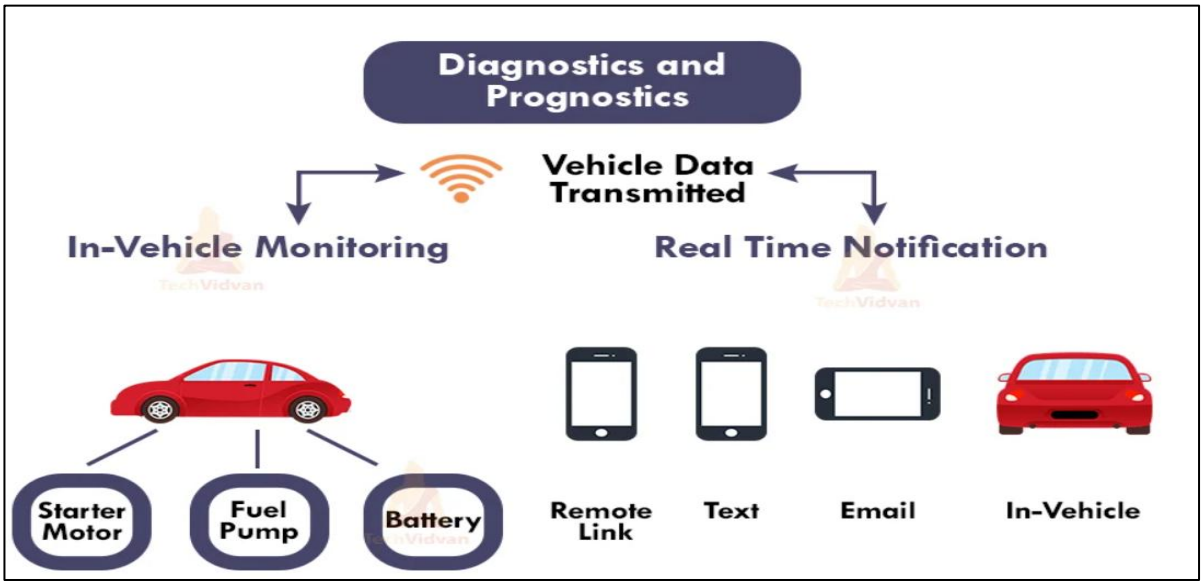


الزراعة

يمكن أن تساعد أنظمة (IoT) القائمة على الذكاء الاصطناعي المزارعين على مراقبة صحة المحاصيل وتحسين الري والتنبؤ بالمحاصيل وتحسين الكفاءة وتقليل استهلاك الموارد. على سبيل المثال، يمكن استخدام المستشعرات لقياس مستويات رطوبة التربة ودرجة الحرارة والرطوبة، والتي يمكن تحليلها باستخدام خوارزميات الذكاء الاصطناعي لتحديد الوقت الأمثل لزراعة المحاصيل وسقيها وحصادها. يمكن أن يساعد ذلك في تقليل استهلاك المياه وتحسين غلة المحاصيل.

النقل

يمكن استخدام الذكاء الاصطناعي لتحسين تدفق حركة المرور وتقليل الازدحام وتعزيز أنظمة النقل العام من خلال تحليل البيانات من البنية التحتية التي تدعم (IoT). على سبيل المثال، يمكن استخدام مستشعرات حركة المرور لجمع بيانات حركة المرور في الوقت الفعلي، والتي يمكن تحليلها باستخدام خوارزميات الذكاء الاصطناعي لتحديد أفضل الطرق للمركبات وتحسين تدفق حركة المرور. بالإضافة إلى ذلك، يمكن لأنظمة النقل العام استخدام أجهزة (IoT) التي تعمل بالذكاء الاصطناعي مثل أنظمة التذاكر الذكية لمراقبة أعداد الركاب وتعديل الخدمات وفقًا لذلك، مما يقلل الازدحام وأوقات الانتظار.



في الختام، تتمتع تطبيقات (IoT) التي تعمل بالذكاء الاصطناعي بإمكانية تحويل العديد من الصناعات من خلال الاستفادة من قوة الاتصال والذكاء. من خلال الاستفادة من أجهزة (IoT) وخوارزميات الذكاء الاصطناعي، يمكن للشركات تقليل التكاليف وتحسين الكفاءة وخلق فرص جديدة للنمو والابتكار.

أخلاقيات الذكاء الاصطناعي ونظام (IoT)

نظرًا لأن تقنيات الذكاء الاصطناعي و(IoT) أصبحت أكثر تكاملاً، تنشأ مخاوف أخلاقية بسبب الكم الهائل من البيانات التي تولدها أجهزة (IoT)، والتي يمكن

استخدامها لتدريب خوارزميات الذكاء الاصطناعي. تشمل الآثار الأخلاقية لاستخدام الذكاء الاصطناعي في أنظمة (IoT) قضايا مثل خصوصية البيانات والأمان والإنصاف. تتطلب هذه المشكلات نهجًا شاملاً يشرك جميع أصحاب المصلحة في تطوير واستخدام أنظمة (IoT) التي تعمل بالذكاء الاصطناعي.

أحد الاهتمامات الأخلاقية الرئيسية هو خصوصية البيانات. تجمع أجهزة (IoT) كمية هائلة من البيانات الشخصية، بما في ذلك الموقع والسلوك والتفضيلات، والتي يمكن استخدامها لتدريب خوارزميات الذكاء الاصطناعي. ومع ذلك، يمكن أيضًا إساءة استخدام هذه البيانات أو سرقتها، مما يؤدي إلى انتهاكات الخصوصية وسرقة الهوية. لمعالجة هذه المشكلة، يحتاج صانعو السياسات والمطورون والمستخدمون النهائيون إلى وضع لوائح خصوصية البيانات التي تحد من استخدام البيانات الشخصية وتضمن الشفافية في جمع البيانات وتخزينها.

قضية أخلاقية مهمة أخرى هي الأمن. غالبًا ما تكون أجهزة (IoT) متصلة بالإنترنت، مما يجعلها عرضة للهجمات الإلكترونية. قد يؤدي الخرق الأمني إلى سرقة البيانات أو التلاعب أو حتى الأذى الجسدي، كما هو الحال في أجهزة (IoT) الطبية. للتخفيف من هذه المخاطر، يجب تصميم أنظمة (IoT) التي تعمل بالذكاء الاصطناعي بميزات أمان قوية، مثل التشفير والتحكم في الوصول، ويجب إجراء تقييمات أمنية منتظمة لتحديد ومعالجة الثغرات الأمنية المحتملة.

أخيرًا، يمكن أن يثير استخدام الذكاء الاصطناعي في أنظمة (IoT) مخاوف تتعلق بالإنصاف. يمكن لخوارزميات الذكاء الاصطناعي أن تديم التحيز والتمييز إذا تم تدريبهم على مجموعات البيانات المتحيزة أو استخدام معايير اتخاذ القرار التمييزية. يمكن أن يؤدي هذا إلى معاملة غير عادلة للأفراد على أساس العرق أو الجنس أو الخصائص الأخرى. لمعالجة هذه المشكلة، يجب على المطورين التأكد من تدريب نماذج الذكاء الاصطناعي على مجموعات بيانات متنوعة وغير متحيزة واختبارها بانتظام من أجل الإنصاف والدقة.

في الختام، يتطلب ضمان الاستخدام المسؤول للذكاء الاصطناعي في أنظمة (IoT) الشفافية والمساءلة والالتزام بالإرشادات الأخلاقية. يحتاج صانعو السياسات

والمطورون والمستخدمون النهائيون إلى العمل معًا لإنشاء أطر تعزز الاستخدام الأخلاقي للذكاء الاصطناعي في (IoT) مع تعظيم الفوائد المحتملة. من خلال معالجة هذه المخاوف الأخلاقية، يمكننا إطلاق الإمكانات الكاملة لتقنيات الذكاء الاصطناعي و(IoT) مع حماية خصوصية الأفراد وأمنهم وتعزيز العدالة والمساواة.

الخاتمة

في الختام، أحدثت (IoT) ثورة في طريقة اتصال الأجهزة والتواصل مع بعضها البعض ومع المستخدمين. لقد مكّن من دمج الأجهزة غير المرتبطة تقليديًا بالإنترنت في النظام البيئي الرقمي، مما يوفر إمكانيات عديدة للابتكار والتحسين عبر مختلف الصناعات. من خلال ربط مليارات الأجهزة بالإنترنت، فإن (IoT) لديها القدرة على تعزيز الكفاءة والإنتاجية والراحة في مجالات مثل الرعاية الصحية والتصنيع والنقل والزراعة والطاقة. يمكن أن توفر البيانات التي تم إنشاؤها بواسطة أجهزة (IoT)، عند معالجتها وتحليلها بشكل فعال، رؤى قيمة ومعلومات قابلة للتنفيذ، مما يتيح اتخاذ قرارات أكثر ذكاءً وتحسين الأنظمة والعمليات. يحمل التبني الواسع النطاق ل(IoT) وعدًا كبيرًا لخلق عالم أكثر اتصالاً وذكاءً.