أكاديمية التعلم
Academy Of Learning

أمن إنترنت الأشياء والحوسبة السحابية

تحت إشراف
المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

الأهداف التفصيلية للمقرر

بنهاية هذا المقرر ستكون المتدربة قادرةً وبكفاءة على أن:

- يحدد مفهوم إنترنت الأشياء ومكوناته الأساسية وآلية عملها
- يشرح معمارية إنترنت الأشياء
- يصف تحديات توظيف إنترنت الأشياء في المؤسسات المختلفة
- يحدد مفهوم الحوسبة السحابية وأنواعها وخدماتها
- يبين النواحي الأمنية في الحوسبة السحابية
- يدرك علاقة الحوسبة السحابية بمجال إنترنت الأشياء
- يعدد التهديدات التي تواجه إنترنت الأشياء وكيفية التصدي لها
- يشرح دور تقنية سلاسل الكتل Blockchain في تأمين أنظمة إنترنت الأشياء

❖ فهرس الكتاب

أولاً: مقدمة إلى إنترنت الأشياء

في هذا الفصل سنتعرف على المواضيع التالية:

- **مفهوم إنترنت الأشياء ومميزاته**
- **مكونات إنترنت الأشياء**
- **معمارية إنترنت الأشياء**
- **أشكال إنترنت الأشياء**
- **توظيف إنترنت الأشياء في مراكز المعلومات**
- **إنترنت الأشياء الاجتماعي**

تمهيد

وفر الإنترنت اتصالاً عالمياً لم يقتصر على البشر، بل أصبح الاتصال يشمل الأشياء. ففي العقود الأخيرة اختُرع إنترنت الأشياء الذي أحدث ثورة في التفاعل بين العالم الرقمي والعالم المادي. في هذا الفصل سنتعرف على مفهوم إنترنت الأشياء وما المقصود بالأشياء. وما هي مميزاته، ومكوناته، ومعماريته، وأشكاله. وأيضا سنذكر كيف تم توظيف إنترنت الأشياء في مراكز المعلومات، وما هو إنترنت الأشياء الاجتماعي.

مفهوم إنترنت الأشياء ومميزاته

إنترنت الأشياء ((Internet of Things (IoT) هو عبارة عن شبكة من الأشياء التي تحتوي على تقنية مضمنة تسمح بالاتصال بالإنترنت، كما تُشير إلى الاتصال الذي يحدث بين هذه الأشياء والأجهزة والأنظمة الأخرى التي تدعم الإنترنت، ويمكن أن تكون هذه الأشياء آلات أو مكونات مادية أو حيوانات أو حتى أشخاصًا. يسمح إنترنت الأشياء (IoT) بالاتصال بالإنترنت بما يتجاوز الأجهزة التقليدية، مثل أجهزة الحاسوب والهواتف الذكية، ويمتد إلى مجموعة متنوعة من الأشياء اليومية.

ما المقصود بالأشياء؟ هي أشياء مادية يمكنها الاتصال بالإنترنت. من الأمثلة على أشياء الإنترنت منظمات الحرارة التابعة لجهاز التكييف، السيارات، المصابيح المنزلية، الساعات المنبهة وغيرها الكثير

ما هو إنترنت الأشياء؟

إنترنت الأشياء (IoT) هو شبكة من الأجهزة الذكية المترابطة التي تتبادل البيانات وتتواصل عبر الإنترنت دون تدخل بشري مباشر. يربط إنترنت الأشياء جميع الأجهزة الذكية المحيطة بالشبكة، تستخدم هذه الأجهزة أجهزة استشعار ومحركات للتواصل مع بعضها البعض، تستشعر المستشعرات الأنشطة المحيطة بينما تستجيب المشغلات للأنشطة المحسوسة، يمكن أن تكون الأجهزة عبارة عن هاتف ذكي ، أو غسالة ملابس ذكية ، أو ساعة ذكية ، أو تلفزيون ذكي ، أو سيارة ذكية ، وما إلى ذلك. افترض أن الحذاء الذكي متصل بالإنترنت، يمكنه جمع بيانات عن عدد الخطوات التي تم قطعها، يمكن للهاتف الذكي الاتصال بالإنترنت لعرض هذه البيانات، يحلل البيانات ويقدم عدد السعرات الحرارية المحروقة ونصائح اللياقة الأخرى للمستخدم.

مثال آخر هو الكاميرا المرورية الذكية التي يمكنها مراقبة الازدحام والحوادث، يرسل البيانات إلى بوابة تستقبل هذه البوابة البيانات من تلك الكاميرا بالإضافة إلى كاميرات أخرى مماثلة، كل هذه الأجهزة المتصلة تنشئ نظاماً ذكياً لإدارة حركة المرور، يقوم بمشاركة البيانات وتحليلها وتخزينها عبر السحابة، عند وقوع حادث، يقوم النظام بتحليل الأثر وإرسال التعليمات لإرشاد السائقين لتجنب وقوع الحادث.

وبالمثل، هناك العديد من الأمثلة في الرعاية الصحية والتصنيع وتوليد الطاقة والزراعة وغيرها الكثير، عيب واحد هو أنه يمكن أن تكون هناك مشكلات تتعلق بالأمان والخصوصية لأن الأجهزة تلتقط البيانات طوال اليوم بشكل عام، تعتبر إنترنت الأشياء تقنية ناشئة وستنمو بشكل كبير في المستقبل.

يتخطى التعريف المفهوم التقليدي (هو تواصل الأشخاص مع الحواسيب والهواتف الذكية عبر شبكة عالمية واحدة ومن خلال بروتوكول الإنترنت التقليدي المعروف)، فما يميز إنترنت الأشياء أنها تتيح للإنسان التحرر من المكان، أي أن الشخص يستطيع التحكم في الأدوات من دون الحاجة إلى التواجد في مكان محدّد للتعامل مع جهاز معين.

مميزات إنترنت الأشياء:

تقنية قوية مثل إنترنت الأشياء IOT لها -بدون مبالغة- المئات من المميزات التي تستطيع تحسين حياتنا، **ومن أهمها:**

١. أتمتة كل ما يمكن أتمتة

ستساعدنا تقنية إنترنت الأشياء على جعل كافة المهام الدورية والروتينية تتم بدون تدخلنا وبدون أي أخطاء، وهذا ما سيوفر نمط حياة مريح للبشر، كما سيساعد الأفراد على أن يصبحوا أكثر إنتاجية.

٢. توفير الكثير من الوقت

استخدام تقنية إنترنت الأشياء ستساعد البشرية على توفير مليارات الساعات يومياً، وذلك من خلال أتمتة كافة المهام الروتينية التي يقوم بها الإنسان عادة، مما سيساعدنا نحن البشر على التركيز على الأشياء المهمة أو تخصيص أوقات الفراغ للراحة أو للاستمتاع.

مثلاً؛ كم ساعة يتم هدرها شهرياً لفتح وقفل كراج سيارتك؟ بوجود إنترنت الأشياء مهام مثل هذه سوف يتم أداؤها بصورة آلية معدة مسبقاً لتوفر لك ساعات من الوقت كل شهر.

٣. تقليل استهلاكنا للطاقة

من خلال مراقبة والتحكم بجميع الأدوات والأجهزة سواء المنزلية أو غيرها سوف يمكن توفير كميات مهولة من الطاقة خاصة تلك المتعلقة بالإضاءة أو بالإهمال البشري، وبجانب تقليل استهلاكنا للطاقة ستساهم أيضاً بتقليل النفقات بشكل معقول والحد من الفاقد.

٤. الحد من الحوادث والمشاكل الصحية

باستخدام تقنية إنترنت الأشياء IOT في النقل والمواصلات وقطاع الصحة سيزداد معدل أعمار البشر، كما ستقل معدلات الوفاة من الحوادث والمشاكل الصحية بدرجة كبيرة.

٥. توفير الكثير من البيانات

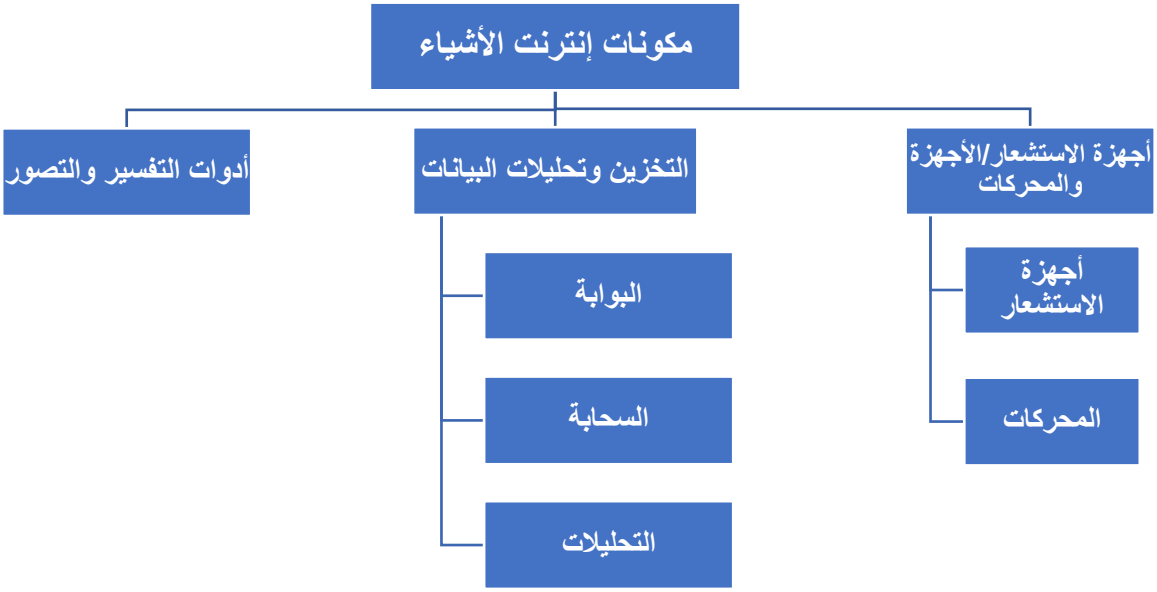
البيانات هي نفط القرن الواحد والعشرين، ولذا فأن مجرد توفير البيانات سوف يساهم في خلق موجة قوية للغاية من التحسين والتطوير سواء من جهة الخدمات أو المنتجات، بالإضافة إلى أنه سيساعد على التخصيص لكل فرد حسب سلوكه ونشاطاته وعاداته.

٦. الأمان والحماية

كون كل شيء مراقب سوف يمنحنا نوعاً من الإحساس بالأمان، كما أنه سيقلل بشكل كبير من نسب حدوث الجرائم أو حتى يمحيها تماماً... عدا بالطبع الإلكترونية منها، والأمان هنا لا يقصد فقط الأمان من الأذى والجرائم، بل أيضاً الأمان والحماية من الحوادث والمخاطر.

مكونات إنترنت الأشياء

يتكون إنترنت الأشياء من عدة مكونات رئيسية تعمل بمثابة اللبنات الأساسية لبناء نظام إنترنت الأشياء. يقدم هذا القسم استكشافا متعمقا للمكونات الرئيسية لإنترنت الأشياء. يتكون إنترنت الأشياء من ثلاث مكونات رئيسية: (١) أجهزة الاستشعار/الأجهزة، والمحركات; (٢) التخزين وتحليلات البيانات؛ و (٣) أدوات التفسير والتصور. يتم تصنيف كل من هذه إلى مكونات فرعية مختلفة. انظر إلى شكل ١.



شكل ١ مكونات إنترنت الأشياء

المكون الأول: أجهزة الاستشعار / الأجهزة والمحركات

أجهزة الاستشعار: تلعب المستشعرات دورا حاسما وأساسيا في نظام إنترنت الأشياء. بالنظر إلى أن إنترنت الأشياء يعمل من خلال جمع البيانات من البيئة المحيطة، فمن الضروري لجميع تطبيقات إنترنت الأشياء لدمج جهاز استشعار واحد أو أكثر لتلبية هذه الحاجة. السمة المميزة لأجهزة إنترنت الأشياء هي وعيها بالسياق، والذي أصبح ممكنا من خلال استخدام تكنولوجيا الاستشعار. أجهزة الاستشعار ليست مدمجة وفعالة من حيث التكلفة فحسب، بل إنها موفرة للطاقة أيضا. ومع ذلك، فهي تخضع لقيود مثل سعة البطارية وسهولة النشر. تم تقديم نظرة عامة على أنواع مختلفة من أجهزة الاستشعار أدناه.

أجهزة الاستشعار المتنقلة الهواتف الذكية، المنتشرة على نطاق واسع وشائعة الاستخدام، مجهزة بأجهزة استشعار مختلفة. نظرا لاستخدامها على نطاق واسع، يستكشف الباحثون إمكانية استخدام الهواتف الذكية كمكونات أساسية في بناء حلول إنترنت الأشياء الذكية. يمكن لهذه التطبيقات تسخير بيانات أجهزة الاستشعار من الهواتف الذكية لتوليد قيمة في المشاهد والنتائج. تتضمن بعض المستشعرات العامة الموجودة في الهواتف الذكية مقياس التسارع ونظام تحديد المواقع العالمي (GPS) ومقياس المغناطيسية ومستشعر الضوء ومستشعر القرب. تأتي بعض الهواتف الذكية، مثل Samsung Galaxy S٤، مزودة بأجهزة استشعار إضافية، بما في ذلك مقياس حرارة ومقياس ضغط جوي ومستشعر رطوبة.

أجهزة الاستشعار الطبية تعد صناعة الرعاية الصحية واحدة من أكثر المجالات تأثيرا حيث مهد الابتكار وإنترنت الأشياء الطريق. سهلت الأجهزة وأجهزة الاستشعار القابلة للارتداء المراقبة عن بعد للأطباء ومكنت الباحثين من جمع البيانات بشكل مستمر وفي الوقت الفعلي. تأتي هذه الأجهزة بأشكال مختلفة، مثل أساور المعصم والساعات الذكية وتصحيحات المراقبة. اكتسبت الساعات الذكية وأجهزة تتبع اللياقة البدنية، المعروفة بتعدد استخداماتها، شعبية بين المستهلكين. وبالمثل، برزت رقع المراقبة كرصيد قيم لقطاع الرعاية الصحية من خلال تمكين العلاج عن بعد للمرضى.

تلعب المستشعرات العصبية دورا حاسما في فهم طريقة عمل المستشعرات البشرية من خلال تمكيننا من فك تشفير إشارات الدماغ، وتقييم الحالة الحالية للدماغ، وعند الضرورة، تحسينها لتحسين التركيز والانتباه. يشار إلى هذه الممارسة عادة باسم الارتجاع العصبي.

أجهزة الاستشعار البيئية والكيميائية بينما تدير الأدوات التقليدية معلمات مثل درجة الحرارة والضغط، تلعب المستشعرات البيئية المتخصصة دورا مهما في تقييم جودة الهواء. تكتشف هذه المستشعرات الغازات والجسيمات، بينما تقيس أيضا مكونات الواجهات مثل درجة الحرارة، والرطوبة، والضغط، والتلوث. إلى جانب ذلك، تلعب المواد الكيميائية دورا حاسما في الكشف عن كل من المواد الكيميائية والكيميائية الحيوية. من بين التقنيات المبتكرة المتاحة الأنف الإلكتروني (الأنف الإلكتروني) واللسان الإلكتروني (اللسان الإلكتروني)، اللذان يعتمدان على التعرف على الأنماط لاستشعار المواد الكيميائية بناء على الرائحة والطعم. تجد هذه المستشعرات تطبيقات قيمة في المدن الذكية لمراقبة مستويات التلوث.

تقنية RFID لتحديد الترددات الراديوية (Radio-Frequency Identification(RFID ، التي تعمل كأجهزة استشعار، يجد استخداما واسع النطاق في تطبيقات إنترنت الأشياء المختلفة. على سبيل المثال، يتم استخدامه لتتبع المنتجات ضمن قوائم الجرد الواسعة أو مراقبة العناصر داخل متاجر البيع بالتجزئة الكبيرة.

المحركات: تلعب المحركات دورا حاسما وتعمل في تناقض مباشر مع أجهزة الاستشعار. إنها تحول الطاقة إلى حركة فيزيائية وعادة ما يتم وضعها على المحيط الخارجي للنظام. خذ، على سبيل المثال، سيناريو يتضمن نظام المنزل الذكي الذي يتضمن العديد من أجهزة الاستشعار والمحركات. في هذا الإعداد، تتلقى المشغلات إشارات من المستشعرات، واعتمادا على السياق، تنفذ إجراءات مثل قفل الأبواب، أو فتحها، أو تبديل الأضواء، أو الأجهزة الكهربائية، أو إيقاف تشغيلها، أو تنظيم درجة حرارة المنزل، أو ضبط أجهزة الإنذار لحالات الطوارئ. بشكل أساسي، تستجيب المشغلات للأوامر وتنفذها بناء على الإشارات التي تتلقاها من أجهزة الاستشعار أو الأجهزة الأخرى.

المكون الثاني: التخزين وتحليلات البيانات

التخزين وتحليلات البيانات جانب آخر مهم من إنترنت الأشياء هو إدارة الحجم الكبير للبيانات التي تم إنشاؤها وتبادلها بواسطة أجهزة إنترنت الأشياء بشكل مستمر. يمثل تخزين هذه البيانات تحديا كبيرا داخل شبكات إنترنت الأشياء. علاوة على ذلك، يجب أن تخضع البيانات التي تم جمعها من هذه الأجهزة للتطوير، معالجة، والتحليل لتمكين الأداء الفعال لنظام إنترنت الأشياء. في هذه العملية، تتعاون البوابات والخدمات السحابية والتحليلات للتعامل مع مهام تخزين البيانات ومعالجتها.

١) البوابة: تعمل البوابات، المصممة لتبسيط نظام إنترنت الأشياء، كوسيلة وسيطة للاتصال بين الأجهزة ونظام السحابة المركزية. الوظائف الرئيسية لبوابات إنترنت الأشياء مذكورة أدناه:

(أ) المعالجة المسبقة للبيانات تعمل بوابة إنترنت الأشياء كوسيط بين أجهزة الاستشعار وسحابة مركزي، حيث تجري تحليلات البيانات الأساسية قبل إعادة توجيه المعلومات مباشرة إلى السحابة. تؤدي هذه الطبقة مهام تصفية البيانات المحلية والتنظيف والمعالجة المسبقة وترجمة البروتوكول. خلال هذه العملية، قد تقوم أيضا بتجميع البيانات أو إزالتها أو تلخيصها لتحسين أوقات الاستجابة وخفض تكاليف الإرسال.

(ب) الحصول على البيانات في هذه الطبقة، يتم جمع البيانات من مصادر متعددة، وتحويلها إلى التنسيق المطلوب، ثم نقلها إلى طبقات المعالجة. يتمثل دور البوابة في هذه المرحلة في توفير اتصال آمن بين أجهزة إنترنت الأشياء وهياكل المعالجة.

(ج) إعادة توجيه البيانات والتخزين المؤقت يتمثل الدور الأساسي للبوابة في ضمان النقل الآمن للبيانات بين طبقة المستشعر والسحابة المركزية. بالإضافة إلى ذلك، تعمل هذه الطبقة كمستودع تخزين مؤقت للبيانات التي تم جمعها.

(د) إدارة الجهاز تسهل هذه الطبقة تكوين الجهاز في الوقت الفعلي، مما يسمح بإجراء تعديلات على حالات الرذيلة وأوضاع التشغيل وإقرارات الخطأ والمزيد.

(ه) التشخيص تحدد بوابة إنترنت الأشياء الأخطاء والأخطاء داخل طبقة التكنولوجيا بأكملها، بما في ذلك التشخيص الذاتي لبوابة إنترنت الأشياء نفسها.

٢) السحابة: تعمل السحابة كمحور مركزي لشبكة إنترنت الأشياء، حيث تتولى أدوارا محورية في معالجة البيانات وتخزينها وإدارتها. تشمل الخصائص الرئيسية للسحابة القدرة على تخزين ومعالجة البيانات الشاملة التي تم إنشاؤها بواسطة الأجهزة، وقابلية التوسع للتعامل مع آلاف الأجهزة دون عناء، والمرونة من خلال السماح بإضافة الأجهزة أو إزالتها حسب الحاجة دون الحاجة إلى إعادة تكوين النظام بالكامل، والإشراف والإدارة من قبل مزود الخدمة السحابية، والفعالية من حيث التكلفة. في حين أن الخدمات السحابية ليست إلزامية لإنترنت الأشياء، فإن التحول الأخير نحو حوسبة الحافة والضباب يمكن معالجة البيانات المحلية. ومع ذلك، يتم دمج السحابة في النظام لقابليتها للتوسع. التخزين وتقديم خدمة فعالة من حيث التكلفة. علاوة على ذلك، توفر الخدمات المستندة إلى السحابة وظائف أمنية مثل التشفير والمصادقة مع تمكين الوصول عن بعد والتحكم في أجهزة إنترنت الأشياء.

٣) التحليلات: يمثل هذا أحد أكثر الطبقات تعقيدا وحيوية داخل إنترنت الأشياء. وهو ينطوي على تحليل البيانات، وتوليد رؤى قيمة من خلال تطبيق خوارزميات التعلم الآلي المتنوعة (ML) وتقنيات التحليل الإحصائي. تشمل التطبيقات غير المألوفة للتحليلات في إنترنت الأشياء الكشف عن الحالات الشاذة والمراقبة البيئية، وإدارة الطاقة، والمدن الذكية، والزراعة.

المكون الثالث: أدوات التفسير والتصور

أدوات التفسير والتصور يعمل هذا الجزء بشكل أساسي كواجهة مستخدم (UI). توفر واجهة المستخدم منصة للمستخدمين للتفاعل مباشرة مع التطبيق أو النظام، مما يسهل الاتصال. لا يعتمد المستخدم في interface دائما على الشاشة. على سبيل المثال، يستخدم جهاز التحكم عن بعد الخاص بالتلفزيون واجهة مستخدم تتكون من أزرار متعددة، بينما تستجيب أجهزة مثل Amazon Echo لأوامر الاتصال الصوتي للتحكم. يعد تلقي الإخطار التلقائي ومراقبة المعلومات بشكل استباقي والتحكم في النظام عن بعد بعض الأمثلة الشائعة لواجهات المستخدم في أنظمة إنترنت الأشياء.

معمارية إنترنت الأشياء

تشير التقديرات المتفائلة إلى أن تصل أجهزة إنترنت الأشياء إلى ٧٥,٤٤ مليار جهاز بحلول نهاية عام ٢٠٢٥، وعلاوة على ذلك، من المتوقع أن يصل نصيب الفرد إلى ١٠ أجهزة ذكية بحلول عام ٢٠٢٥ مقارنة بجهازين ذكيين في عام ٢٠١٥. بسبب متطلبات الاتصال السلس لعدد كبير من الكائنات غير المتجانسة، يستلزم إنترنت الأشياء بنية مرنة الطبقات. في هذا الاتجاه، على الرغم من اقتراح عدد متزايد من البنى لإنترنت الأشياء مع التعاون الوثيق بين البحث والصناعة، حتى الآن، لم يتلق أي منها إجماعا مشتركا، وبالتالي لم يتم إنشاء نموذج مرجعي راسخ بعد.

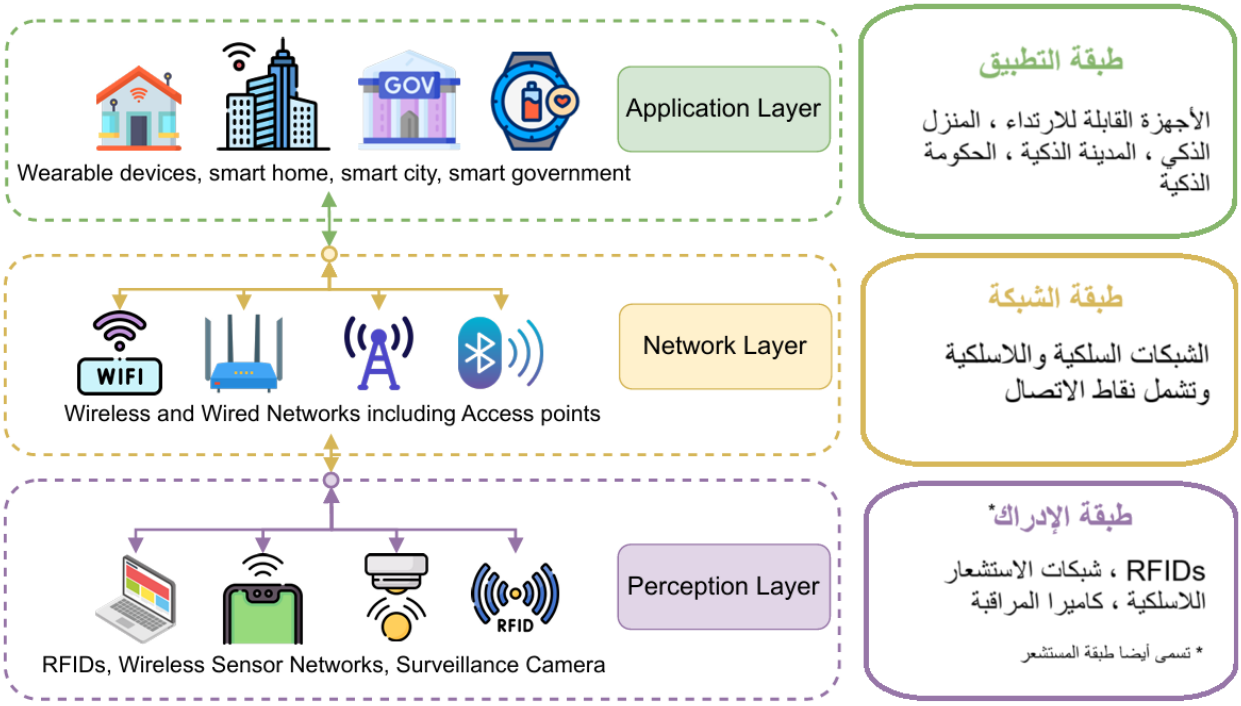
تعتمد النمذجة المعمارية لإنترنت الأشياء على تعديل معيار OSI (ربط الأنظمة المفتوحة) مع التعديلات المناسبة على وصلة البيانات والشبكة وطبقات النقل. فقد تم تقسيم معمارية إنترنت الأشياء إلى ثلاث طبقات انظر إلى الشكل ٢ وهي كالتالي:

١- **طبقة الإدراك:** طبقة الإدراك, المعروف أيضا باسم طبقة المستشعر, هي الطبقة الأساسية لبنية إنترنت الأشياء. تتفاعل هذه الطبقة مع الأجهزة الذكية ، بما في ذلك على سبيل المثال لا الحصر الساعات الذكية والحلقات الذكية ، باستخدام مجموعة من أجهزة الاستشعار والمحركات. يتعلق الهدف الرئيسي لهذه الطبقة بجمع البيانات من هذه الأجهزة الذكية عبر أجهزة الاستشعار ، وبالتالي نقل البيانات المكتسبة إلى الطبقة العليا المعروفة باسم طبقة الشبكة.

٢- **طبقة الشبكة:** طبقة الشبكة ، والمعروفة أيضا باسم طبقة الإرسال ، هي الطبقة الوسطى من بنية إنترنت الأشياء. هذه الطبقة مسؤولة عن تلقي المعلومات التي يتم تمريرها من طبقة الإدراك وتحديد مسارات نقل البيانات المعالجة إلى مختلف أجهزة وتطبيقات إنترنت الأشياء المتصلة باستخدام شبكات متكاملة مثل الاتصالات الآمنة السلكية أو اللاسلكية. طبقة الشبكة هي الطبقة الأساسية لبنية إنترنت الأشياء ثلاثية الطبقات, حيث تستخدم أجهزة مختلفة مثل أجهزة التوجيه والبوابات والمحولات والمحاور وتقوم بتشغيلها باستخدام تقنيات الاتصال المختلفة مثل ,G, LTE, Zigbee٣WiFi, Bluetooth إلخ. باختصار ، طبقة الشبكة مسؤولة عن نقل البيانات من وإلى العديد من التطبيقات من خلال واجهات وبوابات باستخدام تقنيات وبروتوكولات اتصال متعددة.

٣- **طبقة التطبيق:** تعمل هذه الطبقة كطبقة عليا داخل بنية إنترنت الأشياء ، ويشار إليها بطبقة التطبيق أو طبقة الأعمال، وهي مكلفة بتجميع البيانات من طبقة الشبكة، وبالتالي تسعى

جاهدة لتحقيق هدف إنشاء بيئة ذكية ، وهو الهدف النهائي لنموذج إنترنت الأشياء. تستوعب هذه الطبقة مجموعة متنوعة من التطبيقات ، يتميز كل منها بمتطلباته الخاصة. ومن الأمثلة على هذه التطبيقات الشبكات الذكية والمدن الذكية والنقل الذكي. علاوة على ذلك، تتحمل هذه الطبقة مسؤولية الحفاظ على صحة البيانات وسلامتها وسريتها.



شكل ١ معمارية إنترنت الأشياء

البنية ثلاثية الطبقات هي البنية المعممة والأكثر شيوعا، وقد دمجت العديد من الأنظمة هذه البنية. على الرغم من أن هذه البنية متعددة الطبقات تبدو بسيطة للوهلة الأولى، إلا أن وظائف الشبكة وطبقات التطبيقات قد تصبح معقدة في بعض الأحيان. على سبيل المثال، طبقة الشبكة ليست مسؤولة فقط عن مهمة نقل البيانات، ولكنها توفر أيضا خدمات البيانات مثل تجميع البيانات ومعالجتها، إلخ. من ناحية أخرى، فإن طبقة التطبيق ليست مسؤولة وحدها عن تقديم الخدمة للمستخدمين والمستخدمين، ولكنها توفر أيضا تحليل البيانات، وإجراء استخراج البيانات، وما إلى ذلك. لذلك، استجابة لمتطلبات محددة، تم دمج طبقات إضافية، بناء على الطبقات الأساسية. على سبيل المثال، تعمل البنى ذات الطبقات الأربع أو الخمس طبقات على تعزيز مرونة النظام. ومع ذلك، فإن البنية ثلاثية الطبقات بمثابة الأساس لكل هذه الاختلافات. علاوة على ذلك، تتطلب تطبيقات الجيل الجديد أوقات استجابة أقصر واستهلاكا منخفضا للطاقة لأن أجهزة إنترنت الأشياء ذات سعة محدودة. لذلك، استخدم الباحثون طبقات الضباب والسحب. يكتفي هذا المقرر بالطبقات الثلاث الأساسية.

أشكال إنترنت الأشياء

لنلقِ نظرة على بعض أمثلة أنظمة إنترنت الأشياء المستخدمة في الوقت الحالي:

السيارات المتصلة

هناك طرق كثيرة يمكن من خلالها توصيل المركبات، مثل السيارات، بالإنترنت، وربما تكون إحدى هذه الطرق كاميرات لوحة قيادة السيارة الذكية أو أنظمة الترفيه المعلوماتي أو حتى بوابة المركبة المتصلة، وهذه الأجهزة تجمع البيانات من دواسة الوقود، والمكابح، وعداد السرعة، وعداد المسافات، والعجلات، وخزانات الوقود لمراقبة كل من أداء السائق وسلامة السيارة، **للسيارات المتصلة عدة استخدامات منها:**

- مراقبة مجموعات السيارات المستأجرة لزيادة كفاءة استهلاك الوقود وخفض التكاليف.
- مساعدة الآباء على تتبع أسلوب القيادة الذي يسلكه أبناؤهم.
- إخطار الأصدقاء والعائلة تلقائياً في حالة اصطدام السيارة.
- التنبؤ باحتياجات صيانة المركبات ومنعها.

المنازل المتصلة

تركز الأجهزة المنزلية الذكية في الأساس على تحسين كفاءة المنزل وأمانه، فضلاً عن تحسين الشبكات المنزلية، فتراقب بعض الأجهزة مثل المقابس الذكية استهلاك الكهرباء وتوفر منظمات الحرارة الذكية تحكماً أفضل في درجة الحرارة، ويمكن أن تستخدم أنظمة الزراعة في الماء أدوات استشعار إنترنت الأشياء للتحكم في الحديقة في حين تستطيع أجهزة الكشف عن الدخان القائمة على إنترنت الأشياء اكتشاف دخان التبغ، ويمكن لأنظمة حماية المنزل مثل أقفال الأبواب وكاميرات المراقبة وأجهزة الكشف عن تسرب المياه اكتشاف التهديدات ومنعها وإرسال إشعارات لمالكي المنازل .

يمكن استخدام الأجهزة المتصلة في المنزل لعدة أهداف منها:

- إيقاف تشغيل الأجهزة غير المستخدمة تلقائياً.
- تأجير العقارات وإداراتها وصيانتها.
- البحث عن العناصر التي لا تستطيع العثور عليها مثل المفاتيح أو المحافظ.
- أتمتة المهام اليومية مثل التنظيف بالمكنسة الكهربائية وتحضير القهوة وما إلى ذلك.

المدن الذكية

زادت تطبيقات إنترنت الأشياء من كفاءة التخطيط العمراني وصيانة البنية الأساسية، فتستغل الحكومات تطبيقات إنترنت الأشياء لمعالجة مشكلات البنية الأساسية والصحة والبيئة، **ويمكن استخدام تطبيقات إنترنت الأشياء في الحالات التالية**:

- قياس جودة الهواء ومستويات الإشعاع.
- تقليل تكاليف فواتير الطاقة باستخدام أنظمة الإنارة الذكية.
- الكشف عن احتياجات صيانة البنى الأساسية الحيوية مثل الشوارع والجسور وخطوط الأنابيب.
- زيادة الأرباح بالإدارة الفعالة لمواقف السيارات.

المباني الذكية

تستخدم المباني مثل حرم الجامعات والمباني التجارية تطبيقات إنترنت الأشياء لزيادة الكفاءة التشغيلية، **يمكن استخدام أجهزة إنترنت الأشياء في المباني الذكية للأهداف التالية:**

- تقليل استهلاك الطاقة.
- تخفيض تكاليف الصيانة.
- الاستفادة من أماكن العمل بكفاءة أكبر.

توظيف إنترنت الأشياء في مراكز المعلومات

في مؤسسات المعلومات:

- تسريع عمليات التحوُّل الرقمي في أعمال مؤسسات المعلومات، لتتمكّن من تطوير خدماتها عبر تزويد الأشياء التي تقع ضمن دائرة اهتمام واستخدام المستفيدين وموظفي مؤسسات المعلومات بأجهزة استشعار مناسبة، ويمكن لأجهزة الاتصال الوصول إلى هذه الأشياء من خلال شبكة الإنترنت للقيام بالمهام المطلوبة من استعلام وحجز واستدعاء وإرجاع لأوعية المعلومات التقليدية والإلكترونية، إضافة إلى العثور على ما يفقد منها أو ما يوضع في غير مكانه، وكذلك ما يتعلّق بالتحكُّم بالبيئة الداخلية من إضاءة وتكييف، وفتح واغلاق الأبواب والنوافذ، ورصد إعداد الزوار، والتعرُّف إلى نوعياتهم، إن كانوا طلاباً أو باحثين أو أعضاء هيئة تدريس، وكذلك تخصُّصاتهم العلمية والساعات التي يفضِّلون الزيارة فيها عبر اقتفاء أثر كل زائر يحمل بطاقة عضوية ذكية تتضمَّن معلوماته الشخصية والعلمية والمهنة، وسيكون بمقدور المكتبة التعرُّف إلى المجال الموضوعي لكلِّ زائر، كما يمكنها تقديم الخدمة والإرشاد القرائي له عن بعد، ويتم اقتفاء الأثر منذ دخول المستفيد عبر بوابة المكتبة الذكية لتحسين الخدمات المقدمة، والمساعدة على صناعة القرارات، بالاعتماد على تحليل البيانات الضخمة الخاصة بالمستفيدين والمقتنيات والأجهزة والبرمجيات، وأثاث المكتبة وبواباتها، وكل شيء ذي صلة بها.
- ويمكن تحديد موقع المستفيد داخل المكتبة لتقديم الخدمة التي طلبها عن بعد أو الإجابة عن تساؤله أو تسليمه الكتاب الذي طلبه.
- كما يمكن تحميل خريطة موقع الكتاب الذي بحث عنه المستفيد من الفهرس الآلي، وتمكينه من العثور عليه على الرف عبر خاصية تتبع الأشياء.
- ويمكن القيام بالخدمات الذاتية المتعلقة بعملية طلب الكتب وعمل الاستعارة أو الإعادة ذاتياً من دون تدخُّل بشري، سواء عبر الأجهزة التي توفِّرها المكتبة أم من خلال التطبيق الخاص بها المحمَّل على هاتف المستفيد الذكي.
- كذلك بالإمكان مساهمة إنترنت الأشياء في خدمة البحث العلمي، وتكوين مجموعات تعاون بحثية من خلال القدرة على تحديد هوية وأماكن وجود النظراء الذين يلتقون معك في اهتمامات بحثية أو تخصُّص علمي؛ فتبدأ بالتعرُّف إليهم والتواصل وتكوين مجموعات عمل معهم من دون معرفة سابقة.

إنترنت الأشياء الاجتماعي

إنترنت الأشياء هو عامل مهم من الثورة الصناعية الرابعة التي ستغير العديد من نواحي حياتنا إلى الأبد، وهو ما سيؤثر على تقبل المجتمع البشري لهذه التقنية. فعلى سبيل المثال؛ هذا التحول الرقمي سيؤدي إلى فقدان الملايين من الوظائف واختفائها إلى الأبد، وهذا سيؤدي إلى حدوث عواقب اقتصادية مثل تلك التي حدثت في الثورات الصناعية السابقة. يقول الخبراء أنه كما سيؤدي إنترنت الأشياء إلى فقدان الملايين من الوظائف سيؤدي أيضاً إلى خلق الملايين من الوظائف المختلفة، ولكن هذا سيتطلب تعلم الذين فقدوا وظائفهم مهارات جديدة مطلوبة في أسواق العمل. وبمناسبة التحدث عن المهن والمهارات الجديدة المطلوبة، فإن المتخصصين يقولون بأن هناك تخصصات معينة مزدهرة في عصر إنترنت الأشياء.

وهذه التخصصات أو المجالات هي:

- علم تحليل البيانات Data Analysis.
- الذكاء الاصطناعي Artificial Intelligence.
- البرمجة Programming.
- الأمن السيبراني.Cyber-Security
- تصميم واجهات المستخدم UX & UI Design.
- برمجة تطبيقات الهواتف المحمولة Mobile Development.
- هندسة الإلكترونيات Hardware Engineering.
- هندسة الشبكات Networking Engineering.

ما هو إنترنت الأشياء الاجتماعي؟

يمكننا القول بأن "انترنت الأشياء الاجتماعي" يعتبر دمجاً لكلا من مفهومي التواصل الاجتماعي وانترنت الأشياء، ربط الأشياء ببعضها يسهل ربط الأشخاص بها. ذلك يعني ارتباطاً أقوى من الأشخاص بحساباتهم على وسائل التواصل الاجتماعي، بالتالي يجب على منصات التواصل الاجتماعي أن تتطور لتكون قادرة على توصيل الأشياء بعضها ببعض ما يسمح للمستخدمين بالتحكم في شئون حياتهم وتعديل خدماتهم. لا يتعلق الأمر فقط بالتحكم في كل شيء، ولكن أيضاً بمشاركة كل تفاصيل حياتك مع أصدقائك ومجتمعك على وسائل التواصل الاجتماعي. على سبيل المثال، إذا أصيب شخص كبير في السن بنوبة قلبية أثناء تواجده بمفرده في المنزل، باستخدام انترنت الأشياء سيتم ارسال رسالة عبر Facebook أو كتابة تغريدة على Twitter أو رسالة من خلال WhatsApp إلى جيرانه وعائلته على الفور، ما يجعل وسائل التواصل الاجتماعي تدخل حقبة جديدة من ربط كل الأشياء والخدمات والكائنات في عالمنا.

ماذا إذا عن مراقبة وسائل التواصل الاجتماعي؟

إن ربط "انترنت الأشياء" بمنصات مراقبة وسائل التواصل الاجتماعي يعني توفير رؤية أعمق وأكثر فائدة للشركات، ليس فقط لتطوير منتجاتهم وخدماتهم، ولكن أيضاً لاتخاذ قرارات واعية مبنية على البيانات الدقيقة فيما يتعلق بإداراتهم واستراتيجيات عملهم وخططهم للمستقبل، يمكنك النظر للأمر على هذا النحو، إذا كان كل شيء وكل شخص مرتبطاً بوسائل التواصل الاجتماعي، فتخيل المدى الذي قد تصل إليه دقة البيانات المجمعة من أدوات الإصغاء الاجتماعية وكذلك مقدار قوتها وموثوقيتها وغناها بالمعلومات وتعبيرها الدقيق عن حقيقة الأوضاع.

مع التطور والتغير السريع لإنترنت الأشياء يصبح عالمنا أكثر ذكاء وبسرعة مذهلة، على الرغم من أن الخصوصية والأمان يظلان من أكبر التحديات التي تواجه التكنولوجيا الجديدة، فإن الحلول الأكثر ذكاءً ستتغلب عليها بالتأكيد، شيء آخر مؤكد كذلك وهو أننا قد وصلنا إلى هذا العالم الذكي المترابط الذي اعتدنا مشاهدته في الأفلام، وبأسرع مما توقعنا، أصبحت هناك حقيقة واقعة تسمى "إنترنت الأشياء" و"الإنترنت الاجتماعي لكل شيء".

تحديات توظيف إنترنت الأشياء في المؤسسات المختلفة

من أهم التحديات في توظيف انترنت الأشياء في مختلف المؤسسات هي التحديات والتهديدات الأمنية التي يواجهها إنترنت الأشياء :

- **تردد الراديو (RF) التشويش**

يمكن للقراصنة استخدام التشويش اللاسلكي لمنع أجهزة إنترنت الأشياء اللاسلكية عن طريق التدخل في الاتصالات اللاسلكية لإعاقة وظائفها ويمكن القيام بذلك عن طريق الحصول على جهاز تشويش التردد اللاسلكي مما يجعل أجهزة إنترنت الأشياء تحد من قدرتها على الاتصال عن طريق فقدان الاتصال على سبيل المثال يمكن تشويش إنذارات الأمان اللاسلكية السكنية والتجارية المتصلة عبر شبكة خلوية بسهولة وتمكين متطفل من الاختراق دون علم مزود الأمان.

- **هجمات رفض الخدمة الموزعة (DDoS)**

يحدث هجوم DDoS عندما يتم عمل جميع أجهزة الشبكة بشكل غير مستقر لإرسال رسائل غير محدودة تؤدي في النهاية إلى حدوث ازدحام في شبكة إنترنت الأشياء مما يؤدي إلى إيقاف تشغيلها ويستخدم مجرمو الإنترنت هجمات DDoS للتحكم في العديد من الأجهزة المخترقة وبالتالي منع المعلومات المهمة من الوصول إلى وجهتها .

- **تسرب الخصوصية**

يمكن إساءة استخدام جهاز إنترنت الأشياء غير الآمن الذي يسرب عنوان IP الخاص به إذا تم تحديده بواسطة أحد المتسللين للإشارة إلى أي موقع، يوصى بتأمين اتصالات إنترنت الأشياء باستخدام الشبكات الافتراضية الخاصة (VPN) تماماً كما يمكن تأمين شبكة مزود خدمة الإنترنت عن طريق تثبيت VPN على جهاز توجيه لتشفير كل حركة المرور التي تمر عبرها ويمكن تطبيق الشيء نفسه على جهاز إنترنت الأشياء للتأكد من أن عنوان IP الخاص بك خاص وشبكتك الذكية محمية .

- **مخترقيّ الشبكة**

يحدث اختراق الشبكة عندما يتم اختراق جهاز إنترنت الأشياء من خلال الشبكة المتصل بها ويسمح هذا النوع من الخرق الأمني للمتسلل بالوصول إلى الجهاز والتحكم فيه على سبيل المثال يمكنهم التحكم في منظم الحرارة للفرن الصناعي وإشعال حريق أو التسبب في تحطم مركبة مستقلة من خلال التحكم في قيادتها .

- **اقتحام المنزل**

هذا هو أحد الأسباب التي تجعل المنازل الذكية غير مثالية على أنها حقيقة واقعة ويتم تكييفها على نطاق واسع حتى الآن فهو أيضاً أحد أكثر السيناريوهات رعباً التي يمكن أن تحول جهازاً مخصصاً لراحة العميل الفردي إلى تهديد كبير لخصوصية منزله فأجهزة إنترنت الأشياء غير الآمنة التي يتم شحنها إلى مستخدم باسم مستخدم افتراضي كـ "مشرف" وكلمة مرور مثل "١٢٣٤٥" معرضة بشدة للتطفل على المنزل ولا يمكن استخدام هذا فقط في عمليات السطو المخطط لها ولكن أيضاً يغزو الخصوصية التامة للأسرة وهذا هو السبب في أنه من المهم جداً تأمين بيانات اعتماد الجهاز وربطها عبر VPN .

- **عدم وجود تحديثات الجهاز**

تقوم الشركات بتصنيع أجهزة إنترنت الأشياء بمعدل متزايد بسبب الطلب المتزايد ومع ذلك نظرًا لأن تركيزهم ينصب على الإنتاجية والمنافسة فإن الشركات المصنعة ليست حريصة جدًا في التعامل مع المخاطر المتعلقة بأجهزة إنترنت الأشياء ومشكلات الأمان فأغلب الأجهزة في السوق لا تحتوي على تحديثات أمنية كبيرة وبعضها لا يتم تحديثه على الإطلاق حتى إذا كان الجهاز في البداية يلبي متطلبات الأمان فإنه يصبح غير آمن ومعرض للخطر بعد ظهور تقنيات جديدة وتحديات جديدة للأمن السيبراني مما يجعله أكثر عرضة للهجمات الإلكترونية خاصة إذا لم يتم تحديثه، تقدم بعض الشركات المصنعة تحديثات البرامج الثابتة عبر الأثير (OTA) ولكنها تتوقف عن القيام بذلك بمجرد بدء العمل على أجهزة الجيل التالي مما يترك الأجهزة القديمة عرضة لتهديدات الأمان .

- **اتصالات غير آمنة**

لا تقوم معظم أجهزة إنترنت الأشياء بتشفير الرسائل أثناء الاتصال عبر الشبكة مما يجعلها واحدة من أكبر التحديات الأمنية لإنترنت الأشياء فلمنع التطفل تحتاج الشركات إلى تأمين وتشفير اتصالاتها بين الخدمات والأجهزة السحابية ويمكن أن يضمن استخدام تشفير النقل والمعايير مثل TLS الاتصال الآمن وأيضًا يمكن أن يضمن عزل الجهاز باستخدام شبكات مختلفة اتصالاً خاصاً آمناً .

- **صعوبة تحديد حالة الجهاز المخترقة**

أحد التحديات الأخرى التي يواجهها جهاز إنترنت الأشياء هو أنه من الصعب للغاية التأكد مما إذا كان الجهاز قد تم اختراقه أم لا وخاصة عندما يكون هناك عدد كبير من أجهزة إنترنت الأشياء يصبح من الصعب للغاية مراقبة حالة الأمان لجميع الأجهزة وذلك لأن أجهزة إنترنت الأشياء تحتاج إلى خدمات وتطبيقات وبروتوكولات للتواصل ومع وجود المزيد من الأجهزة يصبح من الصعب معرفة أي منها تم اختراقه ونتيجة لذلك تستمر العديد من هذه الأجهزة المخترقة في العمل دون علم المستخدم وتظل بياناته وخصوصيته تتعرض للاختراق.

هناك تحديات أخرى تواجه إنترنت الأشياء، وهي:

- **التوافق**

يمكن أن تشكل الأجهزة المترابطة من مختلف البائعين في شبكة إنترنت الأشياء تحديات في المراقبة والإدارة. تعتمد الصناعات المختلفة حاليا على العديد من المعايير لدعم تطبيقاتها. نظرا للكميات الهائلة من البيانات وأنواع الأجهزة المتنوعة ووجود كيانات مختلفة، يصبح استخدام الواجهات القياسية أمرا بالغ الأهمية. يتم تضخيم هذه الأهمية، خاصة بالنسبة للتطبيقات التي تحتاج إلى استيعاب كل من التعاون بين المؤسسات ومجموعة واسعة من قيود النظام. تتطلب معالجة هذه القضايا من جميع الصناعات الالتزام بمعايير محددة، ولكن تحقيق مثل هذا الامتثال العالمي يمكن أن يكون مهمة شاقة وغير عملية.

- **قابلية التوسع في المستقبل**

من المتوقع أن تنضم الأجهزة غير المتجانسة باستمرار إلى شبكة إنترنت الأشياء الآخذة في التوسع. نتيجة لذلك، مع زيادة عدد الأجهزة، يصبح ضمان الاتصال السلس والإدارة الفعالة للبيانات والأداء العام للنظام على نطاق صغير أمرا صعبا بشكل متزايد. لذلك، تشكل قابلية التوسع في إنترنت الأشياء تحديا مستمرا لمستقبل هذه التكنولوجيا. لمواجهة تحديات قابلية التوسع بشكل فعال، من الضروري إنشاء بنية قابلة للتطوير، باستخدام تقنيات مثل المكونات المعيارية وموازنات التحميل والأنظمة الموزعة.

- **كفاءة الطاقة**

غالبا ما تحتوي الأجهزة الذكية الصغيرة التي تشتمل على أنظمة إنترنت الأشياء على طاقة بطارية محدودة، والتي لا يمكن استبدالها بسهولة. يمكن أن يؤدي هذا القيد إلى أزمة طاقة عالمية وارتفاع استهلاك الطاقة، فضلا عن القيود المفروضة على الذاكرة وقدرات المعالجة.

- **إدارة التنقل**

تشير إدارة التنقل في إنترنت الأشياء إلى القدرة على التعامل مع الأجهزة التي تتحرك داخل الشبكة بسلاسة. إنه جانب حاسم لأن العديد من أجهزة إنترنت الأشياء ليست ثابتة وتحتاج إلى التواصل أثناء تغيير المواقع. يمكن أن يؤدي وجود الأجهزة المحمولة في إعدادات إنترنت الأشياء إلى تحديات في كيفية عمل بروتوكولات التوجيه وشبكات إنترنت الأشياء بكفاءة. لا يمكن للطرق الحالية المستخدمة للأجهزة التي تتحرك، كما هو الحال في شبكات الاستشعار والشبكات المتنقلة المخصصة وشبكات المركبات، التعامل بفعالية مع المشكلات المختلفة المتعلقة بالتوجيه لأن هذه المستشعرات لديها طاقة معالجة وموارد طاقة محدودة. لمعالجة هذه التحديات، تستخدم أنظمة إنترنت الأشياء تقنيات وبروتوكولات إدارة التنقل المختلفة، بهدف توفير اتصال موثوق وسلس للأجهزة المحمولة في النظام البيئي لإنترنت الأشياء.

- **تكلفة الصيانة والخدمات**

تتكون شبكة إنترنت الأشياء من عدد كبير من الأجهزة، باستخدام تقنيات الاتصالات المختلفة المكلفة. هذا يؤدي حتما إلى زيادة تكاليف الصيانة والخدمة لهذه الأجهزة والاتصالات العديدة. وبالتالي، يكمن تحد كبير في معالجة هذه المشكلة من خلال تصميم الأجهزة وأجهزة الاستشعار التي تتطلب الحد الأدنى من الصيانة.

- **مشكلة انقطاع الاتصال بالإنترنت**

يؤدي انقطاع الاتصال بالإنترنت، وهو أمر أساسي لعمليات إنترنت الأشياء، إلى أداء رديء من تطبيقات إنترنت الأشياء وانخفاض في جودة الخدمة. علاوة على ذلك، فإن عمليات إعادة التشغيل على عدد الأجهزة التي يمكن أن تتفاعل بشكل متزامن مع المحطة الرئيسية تحد من وصول المستخدم إلى هذه الخدمات. تمثل هذه المشكلة مشكلة خاصة في إعدادات الشبكة البعيدة أو غير الموثوقة، حيث يثبت الحفاظ على اتصال إنترنت ثابت أنه يمثل تحديا. وبالتالي، معالجة مشكلة انقطاع الاتصال بالإنترنت في إنترنت الأشياء أمر حتمي للحفاظ على موثوقية وكفاءة أنظمة إنترنت الأشياء.

- **معالجة البيانات وتحليلها وإدارتها**

يمثل إجراء معالجة البيانات وتحليلها وإدارتها تحديا هائلا بسبب الطبيعة غير المتجانسة لأجهزة إنترنت الأشياء والنطاق الواسع لتوليد البيانات. في الوقت الحالي، تستخدم معظم الأنظمة المركزية المستندة إلى السحابة لأداء المهام المكثفة من الناحية الحسابية وتقديم البيانات. ومع ذلك، فإن القلق المستمر يدور حول قيود البنى السحابية التقليدية عندما يتعلق الأمر بالتعامل بكفاءة مع الكميات الهائلة من البيانات التي تم إنشاؤها واستخدامها بواسطة الأجهزة التي تدعم إنترنت الأشياء. بالإضافة إلى ذلك، تكافح هذه البنى لدعم المتطلبات الحسابية المرتبطة بها مع تلبية قيود التوقيت الدقيقة أيضا. لمواجهة هذا التحدي، تعتمد معظم الأنظمة حاليا على الحلول الحالية مثل الحوسبة السحابية المتنقلة وحوسبة الضباب، وكلاهما يستخدم معالجة الحافة.

- **تحديات أخرى**

أصبحت مراقبة الجودة وحركة المرور أكثر تعقيدا بسبب العدد الهائل من أجهزة إنترنت الأشياء. تعد إدارة التعريفات الفريدة لكل جهاز إنترنت الأشياء مصدر قلق متزايد أيضا. وكذلك، تواجه الدول تحديات بسبب الانتشار العالمي لإنترنت الأشياء، حيث يمكن جمع البيانات التي يتم إنشاؤها داخل حدودها ونقلها إلى مزودي الخدمة الموجودين في أي مكان في العالم، مما يثير مخاوف بشأن خصوصية البيانات والولاية القضائية.

ستتطلب معالجة هذه التحديات متعددة الأوجه دراسة متأنية وتعاونا دوليا لضمان التنفيذ الفعال والآمن لتكنولوجيا إنترنت الأشياء.

تدريبات الفصل الأول

س١: اختار الإجابة الصحيحة:

١. ..... شبكة من الأجهزة الذكية المترابطة التي تتبادل البيانات وتتواصل عبر الإنترنت دون تدخل بشري مباشر ؟

أ. الحوسبة السحابية

ب. إنترنت الأشياء

ج. الواقع المعزز

د. النسخ الافتراضية

٢. في أي طبقة من طبقات معمارية لإنترنت الأشياء توجد شبكة المستشعرات اللاسلكية؟

أ. طبقة التطبيقات

ب. طبقة النقل

ج. طبقة الشبكة

د. طبقة الإدراك

٣. إنترنت الأشياء الاجتماعي يعتبر دمجاً لكلا من مفهومي التواصل الاجتماعي و ..... ؟

أ. الحوسبة السحابية

ب. إنترنت الأشياء

ج. الواقع المعزز

د. النسخ الافتراضية

٤. من التهديدات المصاحبة لإنترنت الأشياء: ..... و هو عدم حصول معظم هذه الأجهزة المتصلة على تحديثات أمنية كافية؛ لا يتم تحديث البعض على الإطلاق.

أ. الوصول عن بعد

ب. برامج الفدية

ج. هجمات رجل في الوسط

د. عدم وجود تحديثات

٥. من التهديدات المصاحبة لإنترنت الأشياء: .....و هو أن يقوم المجرمون بتشفير نظامك بالكامل ويهددون بإزالة جميع بياناتك ما لم تعطيهم ما يطلبون ؟

أ. الوصول عن بعد

ب. برامج الفدية

ج. هجمات رجل في الوسط

د. عدم وجود تحديثات

٦. من التهديدات المصاحبة لإنترنت الأشياء: ..... و هو اختراق أجهزة إنترنت الأشياء والقيام بتشغيل الكاميرا/الميكروفونات دون علم أصحابها ؟

أ. الوصول عن بعد

ب. برامج الفدية

ج. هجمات رجل في الوسط

د. عدم وجود تحديثات

٧. من التهديدات المصاحبة لإنترنت الأشياء: ..... وهو أن يعترض المتسللون الاتصال بين طرفين ثم يغيرون الرسائل بينما يعتقد كلا الطرفين أنهما يتواصلان مع كل منهما آخر ؟

أ. الوصول عن بعد

ب. برامج الفدية

ج. هجمات رجل في الوسط

د. عدم وجود تحديثات

س٢: ضعي علامة صح أمام العبارة الصحيحة وعلامة خطأ أمام العبارة الخاطئة:

أ. تعد أتمتة كل ما يمكن أتمتة من مميزات إنترنت الأشياء ( )

ب. إنترنت الأشياء يستهلك الكثير من الوقت ( )

ج. يزيد إنترنت الأشياء من استهلاكنا للطاقة ( )

د. لا يعد الحد من الحوادث والمشاكل الصحية من مميزات إنترنت الأشياء ( )

ه. توفير الكثير من البيانات من مميزات إنترنت الأشياء ( )

و. يساهم إنترنت الأشياء في الأمان والحماية ( )

س٣: عددي ثلاث لكل مما يلي:

أ. أشكال إنترنت الأشياء.

ب. التخصصات المزدهرة في مجال علم إنترنت الأشياء.

ج. مكونات إنترنت الأشياء.

حل تدريبات الفصل الأول

حل السؤال الأول:

١- إنترنت الأشياء (أ)
٢- طبقة الإدراك (د)
٣- إنترنت الأشياء (ب)
٤- عدم وجود تحديثات (د)
٥- برامج الفدية (ب)
٦- الوصول عن بعد (ب)
٧- هجمات رجل الوسط (ج)

حل السؤال الثاني:

أ. صح
ب. خطأ
ج. خطأ
د. خطأ
ه. صح
و. صح

حل السؤال الثالث:

أ. من أشكال إنترنت الأشياء: السيارات الذكية، المنازل الذكية، المدن الذكية، المباني الذكية.
ب. من التخصصات المزدهرة في مجال علم إنترنت الأشياء: علم تحليل البيانات، الذكاء الاصطناعي، الأمن السيبراني.
ج. من مكونات إنترنت الأشياء: أجهزة الاستشعار، التخزين وتحليلات البيانات، أدوات التفسير والتصوير

ثانياً: الحوسبة السحابية وأمنها

في هذا الفصل سنتعرف على المواضيع التالية:

- **مفهوم الحوسبة السحابية وعلاقته بإنترنت الأشياء**
- **مكونات بيئة الحوسبة السحابية**
- **نماذج بناء الحوسبة السحابية**
- **مميزات وخصائص الحوسبة السحابية**
- **اقتصاديات بيئة الحوسبة السحابية**
- **أمن الحوسبة السحابية**

مفهوم الحوسبة السحابية وعلاقته بإنترنت الأشياء

ما هي الحوسبة السحابية؟

تحتاج المنظمات إلى الوقت والميزانية لتوسيع نطاق البنية التحتية لتكنولوجيا المعلومات الخاصة بها، في أماكن العمل، يعد توسيع نطاق البنية التحتية لتكنولوجيا المعلومات أمراً صعباً ويتطلب مزيداً من الوقت، توفر الحوسبة السحابية الحل الأمثل لهذه المشكلة، تتكون خدمات الحوسبة السحابية من مراكز البيانات الافتراضية التي توفر الأجهزة والبرامج والموارد عند الحاجة، لذلك يمكن للمؤسسات الاتصال مباشرة بالسحابة واستخدام الموارد اللازمة، هذا يساعد على تقليل التكلفة وتوسيع نطاقها وتقليصها وفقاً لمتطلبات العمل.

إذا يمكن تعريف الحوسبة السحابية بأنها توفير موارد تقنية المعلومات حسب الطلب عبر الانترنت مع تسعير التكلفة حسب الاستخدام. انظر إلى الشكل ٢.

الشكل ٢ مخطط الحوسبة السحابية

ما هي العلاقة بين الحوسبة السحابية وإنترنت الأشياء؟

الحوسبة السحابية هي الطريق لنقل وتخزين بيانات إنترنت الأشياء.

ما هو الفرق بين الحوسبة السحابية وإنترنت الأشياء؟

الحوسبة السحابية هي التكنولوجيا التي تشير إلى تقديم الخدمات المستضافة عبر الإنترنت بينما يقوم إنترنت الأشياء بتوصيل الأجهزة الذكية المحيطة بالشبكة لاستخراج البيانات للتحليل واتخاذ القرار، علاوة على ذلك تتيح إنترنت الأشياء جمع البيانات من العديد من الأجهزة بينما توفر الحوسبة السحابية الأدوات والخدمات اللازمة لتطوير تطبيقات إنترنت الأشياء.

ملخص - الحوسبة السحابية مقابل إنترنت الأشياء

يوضح جدول ١ الاختلاف والعلاقة بين إنترنت الأشياء والحوسبة السحابية. ويتمثل الاختلاف بينهما في أن الحوسبة السحابية توفر خدمات مستضافة عبر الإنترنت بينما تقوم إنترنت الأشياء بتوصيل الأجهزة الذكية المحيطة بالشبكة لمشاركة البيانات وتحليلها لاتخاذ القرار، باختصار، توفر الحوسبة السحابية الطريق لمشاركة بيانات إنترنت الأشياء وتخزينها.

جدول ١ الاختلاف والعلاقة بين أمن إنترنت الأشيا ء والحوسبة السحابية

	إنترنت الأشياء	الحوسبة السحابية
الاختلاف	تهتم بتوصيل الأجهزة الذكية المحيطة بالشبكة لمشاركة البيانات وتحليلها لاتخاذ القرار	توفر خدمات مستضافة عبر الإنترنت
العلاقة	الحوسبة السحابية هي الطريق لنقل وتخزين بيانات إنترنت الأشياء.	

مكونات بيئة الحوسبة السحابية

مكونات الحوسبة السحابية هي المكونات التي تشكل البنية التحتية للسحابات والخدمات السحابية، من التخزين إلى البرمجيات ومن النسخ الاحتياط إلى الأمن.. وغيرها من المكونات.

جميع أنواع الأعمال، سواء كان حجمها صغيراً أو كبيراً واسع النطاق، تتحول إلى الخدمات المستندة إلى السحابة، ازداد اعتماد كل من السحب العامة والخاصة في السنوات القليلة الماضية لسبب وراء هذا التحول هو انخفاض تكاليف التشغيل وزيادة المرونة، تستخدم تقنية الحوسبة السحابية الخوادم البعيدة لتخزين وإدارة والوصول إلى البيانات على الإنترنت بدلاً من امتلاك بنية تحتية محلية.

مكونات الحوسبة السحابية

مكونات الحوسبة السحابية تتكون من جزأين الواجهة الأمامية والنهاية الخلفية، والجزء الأمامي هو الجزء الذي يستخدمه المستخدم، والجزء الخلفي يديره المضيف.

كلا الطرفين متصلان ببعضهما البعض عبر الإنترنت، تشتمل الواجهة الأمامية على تطبيقات وواجهات تساعد المستخدم على الوصول إلى الخدمات السحابية، تدير الشركة التي تقدم الخدمات السحابية الواجهة الخلفية ولديها مرافق تخزين البيانات، والأجهزة الافتراضية، وأنظمة الأمان، والخوادم.

فيما يلي أهم مكونات الحوسبة السحابية وبنيتها التحتية:

١.البنية التحتية للعميل

مكون البنية التحتية للعميل هو جزء من الواجهة التي توفر واجهة مستخدم رسومية للمستخدم للتفاعل مع السحابة.

٢.التطبيق

التطبيق هو أي نظام أساسي مثل تطبيق أو برنامج تقدمه شركة يمكن للعملاء من خلالها الوصول إلى السحابة.

٣.الخدمة

تدير الخدمة السحابية نوع الخدمة التي يحتاجها العميل لاستخدامها وفقاً لمتطلباته، **هناك ثلاثة أنواع من الخدمات في الحوسبة السحابية:**

- **البرامج كخدمة (SaaS):** تُعرف الخدمات المستندة إلى SaaS بخدمات التطبيقات السحابية، يتم تشغيلها مباشرة من خلال متصفح الويب مما يلغي الحاجة إلى أي تنزيل أو تثبيت للتطبيقات – **على سبيل المثال** : Slack Hubspot وتطبيقات Google.
- **النظام الأساسي كخدمة (PaaS):** تشبه خدمات PaaS خدمات SaaS ومع ذلك ، توفر خدمات PaaS نظاماً أساسياً للمستخدمين لإنشاء البرنامج وتحريره وتشغيله، **على سبيل المثال** : سحابة التجارة Magneto و Windows Azure .
- **البنية التحتية كخدمة (IaaS):** تدير IaaS بيئات وقت تشغيل بيانات التطبيق والبرمجيات الوسيطة، يوفر خدمات افتراضية تلغي الحاجة إلى موارد الحوسبة المادية مثل ذاكرة الوصول العشوائي ووحدة المعالجة المركزية ومراكز البيانات في IaaS ، تقوم الشركات بتشغيل الخوادم الافتراضية والشبكات والتخزين على السحابة على أساس مدفوع، **على سبيل المثال:** Google Compute Engine (GCE) و Amazon Elastic Compute Cloud و Amazon Web Services (AWS).

٤.سحابة بيئة التنفيذ

توفر سحابة وقت التشغيل بيئة التنفيذ ووقت التشغيل للأجهزة الافتراضية.

٥.التخزين

يوفر مكون التخزين للحوسبة السحابية سعة التخزين في السحابة لتخزين البيانات وإدارتها، في التخزين السحابي، يمكن الوصول إلى البيانات لعدة عملاء في وقت واحد يكون التخزين السحابي بشكل عام في **شكل ثلاث تكوينات أساسية**: السحابة العامة والسحابة الخاصة والسحابة المختلطة.

٦.البنية التحتية

توفر البنية الأساسية خدمات على مستوى المضيف ومستوى التطبيق ومستوى الشبكة، يتضمن مكونات البرامج والأجهزة مثل خادم أجهزة شبكة التخزين وأي مورد تخزين آخر مطلوب لدعم نموذج الحوسبة السحابية.

٧.الإدارة

تُستخدم الإدارة لإدارة المكونات مثل خدمات التخزين والتطبيقات والبنية التحتية السحابية لوقت التشغيل وقضايا الأمان في الواجهة الخلفية وإنشاء التنسيق.

٨.حماية

تعتبر الحماية أهم مكونات الحوسبة السحابية التي يركز عليها العملاء.

الأمان هو المكون الخلفي للحوسبة السحابية، والذي يضمن أمان البيانات في السحابة، يتضمن نظام الأمان في السحابة مجموعة واسعة من السياسات والتقنيات والتطبيقات وعناصر التحكم المستخدمة لحماية عناوين IP والبيانات والتطبيقات والبنية التحتية والخدمات المقدمة في الحوسبة السحابية.

٩.الإنترنت

جميع مكونات الحوسبة السحابية موجودة بفضل الأنترنت.

الإنترنت هو الوسيط الذي تستخدمه مكونات الواجهة الأمامية والخلفية للتواصل والتفاعل مع بعضها البعض، باستخدام حل قائم على السحابة يمكن للشركات العمل بميزانيات أقل والتخلص من البنية التحتية المحلية، يتم اعتماد الحوسبة السحابية على نطاق واسع نظراً لمزاياها اللانهائية التي تؤثر بشكل إيجابي على الإنشاء والابتكار والتعاون، والأمان وسهولة الاستخدام والمبيعات.

مكونات الحوسبة السحابية حسب الخدمات:

١ .تخزين كخدمة Storage-as-a-service

التخزين كخدمة (يُعرف أيضاً باسم مساحة القرص عند الطلب) ، كما قد تتوقع هو القدرة على الاستفادة من التخزين الموجود فعلياً في موقع بعيد ولكنه منطقياً مورد تخزين محلي لأي تطبيق يتطلب التخزين، هذا هو المكون الأكثر بدائية في الحوسبة السحابية وهو مكون أو نمط يتم الاستفادة منه بواسطة معظم مكونات الحوسبة السحابية الأخرى.

٢.قواعد البيانات كخدمة Database-as-a-service (DaaS)

توفر قاعدة البيانات كخدمة (DaaS) القدرة على الاستفادة من خدمات قاعدة البيانات المستضافة عن بُعد ومشاركتها مع مستخدمين آخرين وجعلها تعمل بشكل منطقي كما لو كانت قاعدة البيانات محلية، يتم تقديم نماذج مختلفة من قبل مزودين مختلفين، ولكن القوة تكمن في الاستفادة من تقنية قواعد البيانات التي قد تكلف عادةً آلاف الدولارات في تراخيص الأجهزة والبرامج.

٣. المعلومات كخدمة Information-as-a-service

المعلومات كخدمة هي القدرة على استهلاك أي نوع من المعلومات، التي تتم استضافتها عن بُعد، من خلال واجهة محددة جيداً مثل واجهة برمجة التطبيقات (API) تشمل الأمثلة معلومات أسعار الأسهم ، والتحقق من العنوان ، وإعداد تقارير الائتمان.

٤.العملية كخدمة Process-as-a-service

العملية كخدمة هي مورد بعيد يمكنه ربط العديد من الموارد معاً، مثل الخدمات والبيانات، سواء كانت مستضافة داخل نفس مورد الحوسبة السحابية أو عن بُعد، لإنشاء عمليات تجارية يمكنك التفكير في عملية الأعمال على أنها تطبيق تعريف يمتد عبر الأنظمة ، ويستفيد من الخدمات الأساسية والمعلومات التي يتم دمجها في تسلسل لتشكيل عملية، عادةً ما تكون هذه العمليات أسهل في التغيير من التطبيقات ، وبالتالي توفر المرونة لأولئك الذين يستفيدون من محركات العملية هذه التي يتم تسليمها عند الطلب.

٥ .التطبيق كخدمة Application-as-a-service (AaaS)

التطبيق كخدمة (AaaS) المعروف أيضاً باسم البرنامج كخدمة (SaaS) ، هو أي تطبيق يتم تسليمه عبر النظام الأساسي للويب إلى المستخدم النهائي ، وعادةً ما يستفيد من التطبيق من خلال المستعرض.

بينما يربط العديد من الأشخاص التطبيق كخدمة بتطبيقات المؤسسة مثل Salesforce SFA ، فإن تطبيقات أتمتة المكاتب هي بالفعل تطبيقات كخدمة أيضاً ، بما في ذلك محرر مستندات Google و Gmailوتقويم Google.

٦ .النظام الأساسي كخدمة Platform-as-a-service (PaaS) (PaaS)

النظام الأساسي كخدمة (PaaS) عبارة عن نظام أساسي كامل، بما في ذلك تطوير التطبيقات، وتطوير الواجهة، وتطوير قواعد البيانات، والتخزين، والاختبار، وما إلى ذلك، يتم تسليمه من خلال نظام أساسي مستضاف عن بُعد للمشتركين، استناداً إلى نموذج مشاركة الوقت التقليدي، يوفر موفرو النظام الأساسي كخدمة الحديثين القدرة على إنشاء تطبيقات من فئة المؤسسات للاستخدام محلياً أو عند الطلب بسعر اشتراك صغير أو مجاناً.

٧ .التكامل كخدمة Integration-as-a-service

التكامل كخدمة هو القدرة على تقديم حزمة تكامل كاملة من السحابة، بما في ذلك التفاعل مع التطبيقات والوساطة الدلالية والتحكم في التدفق وتصميم التكامل وما إلى ذلك، في الأساس يشمل التكامل كخدمة معظم الميزات والوظائف الموجودة في تقنية تكامل تطبيقات المؤسسات التقليدية (EAI) ولكن يتم تقديمها كخدمة.

٨ .الأمن كخدمة Security-as-a-service

الأمن كخدمة، كما قد تكون خمنت، هو القدرة على تقديم خدمات الأمان الأساسية عن بعد عبر الإنترنت، في حين أن الخدمات الأمنية النموذجية المقدمة بدائية، أصبحت الخدمات الأكثر تعقيداً مثل إدارة الهوية متاحة.

٩ .الإدارة / الحوكمة كخدمة كخدمة Management/governance-as-a-service

الإدارة / الحوكمة كخدمة MaaS و GaaS هي أي خدمة عند الطلب توفر القدرة على إدارة واحدة أو أكثر من الخدمات السحابية، هذه عادةً أشياء بسيطة مثل الهيكل، واستخدام الموارد، والافتراضية، وإدارة الجهوزية، أصبحت أنظمة الحوكمة متاحة أيضاً، حيث تقدم ، على سبيل المثال ، القدرة على فرض سياسات محددة على البيانات والخدمات.

١٠. الاختبار كخدمة Testing-as-a-service (TaaS)

الاختبار كخدمة (TaaS) هو القدرة على اختبار الأنظمة المحلية أو السحابية باستخدام برامج الاختبار والخدمات التي يتم استضافتها عن بُعد، وتجدر الإشارة إلى أنه على الرغم من أن الخدمة السحابية تتطلب الاختبار في حد ذاتها، فإن أنظمة الاختبار كخدمة لديها القدرة على اختبار التطبيقات السحابية الأخرى ومواقع الويب وأنظمة المؤسسات الداخلية، ولا تتطلب وجود أجهزة أو برامج داخل المؤسسة.

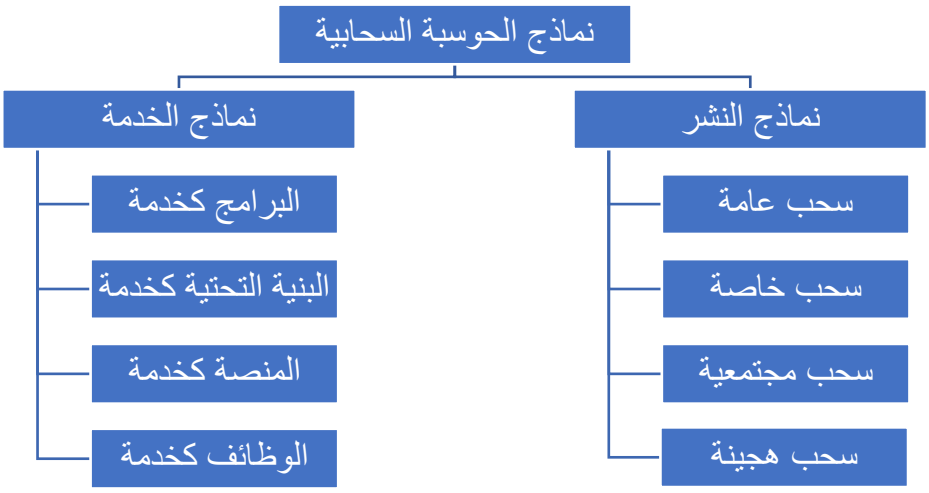
١١. البنية التحتية كخدمة Infrastructure-as-a-service (IaaS)

البنية التحتية كخدمة (IaaS) هي في الواقع مركز بيانات كخدمة، أو القدرة على الوصول عن بعد إلى موارد الحوسبة، من حيث الجوهر، فإنك تستأجر خادماً فعلياً يخصك بما تريد، ولجميع الأغراض العملية، يكون مركز البيانات الخاص بك، أو على الأقل جزءًا من مركز البيانات.

يتمثل الاختلاف بين هذا الأسلوب والحوسبة السحابية الأكثر شيوعاً في أنه بدلاً من استخدام واجهة وخدمة محدودة، يمكنك الوصول إلى الجهاز بأكمله والبرنامج الموجود على هذا الجهاز، باختصار إنها أقل حزماً.

نماذج بناء الحوسبة السحابية

هناك نوعان من النماذج في الحوسبة السحابية تسمى نماذج النشر ونماذج الخدمة، تصف نماذج النشر نوع الوصول إلى السحابة، هذه الأنواع عامة وخاصة ومجتمعية ومختلطة، بينما نماذج الخدمة فهي البرمجة كخدمة، البنية التحتية كخدمة، المنصة كخدمة، والوظائف كخدمة. انظر إلى شكل ٣.

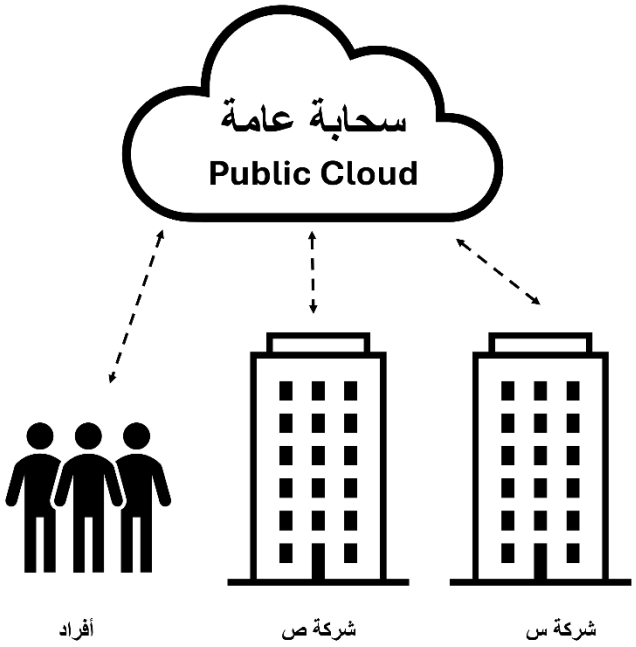


شكل ٣ أنواع نماذج الحوسبة السحابية

تنقسم نماذج الحوسبة السحابية حسب النشر إلى أربعة أنواع، وهي:

١. السحابة العامة والتي توفر الخدمات لعامة الناس.
٢. السحابة الخاصة والتي توفر الخدمات للمؤسسة.
٣. السحابة المجتمعية والتي توفر خدمات لمجموعة من المنظمات
٤. السحابة المختلطة وهي مزيج من السحب العامة والخاصة، في الهجين، تقوم السحابة الخاصة بتنفيذ الأنشطة الهامة بينما تقوم السحابة العامة بتنفيذ أنشطة غير حرجة.

النموذج الأول: السحب العامة Public clouds

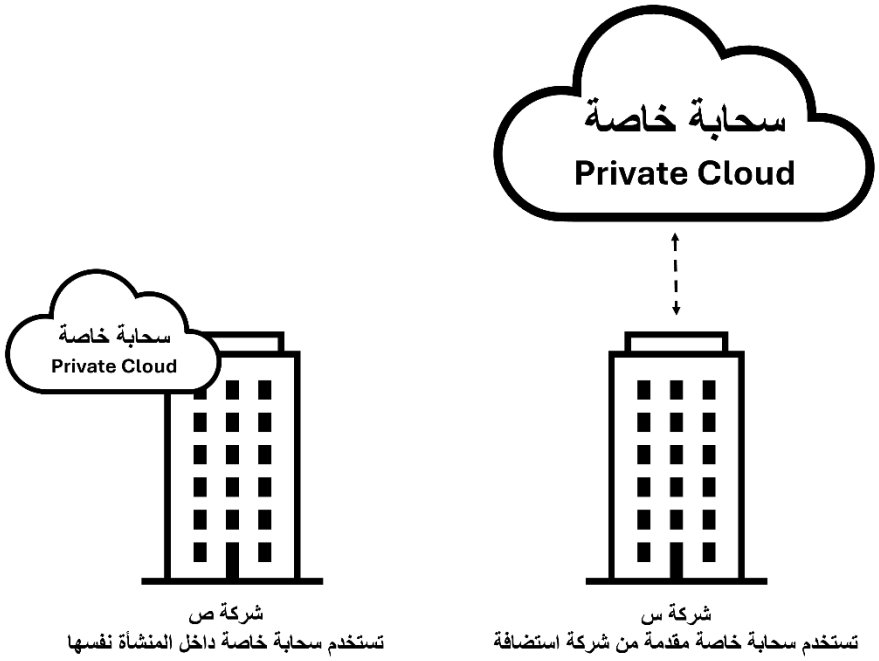


شكل ٤ السحب العامة

مواصفاتها:

١. تقدم خدماتها لعملاء متعددين، انظر إلى شكل ٤.
٢. توجد في منشأة خارجية (منشأة التجميع)
٣. تستضاف في مكان بعيد عن مكان العميل
٤. وسيلة مرنة لتوفير التكاليف والحد من المخاطر
٥. امتداد مؤقت للبنية التحتية للمنشآت

النموذج الثاني: السحب الخاصة Private clouds



شكل ٥ السحب الخاصة

مواصفاتها:

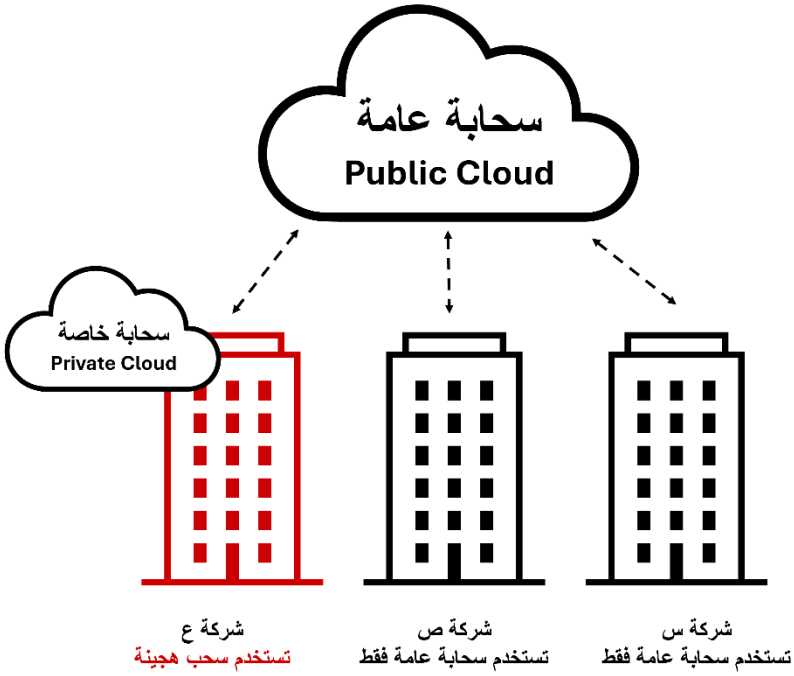
١. يمكن استضافة السحب الخاصة في منشأة خارجية أو في داخل المنشاة، انظر إلى شكل ٥.

٢. قد تكون معتمدة من قبل:

- المنشاة
- مقدم سحابة
- من قبل طرف ثالث مثل شركة الاستضافة

٣. تعطي المنشأة فرصة المراقبة على السحابة.

النموذج الثالث: السحب الهجينة Hybrid clouds

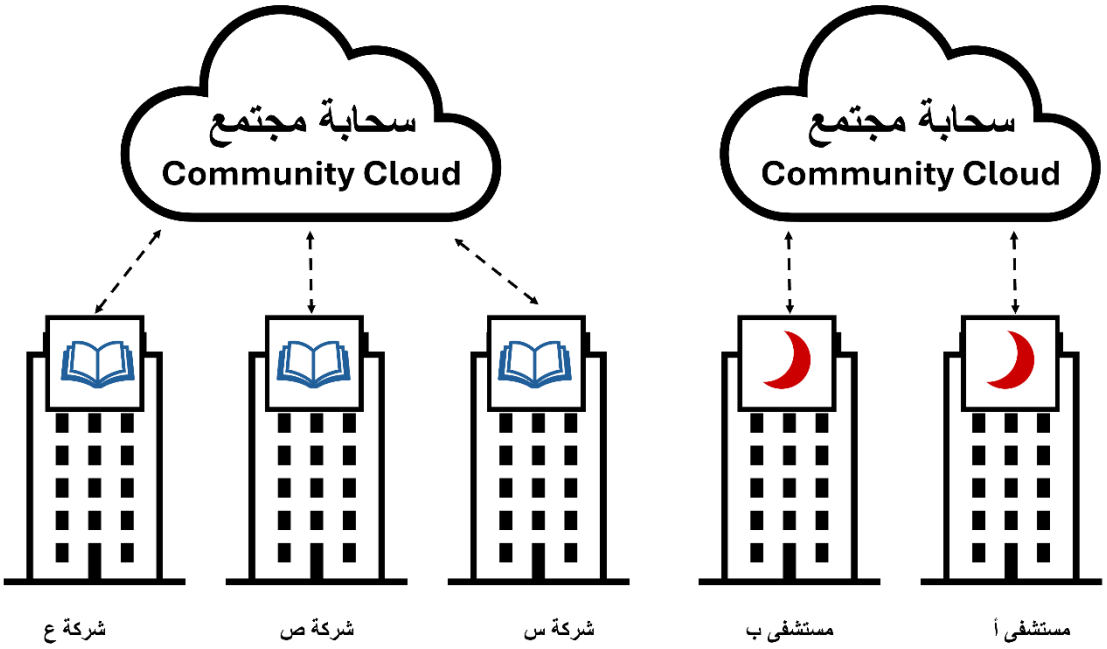


شكل ٦ السحب الهجينة

مواصفاتها:

- تجمع بين خصائص السحب العامة والخاصة، انظر شكل ٦.
- تستخدم في المنشأة ذات البيانات الصغيرة أو التي تحتاج تطبيقات خاصة بها.
- يمكن للعميل الاختيار بين تطبيقات وخدمات السحابة العامة أو السحابة الخاصة
- للمنشاة خيار الحفاظ على السيطرة والأمن.

النموذج الرابع: سحب المجتمع community clouds



شكل ٧ السحب المجتمعية

مواصفاتها:

- تعد النموذج الأحدث من الحوسبة السحابية
- ظهرت نتيجة الضغوط على البيئة التعليمية بهدف تطويرها
- ساعد على نشأتها التعاون بين سوق العمل والتعليم المرتكز على الجودة والابداع
- خصصت خدماتها على المناهج الدراسية واحتياجات المجتمع المهنية والعلمية انظر شكل ٧.

نماذج خدمات الحوسبة السحابية:

يوضح شكل ٨ نماذج الحوسبة السحابية حسب الخدمات.

شكل ٨ أنواع الحوسبة السحابية حسب الخدمة المقدمة

١. البرمجيات كخدمة SaaS (Software as a service)

البرمجيات كخدمة (SaaS) ويعتبر هذا النوع من الخدمات هو الأكثر استخداماً في الحوسبة السحابية، حيث إنها توفر وصول مستأجرين متعددين من السحابة إلى تطبيق معين، تتيح عروض SaaS الاستفادة من السحابة لبنية البرامج وبالتالي تقليل النفقات العامة للدعم والصيانة والعمليات حيث تعمل التطبيقات على أنظمة تابعة للبائع، يتفاعل المستخدمون غالباً بشكل مباشر مع تطبيقات SaaS .

SaaS هو عرض قائم على الاشتراك حيث يشترك المستخدمون في البرنامج بشكل شهري بدلاً من شرائه، لذلك لا توجد تكاليف مسبقة متضمنة، كما أنه يتيح للمستخدمين إنهاء الاشتراك عند رغبتهم بالتوقف عن استخدام الخدمات.

أمثلة على خدمات الحوسبة السحابية SaaS

Netflix أو Gmail أو JIRA أو Dropbox أوSalesforce .

Office 365 هو شكل من أشكال SaaS وفيه يمكن لأي شخص فتح اشتراك شهري لاستخدام مجموعة منتجات Microsoft Office .

ميزات وفوائد خدمة الحوسبة السحابية SaaS

- لا توجد تكلفة إعداد أولية حيث يمكن للمستخدمين الاستفادة من التطبيق بمجرد الاشتراك، بالإضافة لذلك لا توجد تكلفة عليك دفعها من أجل الأجهزة لأن طاقة المعالجة يتم توفيرها بواسطة مزود الخدمة.
- عملية الدفع تعتبر مرنة حيث يدفع المستخدمون مقابل الخدمات التي يحصلون عليها.
- أي تحديثات تصدر للبرنامج تتم بشكل تلقائي ومجاني.
- توفر SaaSالتوافق عبر الأجهزة حيث إنها تمكنك من الوصول إلى التطبيقات من خلال أي أجهزة تدعم الإنترنت، مثل الحاسوب المحمول أو الهاتف الذكي أو سطح المكتب.
- لا تحتاج الشركات إلى الاستعانة بخبير في تقنية المعلومات لتنزيل البرنامج على عدة أنظمة ولا داعي للقلق بشأن تحديث البرنامج على كل جهاز حاسب لأن التحديثات تلقائية كما ذكرنا.

٢. البنية التحتية كخدمة IaaS (Infrastructure as a Service)

تشمل البنية التحتية كخدمة (IaaS)البنية الأساسية للسحابة وتوفر الوصول إلى وظائف الشبكة والأجهزة الافتراضية والأجهزة المخصصة ومساحة التخزين.

Windows Azure و Amazon Web Services هما مزوّدان شائعان لـ IaaS يمكن كل منهما المستخدمين من الاستعانة بمصادر خارجية للبنية التحتية مثل مساحة النسخ الاحتياطي والتخزين والمساحة اللازمة للاختبار والمزيد، يوفر Azure الوصول إلى الشبكات الافتراضية وقوائم انتظار الرسائل وأنظمة التخزين غير العلائقية (قواعد البيانات).

تساعد IaaS المستخدمين على استخدام قوة الحوسبة والمعالجة أو الأجهزة الافتراضية دون الحاجة لاستثمارات في الأجهزة باهظة الثمن أو إدارة الخادم مادياً، يتم سحب موارد الأجهزة من مجموعة متنوعة من الشبكات والخوادم الموزعة عبر مراكز بيانات مختلفة، والتي تتم إدارتها وصيانتها جميعاً بواسطة مزود الخدمة السحابية.

على سبيل المثال، لنفترض أن المستخدم يريد نظامLinux ، فمع IaaS سيحصل على إمكانية الوصول إليه دون الحاجة إلى القلق بشأن شبكة الجهاز الذي تم تثبيت Linux عليه أو النظام الفعلي.

أمثلة على خدمات الحوسبة السحابية IaaS

Amazon EC2 و Windows Azure و Rackspace و Google Compute Engine

ميزات وفوائد خدمة الحوسبة السحابية IaaS

- توفر البنية التحتية النموذجية خدمة توفير الوقت والمال، حيث يتم توفير الأجهزة الأساسية والدعم من قبل مزود الخدمة.
- تتوفر الموارد عند الطلب، أي عند الحاجة لها وبالتالي لا يوجد هدر لأي موارد غير مستخدمة ولا تأخير في إضافة أي موارد.
- نموذج التسعير القائم على المنفعة، أي ادفع فقط مقابل الموارد التي تستخدمها بالفعل.

٣. المنصة كخدمة PaaS (Platform as a service)

المنصة كخدمة (PaaS) يشمل الأجهزة وأنظمة التشغيل اللازمة لنشر وإدارة التطبيقات السحابية، تساعد PaaS على زيادة كفاءة الأعمال دون متاعب إدارة الحلول المستندة إلى السحابة والتخطيط لها وشرائها وصيانتها، يسير كل من PaaS و IaaS جنباً إلى جنب لأنك بحاجة إلى نظام أساسي لإدارة البنية التحتية لتقنية المعلومات.

تعد خدمات Windows Azure السحابية أيضاً موفر PaaS الذي يدعم NET و Node.js و PHP و Python و Java و Ruby مع مجموعات تطوير البرامج و Visual Studio ويضعها تحت تصرف المطورين، حيث يمكن للمطورين إنشاء التطبيقات ونشرها بسهولة.

خدمة الحوسبة السحابية PaaS هي نسخة متقدمة من IaaS ، فهي توفر للمطورين إطار عمل يمكن استخدامه لإنشاء تطبيقات مخصصة عبر الإنترنت دون الحاجة إلى القلق بشأن تخزين البيانات وخدمة البيانات وإدارتها.

تتكون المنصة كخدمة من:

- حلول الاستضافة
- نظام التشغيل
- أدوات برمجية للتصميم والتطوير.
- بيئة البرمجة النصية من جانب الخادم
- نظم إدارة قواعد البيانات
- الوصول إلى الشبكة
- التخزين
- برنامج الخادم
- الدعم

أمثلة على خدمات الحوسبة السحابية PaaS

Google App Engine و Rackspace Cloud Sites و OpenShift و Apache Stratos

ميزات وفوائد خدمة الحوسبة السحابية PaaS

- تجعل PaaS تطوير البرامج أمرًا سهلاً حتى لغير الخبراء حيث يمكن لأي شخص تطوير تطبيق من خلال متصفح الويب.
- لن يحتاج مستخدمو هذه الخدمة ترقية البنية التحتية أو تحديثها لأن موفر خدمة PaaSيتعامل مع جميع تصحيحات التحديث والترقيات وصيانة البرامج المنتظمة.
- توفر PaaS استقلالية الموقع حيث يمكن للمطورين في مواقع مختلفة العمل معًا على نفس بنية التطبيق.
- ليست هناك حاجة للاستثمار في البنية التحتية المادية.

٤. الوظائف كخدمة FaaS (Function as a service)

قبل أن نفهم الوظائف كخدمة FaaS، من المهم أن نفهم المصطلح التقني الأكثر شيوعاً المرتبط بـها وهو الحوسبة بدون خادم Serverless **الحوسبة بدون خادم** هي نموذج تنفيذ الحوسبة السحابية حيث يقوم موفر السحابة بتخصيص موارد الجهاز عند الطلب، مع الاهتمام بالخوادم نيابة عن عملائه، لا يحتاج مطورو التطبيق هنا إلى التعامل مع تخصيص الموارد حيث يتم إدارتها بواسطة مزود الخدمة السحابية.

خدمة FaaS هي خدمة حوسبة سحابية جديدة تماماً وصغيرة جداً تعمل كمغير لقواعد اللعبة للعديد من الشركات، تعتبر Faas مفهوم يندرج تحت الحوسبة بدون خادم يتيح لمطوري البرامج تطوير التطبيقات ونشر "وظيفة" فردية أو منطق عمل أو إجراء بدون صيانة خادم بالإضافة لأنه يزيد من الكفاءة حيث لا يحتاج المطورون إلى النظر في عمليات الخادم لأنها مستضافة خارجياً.

أمثلة على خدمات الحوسبة السحابية FaaS

وظيفة Google Cloud ووظائف Microsoft Azure و Webtask.io و Iron.io و Open Whiskو.AWS Lambda

ميزات وفوائد خدمة الحوسبة السحابية FaaS

- لا يتم إهدار الأموال مطلقاً على الموارد غير النشطة حيث يتم إصدار فاتورة للمستخدمين اعتمادًا على مقدار الوظائف المستخدمة.
- يجعل المطورين أكثر كفاءة حيث يمكنهم التركيز بشكل أكبر على كتابة منطق خاص بالتطبيق بدلاً من الاضطرار إلى التعامل مع لوجستيات الخادم.
- كود FaaS قابل للتطوير والتوسع بطبيعته ومتسامح مع الأخطاء.

قد تختار أن تبدأ بنموذج واحد لخدمة الحوسبة السحابية أو أنك قد تجد الحاجة لاستخدام النماذج الأربعة التي ذكرناها في هذا المقال وكل ذلك يعتمد على حجم وتعقيد عملك، تتيح حلول أعمال الحوسبة السحابية لشركتك الاستفادة من الموارد التي يديرها مقدمو الخدمات السحابية والتي يتم تخزينها في خوادم وشبكات خاصة وآمنة، كما توفر الحلول السحابية حلاً سهلاً لإجراء نسخ احتياطي لبياناتك الهامة مما يساهم في تعزيز خطة التعافي من الكوارث في مؤسستك.

مميزات وخصائص الحوسبة السحابية

تمتاز الحوسبة السحابية بعدد من الخصائص وهي كالتالي:

١- مركزية المستخدم: وتعني أنه بمجرد أن يتصل المستخدم بالسحابة فإنه يصبح مالكا لما يخزنه عليها ويستطيع مشاركة ما يقوم بتخزينه عبر الانترنت مع غيره من المستخدمين.

٢- مركزية المهام: بدلاً من تركيز السحابة على التطبيقات مثل معالجة النصوص وجداول البيانات والبريد الالكتروني وما يمكنا القيام به، ينصب تركيزها على تلبية احتياجات المستخدمين من خلال هذه التطبيقات.

3- مركزية البنية التحتية: توفر السحابة الخوادم الضخمة التي تساعد في اجراء العمليات مما يساعد على التحرر من أعباء انشاء وإدارة البنية التحتية .

4- مركزية التطبيقات والمستندات: والتي يتم تشغيلها وتخزينها وتحريرها بخوادم السحابة من خلال أي جهاز متصل بخط انترنت مما يوفر الإتاحة الدائمة، ويحق للمالك الأصلي أن يخول حق الوصول لملفاته والتعديل ولحذف والإضافة لمن يشاء من العملاء ، وهذا يعزز التعاون بين أعضاء المجموعات.

5-طاقة الحوسبة: وتنتج من خلال ارتباط آلاف من الأجهزة والخوادم معاً.

6- الوصول: حيث يتيح تخزين البيانات في السحابة استرداد المزيد من المعلومات من عدد مختلف من المستودعات.

7- الذكاء: وهو مطلب لاستخراج وتحليل البيانات الضخمة المخزنة على مختلف خوادم السحابة.

8-البرمجة: وهي مطلب أساسي عند التعامل مع العديد من المهام الضرورية بالسحابة مثل حماية أمن المعلومات.

9-المرونة: الحوسبة السحابية توفر المزيد من المرونة (غالباً ما تسمى بالتمدد) في مطابقة موارد تكنولوجيا المعلومات ووظائف العمل التي كانت تعتمد أساليب الحوسبة الماضية، ويمكن أيضاً زيادة تنقل وحركة الموظفين من خلال تمكين الوصول إلى معلومات الأعمال والتطبيقات من خلال مجموعة واسعة من المواقع والخدمات ،كما أن مشاركة المصادر من خلال خدمات الحوسبة توفر سهولة ومرونة أكبر عند أداء المهام المختلفة، وتقدم إمكانيات الربط بين عدة موقع إلكترونية، مثل الشبكات الاجتماعية.

١٠- سهولة التنفيذ: تستطيع المؤسسة اعتماد ونشر تطبيقات الحوسبة السحابية دون الحاجة لشراء الأجهزة، وتراخيص البرامج، أو خدمات التركيب والتشغيل والصيانة.

١١- قابلية التوسع : المنظمات التي تستخدم الحوسبة السحابية لا تحتاج لأن تضيف أجهزة وبرمجيات ذات معايير وكفاءات أعلى عند زيادة عدد المستخدمين ، وليست مضطرة لشراء موسعات جديدة (شراء المزيد من الحواسيب وأنظمة التخزين والمحولات وأجهزة التوجيه) في نهاية المطاف ، فإن معظم هذه الموارد غير مستغلة طيلة الوقت ولكن يمكن بدلا من ذلك جمع وطرح القدرات كما تملي أحمال الشبكة ، كما أنه بإمكانها التطور والتوسع من خلال النقر على المربعات المناسبة الموجودة على موقع مزود الخدمة والحوسبة السحابية تضمن السرعة في الانضمام والتعاطي مع التقنيات الحديثة على الانترنت.

اقتصاديات بيئة الحوسبة السحابية

الاقتصاد الرقمي

الحوسبة السحابية تلعب دورًا محوريًا في بناء الاقتصاد الرقمي الجديد، كما أن المنافسة في هذا المجال تساهم في تيسير اللوائح التنظيمية مما سيشجع الابتكار، ويساعد في خلق منظومة رقمية أفضل لصالح الشركاء والشركات والمستفيدين، كما أن جائحة كورونا ساهمت في الإسراع من وتيرة التوجه العالمي نحو التحول الرقمي واستخدام البيانات، لافتةً إلى أن الحوسبة السحابية باتت اليوم مُمَكِنًا أساسيًا لمجموعة من الخدمات والحلول التقنية الجديدة بما في ذلك الذكاء الاصطناعي، وسلسلة الكتل، والتشفير، والواقع المعزز/الواقع الافتراضي، وغيرها.

الفوائد الاقتصادية للحوسبة السحابية للشركات:

توفر الحوسبة السحابية العديد من الحوافز الاقتصادية والمزايا التجارية الأخرى التي يمكن أن تساعد في تعزيز القيمة الإجمالية للشركة وإيراداتها ثم يتم إنفاق التكلفة الموفرة على تدريب الموظفين. يمكن وضع بعض هذه الفوائد في نقاط، وهي كالتالي:

- **تكلفة مخفضة**

أعظم شيء في الانتقال إلى السحابة هو أنك لا تحتاج إلى أجهزتك الخاصة لأن كل شيء متاح ومستضاف على الخادم، وهذا يساعد في تقليل تكاليف الأجهزة، ويساعد على الابتكارات الجديدة.

- **قابلية التوسع**

يمكن للشركة زيادة أو تقليل متطلبات التشغيل والتخزين الخاصة بهم بسرعة، فمع استخدام السحابة لا يلزمك شراء التحديثات باهظة الثمن وَتثبيتها بنفسك، بل سيديرها مزود الخدمة السحابية نيابة عنك.

- **النشر السريع للمشروع**

تستغرق التطبيقات المستندة إلى السحابة وقتًا أقل لتحقيق الهدف المحدد، ويمكن تنزيل معظم التطبيقات السحابية فور التسجيل، كما توفر السحابة نشر سريع للتطبيقات.

- **التخفيف من المخاطر مع زيادة الأمن**

تزداد التهديدات السيبرانية نشاطًا يومًا بعد يوم وللتخفيف من أخطار فقدان البيانات وخرق البيانات وخطر الوصول غير المصرح به، توفر الحوسبة السحابية ضمانات قوية، كما تقدم السحابة تقنية جدار حماية قوية مع أنظمة مكافحة السرقة وأنظمة مكافحة الفيروسات القوية.

- **بيئة عمل مرنة**

نظرًا لتوفر السحابة على الإنترنت، فإنها تمكن الموظفين من الوصول إلى الملفات من أي مكان في العالم وفي أي وقت وتسمح لهم بالعمل عن بُعد ومن المنزل، وبالتالي تقليل تكلفة نفقات المساحات المكتبية.

وتشير التقديرات إلى أن أكثر من ٢,٦ مليار هاتف ذكي قيد الاستخدام على مستوى العالم وجميعها فيها تطبيقات تتعامل مع السحابة، وتوفر الحوسبة السحابية الوصول المحمول إلى بيانات الأعمال عبر الهواتف الذكية والأجهزة.

مبادئ اقتصاديات السحابة الحديثة

تتيح مبادئ اقتصاديات السحابة الحديثة للمؤسسات تحقيق أقصى قدر من قيمة الأعمال من خلال التكنولوجيا السحابية، وخاصة في المجالات ذات المهام بالغة الأهمية. وتشمل هذه المبادئ:

١. الحجم الصحيح والمناسب لمجموعة التقنية الحديثة (مثال التوسيع التلقائي للحجم في أوقات الذروة)
٢. التحسين المستمر للاستخدام والأسعار (مثال إزالة وحدات التخزين الخاملة لتقليل السعر)
٣. الشفافية في الوقت الحقيقي بشأن الاستخدام والتكاليف والتخصيص (ذلك يمنح فِرق المشاريع المختلفة رؤية واضحة لإدارة موارد السحابة وقدرة على المساءلة وصنع القرار)
٤. التعاون متعدد الوظائف مدفوعًا بقيمة الأعمال

تعمل هذه المبادئ على تحويل المؤسسات من تخطيط التقليدي للسعة إلى التحسين المستمر للطلب الحقيقي. وهي تربط الإنفاق السحابي بنتائج أعمال محددة، وتضفي اللامركزية على عملية صنع القرار، وتعزز التعاون بين جميع أصحاب المصلحة، مما يحول الإدارة المالية من توفير التكاليف إلى إنشاء القيم.

وعلى وجه التحديد، فقد تمكنت المؤسسات من:

- تحويل تخطيط الطاقة الإنتاجية المستقبلي إلى حالة التحسين المستمر للاستخدام والأسعار بناءً على الطلب الحقيقي.
- ربط النفقات السحابية بقيمة الأعمال مثل الحسابات الجديدة والطلبات المستوفاة وزيادة استخدام المعدات التشغيلية.
- نقل ملكية التقنية والمسؤولية التشغيلية والمالية إلى مستوى المنظمة.
- تغيير تركيز الإدارة المالية من توفير المال إلى تحقيق الربح باستخدام 'اقتصاديات الوحدات.'
- تعزيز التعاون بين المديرين التنفيذيين والمستخدمين والمطورين وأمن المعلومات والإدارة المالية والمشتريات ومزودي الخدمات السحابية باستخدام مجموعة مشتركة لإدارة الأعمال التقنية.

أمن الحوسبة السحابية

أ. تهديدات أمن الحوسبة السحابية

أهم ثلاثة عشر تهديداً للحوسبة السحابية اعتماداً على آراء الخبراء، **وجرى ترتيبهم بحسب مستوى الخطورة على النحو التالي:**

١. تسريب البيانات Data Leakage

قد تتسرب البيانات من خلال أي هجوم إلكتروني قد يتعرض له النظام، أو بسبب الأخطاء البشرية أو نتيجةً لوجود ثغرات (نقاط ضعف) في التطبيقات التي نستخدمها، وقد تحدث كذلك بسبب الاستهانة بالممارسات الأمنية اللازمة. وهو الكشف عن معلومات سرية (غير مُخصصة لاطلاع العَلن) بما في ذلك البيانات الشخصية الصحية والمالية والأسرار التجارية والملكية الفكرية وأي بيانات يُمكن من خلالها كشف هوية الأشخاص، وجميعها بيانات قد تصب في صالح أطراف عدة لأسباب مختلفة، وعلى الرغم من أن خطر تسريب البيانات ليس قاصراً على الحوسبة السحابية، إلا أنه دائماً ما يتقدم قائمة الأخطار.

٢. قصور في إدارة الهوية وبيانات الاعتماد والوصول للحسابات

يمكن هذا التهديد الأطراف الخارجية من الوصول إلى البيانات وتعديلها وحذفها، في حين أن النظام يعتبرهم مستخدمين مُخول لهم بالوصول لهذه البيانات. وعلاوةً على ذلك، يمكن للمهاجمين وضع خطط تحكم في المهام الإدارية، ومن التطفل على البيانات وإدخال برمجيات ضارة تبدو كأنها من مصادر مسموح بها، وربما يؤدي ذلك إلى آثار كارثية على المؤسسات والمستخدمين النهائيين .

٣. ضعف أمن واجهات الاستخدام وواجهات برمجة التطبيقات

يقوم مستخدمي الحوسبة السحابية بالاعتماد على العديد من واجهات مستخدمي البرمجيات (user interface)، والواجهات الخاصة برمجة التطبيقات لتنظيم مهام الخدمات السحابية ومراقبتها، ويقوم أمن الخدمات السحابية وتواجدها على حماية الواجهات الخاصة بالتطبيقات، ومن ثَم فهناك حاجة ماسة لتصميمها على نحوٍ يضمن الحماية من المحاولات العرضية والخبيثة للتحايل على أمن البيانات .

٤. الثغرات الأمنية ونقاط الضعف في الأنظمة السحابية

تعتبر نقاط الضعف والثغرات الأمنية في أنظمة التشغيل بوابات يقوم المخترقين باستغلالها في محاولة الدخول إلى نظام ما، ليتم بعد ذلك تحقيق أهداف المخترقين من سرقة البيانات أو السيطرة على النظام أو تعطيل الخدمة عن المستخدمين والعملاء، وتُعرِّض نقاط الضعف أمن جميع الخدمات والبيانات للخطر، ويتفاقم الخطر وتزيد معه فرص الهجوم في ظل تخزين مؤسسات مختلفة لبياناتها سحابياً معتمدة على ذاكرة وموارد مشتركة.

٥. إمكانية سرقة على حسابات المستخدمين

لا تُعد عمليات سرقة الحسابات أمراً جديداً، ولكن الخدمات السحابية ضاعفت هذه التهديدات، وفي حال توصل المهاجمون إلى بيانات دخول المستخدم، فسيصبح بإمكانهم التنصت على الأنشطة والمعاملات، والتلاعب بالبيانات وإرسال معلومات مزيفة، وإعادة توجيه العملاء إلى مواقع غير موثوقة، كما سيتمكن المهاجمون بواسطة البيانات المسروقة من التحكم في وظائف بالغة التأثير في خدمات الحوسبة السحابية ومن ثم تهديد سرية هذه الخدمات وسلامتها وتوافرها .

٦. الأخطار الأمنية الداخلية المحتملة في المؤسسات

بالإضافة إلى الأخطار الخارجية، قد يحدث أي من الأخطار الأمنية على أمن الحوسبة السحابية، وذلك عن طريق العاملين في المؤسسات، حيث يمكن لأي مسؤول إداري يحمل الصلاحيات اللازمة على الأنظمة التي تمكنه من الوصول إلى معلومات مؤثرة، كما قد يتمتع بقدرات على الوصول إلى أنظمة أكثر حساسية تسمح له بالاطلاع على البيانات نفسها في نهاية المطاف، وتظل الأنظمة المعتمدة في تأمينها على مُزودي الخدمات السحابية وحدها عُرضة لأخطارٍ أكبر.

٧. التهديدات المستمرة والهجمات السيبرانية

تتعد أنواع الهجمات السيبرانية (cyber-attack) ومنها التي تحاول التسلل إلى الأنظمة لتكون نقطة دخول لها في البنية التحتية لتكنولوجيا المعلومات للشركات المستهدفة، وتتمكن من خلالها من سرقة البيانات، وتسعى التهديدات المستمرة المتقدمة (Advanced Persistent Threat) إلى بلوغ غاياتها خفيةً على مدار فترات زمنية طويلة، وغالباً ما تتكيف مع التدابير الأمنية المُضادة، وبمجرد وصولها إلى الموقع المُراد، تتنقل في طرق فرعية عبر شبكات مراكز البيانات وتندمج مع الحركة العادية لمرور البيانات سعيًا لتحقيق أهدافها .

٨. ضياع بيانات المستخدمين وفقدانها

قد يتم ضياع العديد من البيانات التي يتم تخزينها في الحوسبة السحابية، دون وجود نسخ احتياطية للبيانات، حيث يتم ذلك لأسباب عديدة غير الهجمات السيبرانية كالكوارث الطبيعية، فقد يسبب الحذف العرضي من جانب مُزودي الخدمة السحابية -الذي قد يكون بسبب الحرائق أو الزلازل- إلى ضياع دائم لبيانات العملاء، ولذلك يتعين على المزودين والعملاء اتباع التدابير المناسبة بعمل نسخة احتياطية للبيانات وتطبيق توجيهات المحافظة على استمرارية العمل والتعافي من الكوارث.

٩. قلة العناية اللازمة في الخطط الإستراتيجية للازمة للنظام

يجب على مديري الأعمال ومقدمي الخدمات مراعاة التقنيات السحابية عند إعداد الخطط الاستراتيجية، لذلك يُعد تطوير خطة جيدة وقائمة على مراجعة متطلبات الأمان عند تقييم التقنيات ومقدمي الخدمات أمراً ضرورياً لزيادة فرص النجاح. وعلى العكس من ذلك، فإن سرعة المؤسسات في اختيار التقنيات والخدمات السحابية دون إجراء تقييم دقيق لميزات الأمان الخاصة بها تجعلها عرضة لمخاطر كبيرة.

١٠. إساءة استخدام الخدمات السحابية

تتبع الهجمات الضارة عدة مسارات، بما في ذلك الخدمات السحابية غير المُؤمّنة بشكل جيد، والعروض المجانية لتجربة الخدمات السحابية، والاحتيال في طرق الدفع، ويمكن للمهاجمين استغلال موارد الحوسبة السحابية لاستهداف المستخدمين أو المؤسسات أو مقدمي الخدمات السحابية الآخرين. وتتضمن أمثلة إساءة الاستخدام هجمات رفض الخدمة المُوزعة والبريد العشوائي وحملات التصيد الإلكتروني .

١١. هجمات الحرمان من الخدمة DoS Attack

تهدف هجمات رفض الخدمة أو الحرمان من الخدمة (Denial of service attack) إلى منع المستخدمين من الوصول إلى بياناتهم أو تطبيقاتهم. يحدث ذلك عن طريق إجبار الخدمة السحابية المستهدفة على استهلاك كميات هائلة من مواردها المحدودة. مثل طاقة المعالجة، أو الذاكرة، أو مساحة التخزين، أو عرض النطاق الترددي للشبكة، ممّا يتسبب هذا الهجوم في إبطاء الخدمة ومنع الجميع من الوصول إليها .

١٢. ثغرات ونقاط ضعف تقنية شائعة

يقوم مقدمي الخدمات السحابية بمشاركة الكثير من الموارد الضرورية لهم، والتي تشمل الأنظمة الرئيسية والبنية التحتية وكذلك التطبيقات اللازمة، وكما يتم استخدام الأجهزة والبرمجيات المُتاحة بالفعل في الأسواق دون تعديلها، الأمر الذي قد يخل بالمعايير الأمنية، وفي بعض الأحيان لا تُصَمم البنية التحتية التي تدعم الخدمات السحابية على نحو يُؤمن خصائص عزل قوية للتطبيقات متعددة العملاء، وقد يؤدي ذلك إلى انتشار ثغرات تقنية من المُحتمل استغلالها في جميع نماذج التسليم .

١٣. تهديدات قد تسمح بقراءة البيانات المشفرة من الذاكرة

في عام ٢٠١٨، كشف الباحثون عن ميزة تصميم لمعظم المعالجات الدقيقة الحديثة، والتي يمكن أن تسمح بقراءة المحتوى، بما في ذلك البيانات المشفرة من الذاكرة باستخدام كود (Java) خبيث، وتظهر هذه المشكلة في صورتين تسمى (Meltdown) و (Specter)، كلاهما يسمح بهجمات القناة الجانبية التي تلغي العزلة بين التطبيقات، ويؤثر النوعان على أنواع مختلفة من الأجهزة من الهواتف الذكية إلى الخوادم ،وبالتالي يتم تصنيفهما ضمن التهديدات التي تستهدف الحوسبة السحابية.

ب. إجراءات أمن الحوسبة السحابية

ما هو الأمن السحابي؟

الأمن السحابي هو مجموعة كاملة من التقنيات والبروتوكولات وأفضل الممارسات التي تحمي بيئات الحوسبة السحابية والتطبيقات التي تعمل في السحابة والبيانات المحفوظة فيها، ونظراً لأن الحوسبة السحابية تُستخدم الآن من قبل أكثر من ٩٠٪ من الشركات الكبرى، فإن الأمن السحابي يُعد جزءاً حيوياً من الأمن السيبراني للشركات. حيث تؤثر مخاطر أمن الحوسبة السحابية أيضاً على المستهلكين من الأفراد، حتى لو لم يدركوا ذلك دائماً، ويمكن للمستهلكين استخدام السحابة لتخزين الملفات ونسخها احتياطياً باستخدام بعض الخدمات مثل (Dropbox) أو لبعض الخدمات مثل البريد الإلكتروني والتطبيقات المكتبية أو لعمل نماذج وحسابات ضريبية.

يمكن للشركات الإصرار على استخدام السحب الخاصة وهو البديل المتوفر عبر الإنترنت لامتلاك مبنى مكتبي أو مقر خاص بك. بينما يستخدم الأفراد والشركات الصغيرة الخدمات السحابية العامة، فإن ذلك يشبه مشاركة مكتب أو العيش في مبنى سكني مع مئات من المستأجرين الآخرين. لذلك يجب أن يكون أمانك مصدر قلق رئيسياً، عليك التأكد من أن بياناتك منفصلة عن بيانات العملاء الآخرين، سواء كانت مُشفرة بشكل منفصل أو مُقسَّمة منطقياً لتخزين منفصل.

إجراءات وممارسات أمان الحوسبة السحابية:

١. الاستراتيجية والسياسة:

يجب أن يأخذ برنامج أمان السحابة الشامل في الاعتبار الملكية والمساءلة (داخلياً / خارجياً) لمخاطر أمان السحابة والثغرات في الحماية / الامتثال وتحديد الضوابط اللازمة لنضج الأمان والوصول إلى الحالة النهائية المرغوبة.

٢. تجزئة الشبكة:

في البيئات متعددة المستأجرين، يجب تقييم التقسيم الموجود بين موارد الشخص المعني وموارد العملاء الآخرين، والاستفادة من نهج المنطقة لعزل الخوادم والتطبيقات والأنظمة الكاملة عن بعضها البعض عندما يكون ذلك ممكناً.

٣. إدارة الهوية والوصول وإدارة الوصول المميز:

الاستفادة من إدارة الهوية وعمليات المصادقة القوية لضمان وصول المستخدمين المصرح لهم فقط إلى بيئة السحابة والتطبيقات والبيانات، وفرض أقل امتياز لتقييد الوصول المميز وتقوية موارد السحابة (على سبيل المثال إلغاء تنشيط السعات / الميزات / الوصول غير الضرورية) والتأكد من أن الامتيازات تستند إلى الأدوار وأن الوصول المميز يتم تدقيقه وتسجيله عبر مراقبة الجلسة.

<u>ضوابط أمان السحابة</u>

تكون بنية أمان السحابة فعالة فقط في حالة وجود عمليات التنفيذ الدفاعية الصحيحة، يجب أن تتعرف بنية أمان السحابة الفعالة على المشكلات التي ستنشأ مع إدارة الأمان تعالج إدارة الأمن هذه المشكلات من خلال الضوابط الأمنية. يتم وضع هذه الضوابط لحماية أي نقاط ضعف في النظام وتقليل تأثير الهجوم، على الرغم من وجود العديد من أنواع عناصر التحكم وراء بنية أمان السحابة، **إلا أنه يمكن العثور عليها عادةً في إحدى الفئات التالية:**

١. الضوابط الرادعة

تهدف عناصر التحكم هذه إلى تقليل الهجمات على نظام السحابة، تماماً مثل علامة التحذير على السياج أو الممتلكات، تعمل ضوابط الردع عادةً على تقليل مستوى التهديد من خلال إبلاغ المهاجمين المحتملين بأنه سيواجهون عواقب وخيمة في حالة استمرارهم. يعتبرها البعض مجموعة فرعية من الضوابط الوقائية.

٢. الضوابط الوقائية

تعمل الضوابط الوقائية على تقوية النظام ضد الحوادث، بشكل عام عن طريق تقليل نقاط الضعف إن لم يكن القضاء عليها فعلياً، المصادقة القوية لمستخدمي السحابة. على سبيل المثال، تجعل من غير المحتمل أن يتمكن المستخدمون غير المصرح لهم من الوصول إلى الأنظمة السحابية، ويزيد احتمال التعرف على مستخدمي السحابة بشكل إيجابي.

٣. ضوابط المباحث

تهدف الضوابط التحريرية إلى اكتشاف أي حوادث تحدث والتفاعل معها بشكل مناسب، في حالة وقوع هجوم، سيشير عنصر تحكم المباحث إلى الضوابط الوقائية أو التصحيحية لمعالجة المشكلة، يتم استخدام مراقبة أمن النظام والشبكة، بما في ذلك ترتيبات الكشف عن التسلل والوقاية منه، للكشف عن الهجمات على الأنظمة السحابية والبنية التحتية للاتصالات الداعمة.

٤. الضوابط التصحيحية

تقلل الضوابط التصحيحية من عواقب أي حادث، عادة عن طريق الحد من الضرر، تدخل حيز التنفيذ أثناء أو بعد وقوع الحادث، تعد استعادة النسخ الاحتياطية للنظام من أجل إعادة بناء نظام مخترق مثالاً على التحكم التصحيحي .

أبعاد أمان السحابة

يوصى عموماً باختيار ضوابط أمن المعلومات وتنفيذها وفقاً للمخاطر وبما يتناسب معها، عادةً عن طريق تقييم التهديدات ونقاط الضعف والتأثيرات، يمكن تجميع مخاوف أمان السحابة بطرق مختلفة، قامت شركة Gartner بتسمية سبعة بينما حدد تحالف أمان السحابة اثني عشر مجالاً للقلق وسطاء أمان الوصول إلى السحابة (CASBs) عبارة عن برمجيات توضع بين مستخدمي السحابة والتطبيقات السحابية لتوفير رؤية لاستخدام التطبيقات السحابية وحماية البيانات والحوكمة لمراقبة جميع الأنشطة وفرض سياسات الأمان.

الأمن والخصوصية

إدارة الهوية

سيكون لكل مؤسسة نظام إدارة الهوية الخاص بها للتحكم في الوصول إلى موارد المعلومات والحوسبة، يقوم مقدمو الخدمات السحابية إما بدمج نظام إدارة هوية العميل في البنية التحتية الخاصة بهم ، باستخدام تقنية الاتحاد أو SSO ، أو نظام تحديد الهوية القائم على القياسات الحيوية ، أو توفير نظام إدارة هوية خاص بهم Cloud ID، على سبيل المثال ، يوفر تحديداً حيوياً قائماً على السحابة ومتعدد المؤسسات للحفاظ على الخصوصية، يربط المعلومات السرية للمستخدمين بقياساتهم الحيوية ويخزنها بطريقة مشفرة، من خلال استخدام تقنية تشفير قابلة للبحث، يتم إجراء تحديد المقاييس الحيوية في مجال مشفر للتأكد من أن موفر السحابة أو المهاجمين المحتملين لا يتمكنون من الوصول إلى أي بيانات حساسة أو حتى محتويات الاستعلامات الفردية.

الأمن المادي

يقوم مقدمو الخدمات السحابية بتأمين أجهزة تكنولوجيا المعلومات (الخوادم وأجهزة التوجيه والكابلات وما إلى ذلك) فعلياً ضد الوصول غير المصرح به والتداخل والسرقة والحرائق والفيضانات وما إلى ذلك ، ويضمنون أن الإمدادات الأساسية (مثل الكهرباء) قوية بما يكفي لتقليل احتمالية الانقطاع، يتم تحقيق ذلك عادةً من خلال خدمة التطبيقات السحابية من مراكز البيانات "ذات المستوى العالمي" (أي المحددة والمصممة والمُنشأة والمدارة والمراقبة والصيانة) بشكل احترافي .

أمن الموظفين

عادة ما يتم التعامل مع مختلف مخاوف أمن المعلومات المتعلقة بتكنولوجيا المعلومات والمهنيين الآخرين المرتبطين بالخدمات السحابية من خلال أنشطة ما قبل التوظيف وما بعده مثل الفحص الأمني للموظفين المحتملين، والتوعية الأمنية، وبرامج التدريب والاستباقية .

خصوصية

يضمن مقدمو الخدمة إخفاء جميع البيانات الهامة (أرقام بطاقات الائتمان، على سبيل المثال) أو تشفيرها وأن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى البيانات بأكملها، علاوة على ذلك ، يجب حماية الهويات وبيانات الاعتماد الرقمية كما ينبغي حماية أي بيانات يجمعها المزود أو ينتجها عن نشاط العميل في السحابة .

اختبار الضعف والاختراق في السحابة

يعد مسح السحابة من الخارج والداخل باستخدام منتجات مجانية أو تجارية أمراً بالغ الأهمية لأنه بدون بيئة صلبة ، تعتبر خدمتك هدفًا سهلاً، يجب تقوية الخوادم الافتراضية تماماً مثل الخادم المادي ضد تسرب البيانات والبرامج الضارة ونقاط الضعف المستغلة "يمثل فقد البيانات أو تسربها ٢٤,٦٪ والبرامج الضارة المرتبطة بالسحابة ٣,٤٪ من التهديدات التي تسبب انقطاع السحابة"

يجب أن يتم تفويض اختبار المسح والاختراق من داخل أو خارج السحابة من قبل مزود السحابة، نظراً لأن السحابة عبارة عن بيئة مشتركة مع عملاء أو مستأجرين آخرين، فإن اتباع قواعد اختبار الاختراق للمشاركة خطوة بخطوة يعد مطلباً إلزامياً، يمكن أن يؤدي انتهاك سياسات الاستخدام المقبول إلى إنهاء الخدمة.

أمن البيانات

هناك العديد من التهديدات الأمنية المرتبطة بخدمات البيانات السحابية، وهذا يشمل التهديدات التقليدية والتهديدات غير التقليدية، تشمل التهديدات التقليدية ، التنصت على الشبكة، والغزو غير القانوني ، وهجمات رفض الخدمة ، ولكن أيضاً تهديدات محددة للحوسبة السحابية ، مثل هجمات القناة الجانبية ،ونقاط الضعف الافتراضية ، وإساءة استخدام الخدمات السحابية، متطلبات الأمان التالية تحد من التهديدات.

١. سرية البيانات

هي خاصية عدم إتاحة محتويات البيانات أو الكشف عنها للمستخدمين غير القانونيين، يتم تخزين البيانات الخارجية في سحابة وخارج سيطرة المالكين المباشرة، يمكن للمستخدمين المصرح لهم فقط الوصول إلى البيانات الحساسة بينما لا ينبغي للآخرين ، بما في ذلك مقدمي خدمات الحوسبة السحابية ، الحصول على أي معلومات من البيانات، وفي الوقت نفسه ، يتوقع مالكو البيانات الاستفادة الكاملة من خدمات البيانات السحابية ، على سبيل المثال ، البحث عن البيانات ، وحساب البيانات ، ومشاركة البيانات ، دون تسرب محتويات البيانات إلى مقدمي خدمات الحوسبة السحابية أو الخصوم الآخرين.

٢. التحكم في الوصول

تعني إمكانية التحكم في الوصول أن مالك البيانات يمكنه إجراء تقييد انتقائي للوصول إلى البيانات الخاصة به التي يتم الاستعانة بمصادر خارجية لها في السحابة. يمكن أن يصرح المالك للمستخدمين القانونيين بالوصول إلى البيانات، بينما لا يمكن للآخرين الوصول إليها بدون أذونات. علاوة على ذلك ، من المستحسن فرض تحكم دقيق في الوصول إلى البيانات الخارجية ، أي يجب منح مستخدمين مختلفين امتيازات وصول مختلفة فيما يتعلق بأجزاء البيانات المختلفة. يجب أن يتحكم المالك في ترخيص الوصول فقط في بيئات السحابة غير الموثوق بها.

٣. التكامل

تتطلب سلامة البيانات الحفاظ على دقة البيانات واكتمالها وضمانها. يتوقع مالك البيانات دائمًا أنه يمكن تخزين بياناته في السحابة بشكل صحيح وجدير بالثقة. وهذا يعني أنه لا ينبغي التلاعب بالبيانات بشكل غير قانوني أو تعديلها بشكل غير صحيح أو حذفها عمدًا أو تلفيقها بشكل ضار. إذا تسببت أي عمليات غير مرغوب فيها في إتلاف البيانات أو حذفها، فيجب أن يكون المالك قادرًا على اكتشاف التلف أو الخسارة. علاوة على ذلك، عند تلف جزء من بيانات الاستعانة بمصادر خارجية أو فقدها، لا يزال من الممكن استرجاعها بواسطة مستخدمي البيانات.

التشفير

بعض خوارزميات التشفير المتقدمة التي تم تطبيقها في الحوسبة السحابية تزيد من حماية الخصوصية، في ممارسة تسمى تمزيق التشفير، يمكن حذف المفاتيح ببساطة عندما لا يكون هناك استخدام للبيانات.

أ. التشفير المستند إلى السمات (ABE)

التشفير المستند إلى السمات هو نوع من تشفير المفتاح العام حيث يعتمد المفتاح السري للمستخدم والنص المشفر على سمات (مثل الدولة التي يعيش فيها أو نوع الاشتراك الذي لديه) في مثل هذا النظام، لا يمكن فك تشفير النص المشفر إلا إذا كانت مجموعة سمات مفتاح المستخدم تتطابق مع سمات النص المشفر.

- **سياسة النص المشفر ABE (CP-ABE)**

  فيCP-ABE ، يتحكم المشفر في إستراتيجية الوصول، يركز العمل البحثي الرئيسي لـ-CP ABEعلى تصميم بنية الوصول.

- **مفتاح السياسة ABE (KP-ABE)**

  فيKP-ABE ، تُستخدم مجموعات السمات لوصف النصوص المشفرة وترتبط المفاتيح الخاصة بالنهج المحدد الذي سيكون لدى المستخدمين.

ب. تشفير متجانس بالكامل (FHE)

يسمح التشفير المتجانس تماماً بإجراء عمليات حسابية على البيانات المشفرة ، كما يسمح بحساب مجموع ومنتج البيانات المشفرة دون فك التشفير.

ج. التشفير القابل للبحث (SE)

التشفير القابل للبحث هو نظام تشفير يوفر وظائف بحث آمنة عبر البيانات المشفر، **يمكن تصنيف مخططات SE إلى فئتين SE :** استناداً إلى تشفير المفتاح السري (أو المفتاح المتماثل) ، و SE المستند إلى تشفير المفتاح العام، من أجل تحسين كفاءة البحث ، ينشئ SE المتماثل المفتاح عموماً فهارس الكلمات الرئيسية للإجابة على استفسارات المستخدم، هذا له عيب واضح في توفير طرق وصول متعددة الوسائط لاسترداد البيانات غير المصرح به ، وتجاوز خوارزمية التشفير عن طريق إخضاع إطار العمل لمعلمات بديلة داخل بيئة السحابة المشتركة .

الالتزام

العديد من القوانين واللوائح المتعلقة بتخزين واستخدام البيانات، في الولايات المتحدة، تشمل هذه القوانين قوانين الخصوصية أو حماية البيانات ، ومعيار أمان بيانات صناعة بطاقات الدفع (PCI DSS) ، وقانون نقل التأمين الصحي والمساءلة (HIPAA) ، وقانون Sarbanes-Oxley ، وقانون إدارة أمن المعلومات الفيدرالي لعام ٢٠٠٢ (FISMA) ، وقانون حماية خصوصية الأطفال عبر الإنترنت لعام ١٩٩٨ ، من بين أمور أخرى. توجد معايير مماثلة في ولايات قضائية أخرى، مثل معيار أمان السحابة متعدد المستويات في سنغافورة .

قد يتم تطبيق قوانين مماثلة في ولايات قضائية مختلفة وقد تختلف بشكل ملحوظ عن تلك المطبقة في الولايات المتحدة، غالباً ما يحتاج مستخدمو الخدمة السحابية إلى أن يكونوا على دراية بالاختلافات القانونية والتنظيمية بين السلطات القضائية، على سبيل المثال ، قد تكون البيانات المخزنة بواسطة مزود خدمة سحابية موجودة في سنغافورة على سبيل المثال وعكسها في الولايات المتحدة.

تفرض العديد من هذه اللوائح ضوابط معينة (مثل ضوابط الوصول القوية ومسارات التدقيق) وتتطلب تقارير منتظمة، يجب على عملاء السحابة التأكد من أن موفري الخدمات السحابية لديهم يفيون بهذه المتطلبات بشكل مناسب حسب الاقتضاء، مما يمكنهم من الامتثال لالتزاماتهم لأنهم، إلى حد كبير، يظلون مسؤولين.

استمرارية الأعمال واستعادة البيانات

مقدمي سحابة يكون استمرارية الأعمال واستعادة البيانات يمكن الحفاظ على خطط موضوعة لضمان الخدمة في حالة وقوع كارثة أو حالة طارئة والتي سيتم استرداد أي فقدان البيانات، يمكن مشاركة هذه الخطط مع العملاء ومراجعتها من قبل العملاء ، بشكل مثالي مع ترتيبات الاستمرارية الخاصة بالعملاء، قد تكون تمارين الاستمرارية المشتركة مناسبة ، مثل محاكاة انقطاع كبير للإنترنت أو التيار الكهربائي على سبيل المثال .

سجل وتتبع المراجعة

بالإضافة إلى إنتاج السجلات ومسارات التدقيق، يعمل مقدمو الخدمات السحابية مع عملائهم للتأكد من أن هذه السجلات ومسارات التدقيق مؤمنة بشكل صحيح، ويتم الاحتفاظ بها طالما يطلبها العميل، ويمكن الوصول إليها لأغراض التحقيق الجنائي على سبيل المثال eDiscovery.

متطلبات الامتثال الفريدة

بالإضافة إلى المتطلبات التي يخضع لها العملاء، قد تخضع أيضاً مراكز البيانات التي يستخدمها موفرو السحابة لمتطلبات الامتثال، يمكن أن يؤدي استخدام موفر خدمة السحابة (CSP) إلى مخاوف أمنية إضافية حول اختصاص البيانات نظراً لأن بيانات العميل أو المستأجر قد لا تظل على نفس النظام ، أو في نفس مركز البيانات أو حتى داخل نفس السحابة الخاصة بالموفر.

أدخلت لائحة اللائحة العامة لحماية البيانات (GDPR) الخاصة بالاتحاد الأوروبي متطلبات امتثال جديدة لبيانات العملاء .

المسائل القانونية والتعاقدية

بصرف النظر عن مشكلات الأمان والامتثال المذكورة أعلاه ، سيتفاوض مقدمو الخدمات السحابية وعملائهم على الشروط المتعلقة بالمسؤولية (التي تنص على كيفية حل الحوادث التي تنطوي على فقدان البيانات أو التسوية ، على سبيل المثال (والملكية الفكرية ونهاية الخدمة (عندما تكون البيانات و يتم إرجاع التطبيقات في النهاية إلى العميل) بالإضافة إلى ذلك ، هناك اعتبارات للحصول على البيانات من السحابة التي قد تكون متورطة في التقاضي، تمت مناقشة هذه القضايا في اتفاقيات مستوى الخدمة (SLA).

السجلات العامة

قد تشمل القضايا القانونية أيضاً متطلبات حفظ السجلات في القطاع العام ، حيث يُطلب من العديد من الوكالات بموجب القانون الاحتفاظ بالسجلات الإلكترونية وإتاحتها بطريقة معينة، قد يتم تحديد ذلك من خلال التشريع ، أو قد يتطلب القانون من الوكالات الامتثال للقواعد والممارسات التي وضعتها وكالة حفظ السجلات، يجب على الوكالات العامة التي تستخدم الحوسبة السحابية والتخزين أن تأخذ هذه المخاوف في الاعتبار.

ج. دور مقدمي الخدمات السحابية في أمنها

ان أمان السحابة عبارة عن مسؤولية أمنية مشتركة بين مقدم الخدمة السحابية والعميل، يعد نموذج المسؤولية المشتركة لأمان السحابة بمثابة بنية أساسية لأمان السحابة وإدارة المخاطر لنقل تقسيم العمالة بين مقدم الخدمة السحابية والمشترك في الخدمة.

يحظى الفهم الواضح لنموذج المسؤولية الأمنية المشتركة لجميع أنواع الخدمات السحابية بقدر كبير من الأهمية بالنسبة لبرامج أمان السحابة، لسوء الحظ، يمكن القول أيضاً أن نموذج المسؤولية الأمنية المشتركة يعد أحد مفاهيم الأمان الأقل وضوحاً في السحابة، في الحقيقة، يفهم ٨ بالمائة فقط من المديرين التنفيذيين بصورة كاملة دورهم في تأمين SaaS مقارنة بمقدم الخدمات السحابية (CSP) وببساطة، يحدد نموذج المسؤولية الأمنية المشتركة نطاق مسؤولية مقدم الخدمة السحابية فيما يتعلق بالحفاظ على الأمان وتوافر الخدمة، ومسؤولية العميل فيما يتعلق بضمان الاستخدام الآمن للخدمة ومجال تشاركهما في واجب محدد.

من الضروري أن تفهم الشركات مسؤولياتها، يمكن أن يؤدي الإخفاق في حماية البيانات بصورة مناسبة إلى عواقب وخيمة ومكلفة، قد لا تتمكن العديد من المؤسسات التي ستتعرض لنتيجة الخرق من استيعاب التكلفة، حتى الشركات الكبيرة قد تلاحظ التأثير على شؤونها المالية، يتمثل الهدف من نموذج المسؤولية الأمنية المشتركة في توفير المرونة بالإضافة إلى الأمان المدمج الذي يسمح بالنشر السريع، لذلك، يتعين على المؤسسات فهم مسؤوليات أمان السحابة الخاصة بها - يُشار إليه بوجه عام باسم أمان السحابة مقابل الأمان في السحابة.

د. حقوق مستخدمي الحوسبة السحابية

خصت مؤسسة "Gartner" حقوق المستخدم والمسؤوليات الواقعة عليه في النقاط التالية:

- الحق في الحفاظ على الملكية واستخدامها والسيطرة على البيانات الخاصة
- الحق في الحصول على اتفاق مستوى الخدمة يتضمن الالتزامات التقنية والمادية والإجراءات العامة
- الحق في استقبال الإخطار وحرية الاختيار للتعديلات التي تؤثر في العمليات التجارية للمستخدم
- الحق في معرفة القيود التقنية أو متطلبات الخدمة مسبقا
- الحق في معرقة المتطلبات القانونية للدول التي يعمل فيها مقدم الخدمة مقدما
- الحق في معرقة إجراءات وسياسة عملية الأمن التي يتبناها مزود الخدمة

تدريبات الفصل الثاني

س١: اختار الإجابة الصحيحة لما يلي:

١) ..... هي توفير موارد تقنية المعلومات حسب الطلب عبر الانترنت مع تسعير التكلفة حسب الاستخدام؟

أ. الحوسبة السحابية

ب. المواقع

ج. البرامج

د. الوظائف

٢) تعد استطاعة المؤسسة اعتماد ونشر تطبيقات الحوسبة السحابية دون الحاجة لشراء الأجهزة أحد مميزات الحوسبة السحابية، وهي:

أ. الذكاء

ب. سهولة التنفيذ

ج. قابلية التوسع

د. البرمجة

٣) أي مما يلي ليس من مبادئ اقتصاديات السحابة الحديثة

أ. الحجم السليم

ب. تحسين الاستخدام باستمرار

ج. التعاون عبر الوظائف لتعزيز القرار حسب قيمة الأعمال

د. بقاء الأسعار ثابته

٤) من ضوابط أمان السحابة: ..... وتهدف إلى اكتشاف أي حوادث تحدث والتفاعل معها بشكل مناسب؟

أ. الضوابط الرادعة

ب. الضوابط الوقائية

ج. ضوابط المباحث

د. ضوابط التصحيحية

٥) من ضوابط أمان السحابة: ..... وتعمل على تقوية النظام ضد الحوادث بشكل عام عن طريق تقليل نقاط الضعف إن لم يكن القضاء عليها؟

أ. الضوابط الرادعة

ب. الضوابط الوقائية

ج. ضوابط المباحث

د. ضوابط التصحيحية

٦) من ضوابط أمان السحابة: ..... وتهدف إلى تقليل الهجمات على نظام السحابة؟

أ. الضوابط الرادعة

ب. الضوابط الوقائية

ج. ضوابط المباحث

د. ضوابط التصحيحية

٧) .....يعتبر هذا النوع من الخدمات الأكثر استخداما في الحوسبة السحابية، حيث انها توفر وصول مستأجرين متعددين من السحابة الى تطبيق معين؟

أ. الوظيفة كخدمة FaaS

ب. المنصة كخدمة PaaS

ج. البنية التحتية كخدمة IaaS

د. البرمجيات كخدمة SaaS

٨) هو عرض قائم على الاشتراك حيث يشترك المستخدمون في البرنامج بشكل شهري بدلا من شرائه؟

أ. البنية التحتية كخدمة IaaS

ب. الوظائف كخدمة FaaS

ج. البرمجيات كخدمة SaaS

د. المنصة كخدمة PaaS

٩) من ضوابط أمان السحابة: ..... وهي تقلل من عواقب أي حادث، عادة عن طريق الحد من الضرر؟

أ. الضوابط الرادعة

ب. الضوابط الوقائية

ج. ضوابط المباحث

د. ضوابط التصحيحية

١٠) .....من مميزاته توفير التوافق عبر الأجهزة؟

أ. الوظيفة كخدمة FaaS

ب. المنصة كخدمة PaaS

ج. البرمجيات كخدمة SaaS

د. البنية التحتية كخدمة IaaS

س٢: ضع علامة صح عند العبارة الصحيحة وعلامة خطأ أمام العبارة الخاطئة

١. تستغرق التطبيقات المستندة إلى السحابة وقتًا أقل لتحقيق الهدف المحدد ( )

٢. عند الانتقال إلى السحابة لا تحتاج إلى أجهزتك الخاصة لأن كل شيء متاح ومستضاف على الخادم ( )

٣. استخدام كلمات المرور الافتراضية لا يعد من التهديدات المصاحبة لإنترنت الأشياء ( )

٤. التطبيق هو الشخص المسؤول عن استئجار الخدمة من مزود الخدمات السحابية واستخدامها ( )

٥. لا تعد الإدارة من مكونات الحوسبة السحابية ( )

٦. تتكون بنية الحوسبة السحابية من جزئين، وهما الواجهة الأمامية والنهاية الخلفية ( )

٧. البنية التحتية تكون موجودة لدى مزودي الخدمات السحابية في أماكن آمنة ( )

٨. تعد الحماية أهم مكونات الحوسبة السحابية التي يركز عليها العميل ( )

س٣: صل العامود (أ) بما يناسبه من العامود (ب)

م	(أ)	الإجابة	(ب)
١	السحب العامة PUBLIC CLOUD		تقدم خدماتها لعملاء متعددين
٢	السحب الخاصة PRIVATE CLOUD		تجمع بين خصائص السحب العامة والخاصة
٣	السحب الهجينة HYBRID CLOUD		تعد النموذج الأحدث من الحوسبة السحابية
٤	سحب المجتمع COMMUNITY CLOUD		تعطي المنشأة فرصة المراقبة على السحابة

س٤: اذكر الفوائد الاقتصادية للحوسبة السحابية للشركات.

س٥: ماهي أهم مكونات الحوسبة السحابية وبنيتها التحتية.

حل تدريبات الفصل الثاني

حل السؤال الأول:

١- الحوسبة السحابية (أ)

٢- سهولة التنفيذ (ب)

٣- بقاء الأسعار ثابته (د)

٤- ضوابط المباحث (ج)

٥- الضوابط الوقائية (ب)

٦- الضوابط الرادعة (أ)

٧- البرمجيات كخدمة SaaS (د)

٨- البرمجيات كخدمة SaaS (ج)

٩- ضوابط التصحيحية (د)

١٠- البرمجيات كخدمة (ج)

حل السؤال الثاني:

١. صح

٢. صح

٣. خطأ

٤. خطأ

٥. خطأ

٦. صح

٧. صح

٨. صح

حل السؤال الثالث:

١. السحب العامة (١) تقدم خدماتها لعملاء متعددين

٢. السحب الهجينة (٣) جمع بين خصائص السحب العامة والخاصة

٣. سحب المجتمع (٤) تعد النموذج الأحدث من الحوسبة السحابية

٤. السحب الخاصة (٢) تعطي المنشأة فرصة المراقبة على السحابة

حل السؤال الرابع:

الفوائد الاقتصادية للحوسبة للشركات:

- تكلفة مخفضة
- قابلية التوسع
- النشر السريع للمشروع
- التخفيف من المخاطر مع زيادة الأمن
- بيئة عمل مرنة

حل السؤال الخامس:

- البنية التحتية للعميل
- التطبيق
- الخدمة
- سحابة بيئة التنفيذ
- التخزين
- البنية التحتية
- الإدارة
- الحماية
- الإنترنت

ثالثاً: أمن إنترنت الأشياء

في هذا الفصل سنتعرف على المواضيع التالية:

- مفهوم وأهمية أمن إنترنت الأشياء
- التهديدات المصاحبة لإنترنت الأشياء
- نظرة عامة على بروتوكولات وآليات الأمن في إنترنت الأشياء
- الأمان في بروتوكولات وتقنيات إنترنت الأشياء
- مشكلات الأمان وحلولها
- أدوات الأمن والاختراقIoT

مفهوم وأهمية أمن إنترنت الأشياء

الأمن السيبراني هو مزيج بين التقنيات والعمليات المخصصة لحماية الشبكات والأجهزة والبرامج والحماية من هجمات البيانات أو اختراق الوصول. يتم أيضا دمج نظام الأمن السيبراني مع أنظمة أمان الشبكات وأنظمة أمان الأجهزة. تتمتع أجهزة إنترنت الأشياء بمستوى محدود من الأمان باستخدام الأساليب التقليدية التي تحددها برامج مكافحة الفيروسات وجدار الحماية. والتي تتطلب مستوى معينا من المعرفة لتكوينها وتخصيصها لكل شبكة، مما يجعل من الصعب تعميمها.

تؤكد نقاط الضعف هذه على الحاجة الملحة إلى اتباع نهج شامل واستباقي لتأمين الأنظمة البيئية لإنترنت الأشياء، بما في ذلك المصادقة القوية والتشفير وصيانة البرامج الثابتة وأمن الواجهة وإدارة التصحيح وإدارة بيانات الاعتماد والحماية المادية وتعليم المستخدم والحفاظ على الخصوصية.

تعد معالجة هذه المشكلات أمرًا بالغ الأهمية في التخفيف من التهديدات المتطورة باستمرار التي تواجهها أجهزة إنترنت الأشياء. مع ظهور الذكاء الاصطناعي والفوائد التي يقدمها، أصبح عرضة للعديد من التحديات. تشمل التحديات الأمنية الحالية للذكاء الاصطناعي الهجمات العدائية، ومخاوف الخصوصية، والتحيز، ونقاط الضعف الأمنية النموذجية، ومشكلات الموثوقية، والفجوات في التفسير، وتسميم البيانات، وتحديات قابلية التوسع. وهناك حاجة إلى جهود متعددة التخصصات لتعزيز المتانة والشفافية والامتثال التنظيمي مع تخفيف المخاطر التي تهدد الخصوصية والعدالة والملكية الفكرية.

العقبات الحرجة التي تقف في طريق المحاولات المستقبلية لرؤية إنترنت الأشياء مقبولة بالكامل في المجتمع، هي العيوب الأمنية ونقاط الضعف. تتم إدارة عمليات إنترنت الأشياء اليومية بنجاح من خلال المخاوف الأمنية. في المقابل، لديهم هيكل مركزي ينتج عنه العديد من النقاط الضعيفة التي قد تتعرض للهجوم. يمكن الاستيلاء على أجهزة إنترنت الأشياء غير الآمنة واستخدامها في شبكات الروبوت، مما يؤدي إلى هجمات إلكترونية مثل DDoS والبريد العشوائي والتصيد الاحتيالي.

نظرا لوجود العديد من الأجهزة المتصلة، قد يكون من الصعب ضمان أمان جهاز إنترنت الأشياء. يجب على المستخدمين اتباع ممارسات الأمان الأساسية، مثل تغيير كلمات المرور الافتراضية وحظر الوصول عن بعد غير المصرح به. يجب على المصنعين والبائعين الاستثمار في تأمين مديري أدوات إنترنت الأشياء من خلال إخطار المستخدمين بشكل استباقي بالبرامج القديمة، وفرض إدارة قوية لكلمات المرور، وتعطيل الوصول عن بعد للوظائف غير الضرورية، وإنشاء تحكم صارم في الوصول إلى واجهة برمجة التطبيقات.

التهديدات المصاحبة لإنترنت الأشياء

إن عملية تبادل البيانات بين الأجهزة الذكية قد تؤثر على خصوصية الأفراد، وكذلك يمكن أن تؤثر على قضايا أخرى حساسة لها علاقة بالأمن والحماية من الناحية التقنية بشكل عام، وبأمن المستخدمين ومعلوماتهم الشخصية بشكل خاص، **ومن هذه القضايا:**

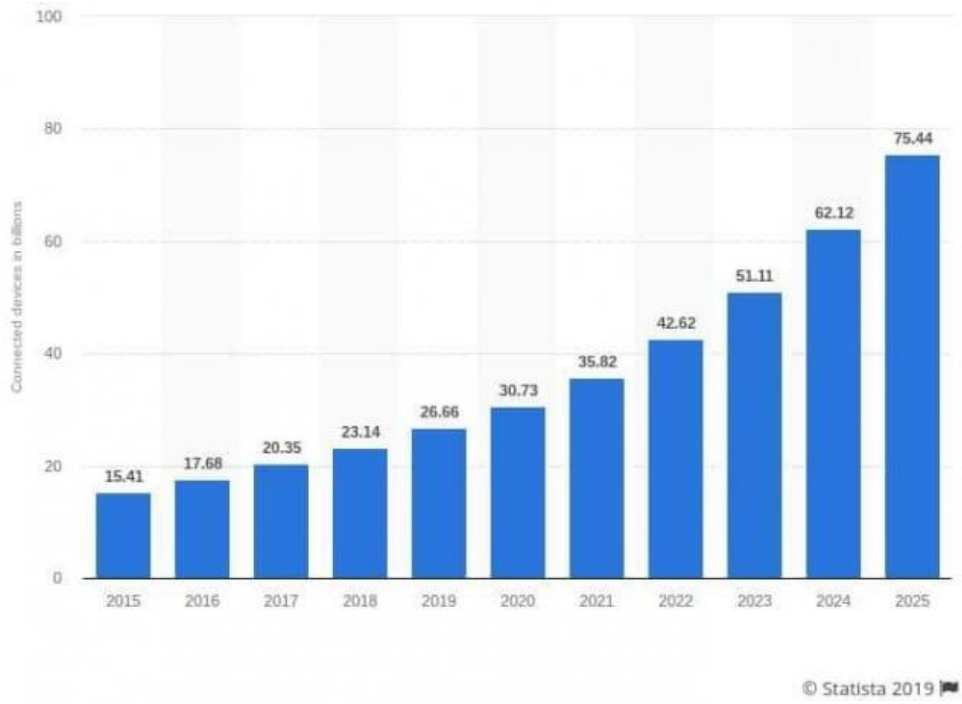
عدم مراقبة الأجهزة التي تحتوي على مستشعرات، بالشكل الصحيح، وكذلك عمليات التشويش المتعمَّدة؛ والتي يقوم بها بعض الأشخاص بهدف تعطيل أنظمة التواصل بين هذه الأجهزة الذكية بطريقة غير قانونية وبدوافع التخريب والعبث، وكذلك دراسة التهديدات التي تتعرض لها أنترنت الأشياء (IoT)وكذلك الآليات والتقنيات المتبعة لإحداث خلل والبحث عن الثغرات الموجودة في طبقات إنترنت الأشياء (IoT)، وكذلك سيتم دراسة البنية التحتية وسجلات الملفات في إنترنت الأشياء(IoT) .

غالباً ما نقوم بالتعامل مع أمن وحماية المعلومات على أنها شيء قائم وحده، فنحن لا نضعها بالحسبان خلال مرحلة التخطيط لبناء البنية التحتية للشبكات سواءً السلكية أو اللاسلكية، وانما نبدأ بالتفكير بها بعد الانتهاء من مرحلة التخطيط وفي العادة نقوم بوضع جدار ناري firewall خارجي لحماية جميع الشبكة الداخلية؛ سواء كان برنامج software مُحمّل على جهاز خادم، أو كقطعة منفصلة ملموسة hardware وهذه الطريقة تعطي أداء وكفاءة جيدة، ولكن في بعض الأحيان تعتبر نقطة ضعف في نظام الحماية، حيث أن جميع الأجهزة بأنواعها المختلفة داخل الشبكة الواحدة يجب أن تكون محمية بذاتها وذلك للحصول على نظام حماية يعمل بكفاءة كبيرة ودرجة عالية من الأمان، وبغير ذلك سيكون النظام عرضة للاختراق ومتوفر لأي هجمة خارجية.

هناك العديد من التهديدات الأمنية لإنترنت الأشياء التي تسود في أيامنا هذه الأجهزة المستخدمة في إنترنت الأشياء والتي تجعل عالم التكنولوجيا هذا أكثر عرضة للخطر منها:

١. عدم وجود تحديثات

يوجد حالياً حوالي ٢٣ مليار جهاز إنترنت الأشياء حول العالم بحلول عام ٢٠٢٠، سيرتفع هذا الرقم إلى ما يقرب من ٣٠ ملياراً، كما يقول تقرير Statista هذه الزيادة الهائلة في عدد الأجهزة المتصلة بإنترنت الأشياء لا تأتي دون أي عواقب. انظر إلى شكل ٩.



شكل ٩ قاعدة الأجهزة المتصلة بإنترنت الأشياء (IoT) المثبتة في جميع أنحاء العالم من ٢٠١٥ إلى ٢٠٢٥ (بالمليارات)

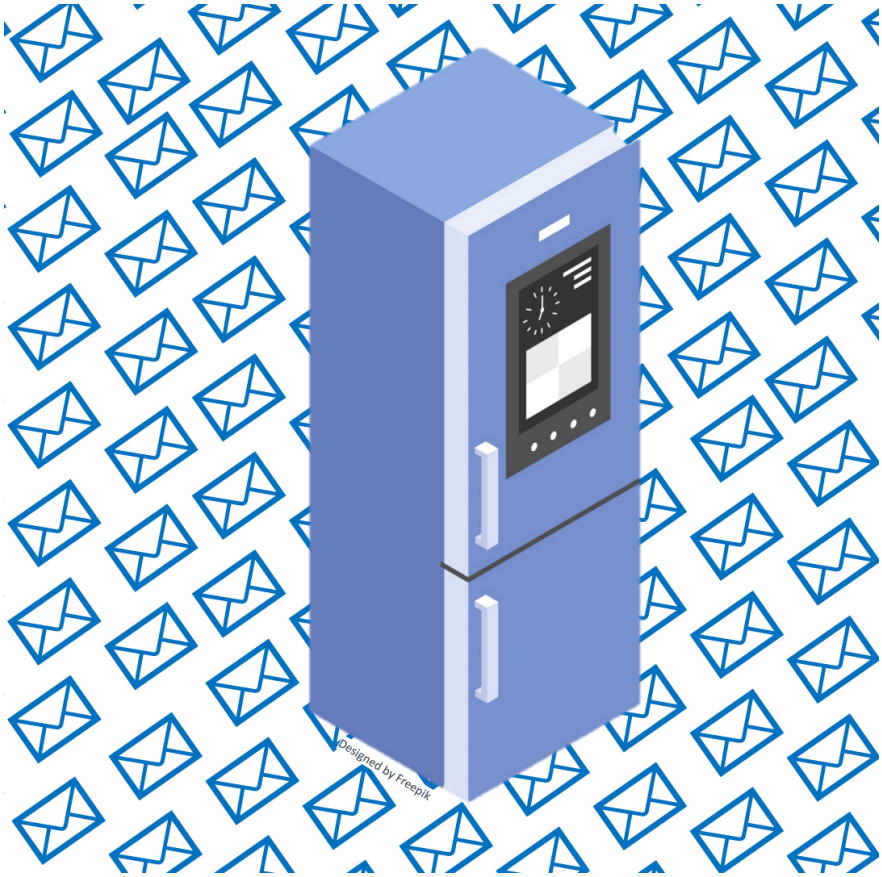
أكبر مشكلة مع جميع الشركات التي تنتج هذه الأجهزة هي أنها غير مبالية فيما يتعلق بالتعامل مع مشكلات الأمان والمخاطر المتعلقة بالأجهزة، لا تحصل معظم هذه الأجهزة المتصلة على تحديثات أمنية كافية، لا يتم تحديث البعض على الإطلاق.

الأجهزة التي كان يُعتقد في السابق أنها آمنة أصبحت عرضة للخطر تماماً وغير آمنة مع تطور التكنولوجيا، مما يجعلها عرضة لمجرمي الإنترنت والمتسللين.

يتنافس المصنعون مع بعضهم البعض ويطلقون الأجهزة كل يوم دون التفكير كثيراً في مخاطر ومشكلات الأمان. توفر معظم الشركات المصنعة تحديثات البرامج الثابتة عبر الهواء (OTA)، ولكن هذه التحديثات تتوقف بمجرد بدء العمل على أجهزتهم الجديدة ، مما يترك جيلهم الحالي عرضة للهجمات، فإذا فشلت الشركات في توفير تحديثات الأمان لأجهزتها بانتظام، فإنها تعرض قاعدة عملائها للهجمات السيبرانية المحتملة وخروقات البيانات.

٢. أجهزة إنترنت الأشياء تم اختراقها وترسل رسائل بريد إلكتروني عشوائية

لقد جلب لنا تطور التكنولوجيا عدداً كبيراً من الأجهزة الذكية التي تشمل، على سبيل المثال لا الحصر، الأجهزة الذكية، ونظام المنزل الذكي، وما إلى ذلك، تستخدم هذه الأجهزة قوة حوسبة مماثلة للأجهزة الأخرى المتصلة بإنترنت الأشياء ويمكن استخدامها في أنشطة مختلفة، انظر شكل ١٠.



شكل ١٠ أجهزة إنترنت الأشياء تم اختراقها وترسل رسائل بريد إلكتروني عشوائية

يمكن تحويل الجهاز المخترق إلى خادم بريد إلكتروني، وفقا لـتقرير من شركة أمان الإنترنت Proofpoint، تم استخدام ثلاجة ذكية لإرسال آلاف رسائل البريد الإلكتروني العشوائية دون أن يكون لدى أصحابها أي دليل، يمكن تحويل معظم هذه الأجهزة الذكية إلى خوادم بريد إلكتروني بغرض إرسال بريد إلكتروني عشوائي.

٣. أجهزة إنترنت الأشياء التي تم تجنيدها في شبكات Botnets

على غرار الأجهزة التي يتم اختراقها وتحويلها إلى خوادم بريد إلكتروني للرسائل العشوائية الجماعية يمكن أيضاً استخدام أجهزة إنترنت الأشياء الذكية كشبكات روبوت لإجراء هجمات DDoS رفض الخدمة الموزع.

في الماضي، استخدم المتسللون أجهزة مراقبة الأطفال وكاميرات الويب وصناديق البث والطابعات وحتى الساعات الذكية لتنفيذ هجمات DDoS واسعة النطاق، يحتاج المصنعون إلى فهم المخاطر المرتبطة بالأجهزة المتصلة بإنترنت الأشياء واتخاذ جميع الخطوات اللازمة لتأمين أجهزتهم .

٤. اتصالات غير آمنة

لا تقوم العديد من أجهزة إنترنت الأشياء بتشفير الرسائل عند إرسالها عبر الشبكة، يعد هذا أحد أكبر التحديات الأمنية لإنترنت الأشياء الموجودة هناك، تحتاج الشركات إلى التأكد من أن الاتصال بين الأجهزة والخدمات السحابية آمن ومشفّر.

أفضل ممارسة لضمان الاتصال الآمن هي استخدام تشفير النقل واستخدام معايير مثل بروتوكول الـ Transport Layer Security (TLS)يساعد عزل الأجهزة من خلال استخدام شبكات مختلفة أيضاً في إنشاء اتصال آمن وخاص، مما يحافظ على البيانات المرسلة آمنة وسرية. بدأت معظم التطبيقات والخدمات في تشفير رسائلها من أجل الحفاظ على أمان معلومات المستخدمين .

٥. استخدام كلمات المرور الافتراضية

تشحن معظم الشركات الأجهزة بكلمات مرور افتراضية ولا تخبر عملائها حتى بتغييرها، يعد هذا أحد أكبر التهديدات الأمنية لإنترنت الأشياء حيث إن كلمات المرور الافتراضية هي معرفة شائعة، ويمكن للمجرمين بسهولة وضع أيديهم على كلمات المرور باستخدام التأثير الغاشم. انظر شكل ١١.

شكل ١١ مثال على كلمات مرور افتراضية وكلمات مرور قوية

تترك بيانات الاعتماد الضعيفة جميع الأجهزة المتصلة بإنترنت الأشياء تقريباً عرضة للتأثير الغاشم واختراق كلمات المرور، تضع الشركات التي تستخدم بيانات اعتماد غير آمنة على أجهزة إنترنت الأشياء الخاصة بها كل من عملائها وعملاء الأعمال التجارية عرضة لخطر التعرض لهجمات مباشرة والإصابة من خلال استخدام محاولات القوة الغاشمة.

٦. الوصول عن بعد

الوثائق الصادرة عن ويكيليكس ذكر أن وكالة المخابرات المركزية الأمريكية (CIA) كانت تخترق أجهزة إنترنت الأشياء وتقوم بتشغيل الكاميرا / الميكروفونات دون علم أصحابها، حسناً إن احتمال دخول المهاجمين إلى أجهزتك وتسجيل أصحابها دون علمهم أمر مرعب، ولم تستخدمه سوى الحكومة نفسها.

أشارت وثائقهم إلى نقاط ضعف هائلة في أحدث البرامج مثل Android و iOS، مما يعني أن المجرمين يمكنهم أيضاً الاستفادة من نقاط الضعف هذه وتنفيذ أعمال شنيعة الجرائم .

٧. تسريبات المعلومات الشخصية

يمكن لمجرمي الإنترنت ذوي الخبرة إحداث أضرار جسيمة حتى من خلال اكتشاف عناوين بروتوكول الإنترنت (IP) من خلال أجهزة إنترنت الأشياء غير الآمنة، يمكن استخدام هذه العناوين لتحديد موقع المستخدم وعنوان سكنه الفعلي. انظر شكل ١٢.

شكل ١٢ رسم لتسريب المعلومات الشخصية

هذا هو السبب في أن العديد من خبراء أمن الإنترنت يوصون بتأمين اتصال إنترنت الأشياء الخاص بك من خلال شبكة افتراضية خاصة (VPN) تثبيت VPN على جهاز التوجيه الخاص بك سوف يقوم بتشفير كل حركة المرور من خلال مزود خدمة الإنترنت، يمكن أن تحافظ VPN على خصوصية عنوان بروتوكول الإنترنت الخاص بك وتأمين شبكتك المنزلية بالكامل.

٨. غزوات المنزل

يجب أن يكون هذا أحد أكثر تهديدات أمان إنترنت الأشياء رعباً لأنه يسد الفجوة بين العالم الرقمي والعالم المادي، كما ذكرنا سابقاً، يمكن لجهاز إنترنت الأشياء غير الآمن تسريب عنوان IP الخاص بك والذي يمكن استخدامه لتحديد عنوان إقامتك.

يمكن للقراصنة بيع هذه المعلومات إلى مواقع الويب السرية حيث تعمل الجماعات الإجرامية، أيضاً إذا كنت تستخدم أنظمة أمان منزلية ذكية متصلة بإنترنت الأشياء، فيمكن اختراقها أيضاً لهذا السبب تحتاج إلى تأمين أجهزتك المتصلة من خلال أمان إنترنت الأشياء واستخدام الشبكات الافتراضية الخاصة.

٩. الوصول إلى السيارة عن بعد

ليس مخيفاً مثل اقتحام شخص ما لمنزلك، ولكنه لايزال أمرًا مرعباً للغاية، اليوم عندما نتوق جميعاً إلى سيارات القيادة الذكية، هناك أيضاً مستوى عالٍ من المخاطر المرتبطة بهذه السيارات المتصلة بإنترنت الأشياء .

قد يتمكن المتسللون المهرة من الوصول إلى سيارتك الذكية واختطافها من خلال الوصول عن بُعد، هذه فكرة مخيفة لأن شخصاً آخر يسيطر على سيارتك سيجعلك عرضة لعدد كبير من الجرائم، لحسن الحظ، يولي مصنعو السيارات الذكية اهتماماً وثيقاً بتهديدات "أمان إنترنت الأشياء" ويعملون بجد لتأمين أجهزتهم من أي نوع من الاختراق.

١٠. برامج الفدية

تم استخدام برامج الفدية الضارة على أجهزة الحاسوب وشبكات الشركات لفترة طويلة، يقوم المجرمون بتشفير نظامك بالكامل ويهددون بإزالة جميع بياناتك ما لم تدفع "الفدية"، وبالتالي الاسم. انظر إلى شكل ١٣.

شكل ١٣ رسم لبرنامج الفدية

إنها مسألة وقت فقط قبل أن يبدأ المهاجمون في إغلاق الأجهزة الذكية المختلفة والمطالبة بفدية لفتحها، اكتشف الباحثون بالفعل طريقة تثبيت برامج الفدية على منظمات الحرارة الذكية وهو أمر مقلق للغاية حيث يمكن للمجرمين رفع درجة الحرارة أو خفضها حتى يتم دفع الفدية، الأمر الأكثر ترويعاً هو سيطرة المهاجمين على أنظمة الأمن المنزلية أو الأجهزة الذكية، كم ستدفع لفتح باب المرآب المتصل بإنترنت الأشياء؟

١١. سرقة البيانات

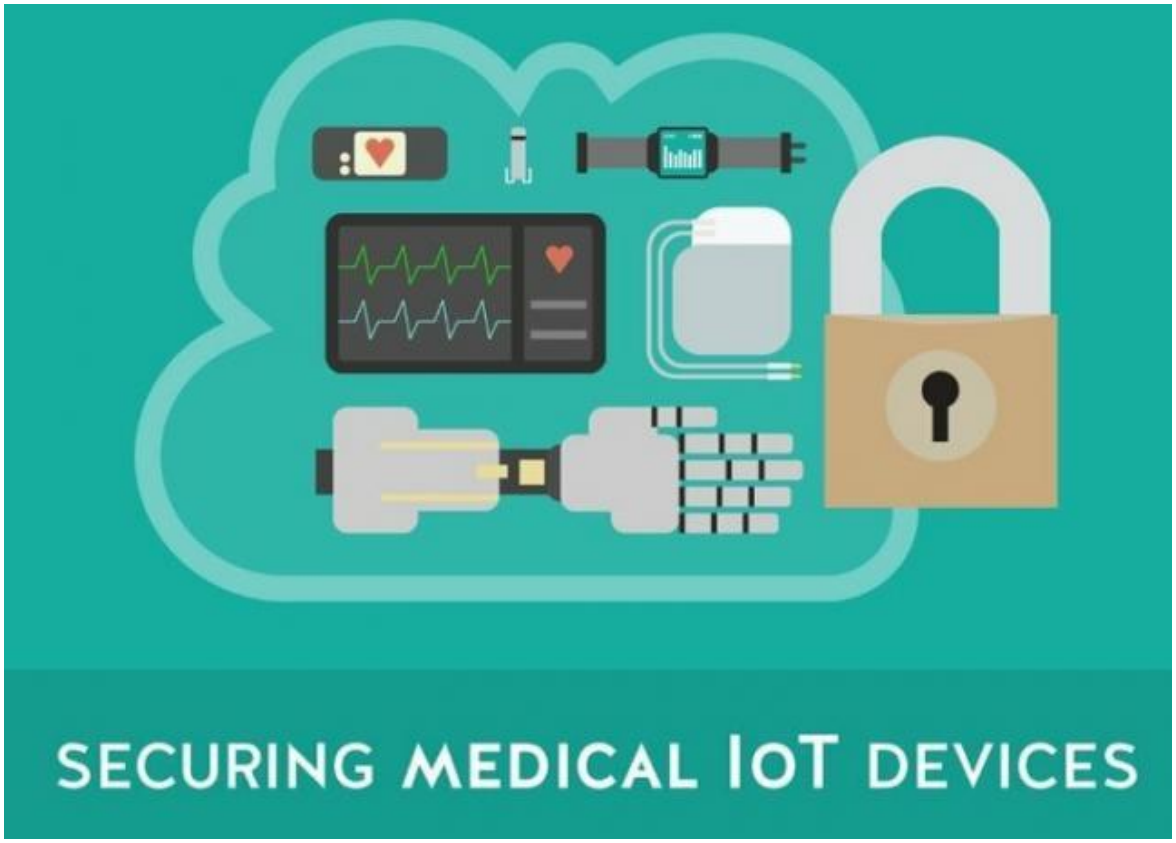
يتابع المتسللون دائماً البيانات التي تتضمن، على سبيل المثال لا الحصر، أسماء العملاء وعناوين العملاء وأرقام بطاقات الائتمان والتفاصيل المالية والمزيد، حتى عندما يكون لدى الشركة أماناً مشدداً لإنترنت الأشياء، هناك موجهات هجوم مختلفة يمكن لمجرمي الإنترنت استغلالها. انظر شكل ١٤.

شكل ١٤ رسم لسرقة البيانات

على سبيل المثال، يكفي جهاز إنترنت الأشياء الضعيف لتعطيل شبكة بأكملها والوصول إلى المعلومات الحساسة، إذا كان هذا الجهاز متصلاً بشبكة الشركة، فيمكن للقراصنة الوصول إلى الشبكة واستخراج جميع البيانات القيمة، ثم يسيء المتسللون استخدام هذه البيانات، أو يبيعونها لمجرمين آخرين مقابل مبلغ كبير.

١٢. المساومة على الأجهزة الطبية

قد يبدو هذا وكأنه فليم سينمائي، لكن هذا لا يجعله أقل تهديداً لأمن إنترنت الأشياء، أظهرت إحدى حلقات مسلسل ما هجوماً استهدف فيه المجرمون جهازاً طبياً مزروعاً لاغتيال شخص. انظر شكل ١٥.



شكل ١٥ المساومة على الأجهزة الطبية

الآن، لم يتم تنفيذ هذا النوع من الهجوم في الحياة الواقعية، لكنه لا يزال يمثل تهديداً، يكفي أن السابق نائب رئيس الولايات المتحدة ديك تشيني تمت إزالة الميزات اللاسلكية لجهاز إزالة رجفان القلب المزروع لتجنب مثل هذه السيناريوهات، نظراً لارتباط المزيد والمزيد من الأجهزة الطبية بإنترنت الأشياء، تظل هذه الأنواع من الهجمات محتملة.

١٣. المزيد من الأجهزة والمزيد من التهديدات

هذا هو الجانب السلبي لزيادة هائلة في أجهزة إنترنت الأشياء، زاد عدد الأجهزة الموجودة خلف جدار الحماية لديك بشكل ملحوظ في العقد الماضي، مرة أخرى في اليوم، كان علينا فقط القلق بشأن تأمين أجهزة الحاسب الشخصية الخاصة بنا من الهجمات الخارجية .

الآن، في هذا العصر، لدينا عدد كبير من أجهزة إنترنت الأشياء المختلفة لنقلق بشأنها، بدءاً من هواتفنا الذكية اليومية إلى الأجهزة المنزلية الذكية وغير ذلك الكثير، نظراً لوجود العديد من الأجهزة التي يمكن اختراقها، فسيكون المتسللون دائماً يبحثون عن أضعف رابط وخرقه .

١٤. هجمات إنترنت الأشياء الصغيرة

نتعرف دائماً على هجمات إنترنت الأشياء واسعة النطاق، سمعنا عن الروبوتات Mirai منذ عامين / قبل Mirai؛ كان هناك ريبر الذي كان أخطر بكثير من ميراي، على الرغم من أن الهجمات واسعة النطاق تسبب المزيد من الضرر ، إلا أننا يجب أن نخشى أيضاً الهجمات الصغيرة التي غالباً ما لا يتم اكتشافها. غالباً ما تتجنب الهجمات الصغيرة النطاق الكشف وتتسلل عبر الثغرات، سيحاول المتسللون استخدام هذه الهجمات الصغيرة لتنفيذ خططهم بدلاً من السعي وراء الأسلحة الكبيرة.

١٥. الأتمتة والذكاء الاصطناعي

يتم استخدام الأدوات بالفعل في العالم، هناك أدوات تساعد في تصنيع السيارات بينما يقوم الآخرون بغربلة كمية كبيرة من البيانات، ومع ذلك هناك جانب سلبي لاستخدام الأتمتة لأنه لا يتطلب سوى خطأ واحد في الشفرة أو خطأ خوارزمية لإسقاط الذكاء الاصطناعي بالكامل، الشبكة ومعها البنية التحتية بأكملها المتابعة. انظر شكل 16.

شكل 16الأتمتة والذكاء الاصطناعي

والأتمتة هي مجرد كود، إذا تمكن شخص ما من الوصول إلى هذا الرمز، فيمكنه التحكم في الأتمتة وتنفيذ ما يريد، لذلك علينا التأكد من أن أدواتنا تبقى آمنة ضد مثل هذه الهجمات والتهديدات.

١٦. العامل البشري

حسناً، إنه ليس تهديداً مباشراً، ولكن هناك حاجة للقلق بشأن العدد المتزايد من الأجهزة، نظراً لأنه مع كل جهاز، يزداد أيضاً عدد البشر الذين يتفاعلون مع إنترنت الأشياء، لا يهتم الجميع بالأمن السيبراني؛ البعض لا يعرف حتى أي شيء عن الهجمات الرقمية أو يعتبرها خرافة.

غالباً ما يكون لدى هؤلاء الأشخاص أدنى معايير الأمان عندما يتعلق الأمر بتأمين أجهزة إنترنت الأشياء الخاصة بهم. يمكن لهؤلاء الأفراد وأجهزتهم غير المؤمنة أن تتسبب في هلاك مؤسسة أو شبكة شركة إذا اتصلوا بها .

١٧. نقص المعرفة

هذا أيضاً تهديد آخر يمكن حله بسهولة من خلال المشاركة الصحيحة للمعرفة، إما أن الناس لا يعرفون الكثير عن إنترنت الأشياء أو لا يهتمون، غالباً ما يكون نقص المعرفة سبباً في حدوث أضرار جسيمة لشبكة الشركة أو الشبكة الشخصية.

يجب إعطاء الأولوية لتوفير جميع المعارف الأساسية المتعلقة بإنترنت الأشياء والأجهزة المتصلة والتهديدات لكل فرد، قد يكون الحصول على معرفة أساسية حول تأثير إنترنت الأشياء وتهديداته الأمنية هو الفرق بين وجود شبكة آمنة وخرق البيانات .

١٨. قلة الوقت / المال

لن يستثمر معظم الأشخاص أو المنظمات في بنية تحتية آمنة لإنترنت الأشياء لأنهم يجدونها تستغرق وقتاً طويلاً أو باهظة الثمن، هذا يجب أن يتغير خلاف ذلك، ستواجه الشركات خسائر مالية فادحة من خلال الهجوم.

البيانات هي أثمن الأصول التي يمكن أن تمتلكها أي شركة، خرق البيانات يعني خسارة ملايين الدولارات الاستثمار في أ إعداد آمن لإنترنت الأشياء لن يكون مكلفاً مثل الاختراق الهائل للبيانات .

١٩. آلة التصيد

سيصبح التصيد الآلي للاحتيال مصدر قلق كبير في السنوات القادمة سيتسلل المتسللون إلى أجهزة وشبكات إنترنت الأشياء لإرسال إشارات وهمية من شأنها أن تجعل أصحابها يتخذون إجراءات قد تضر بالشبكة التشغيلية.

يمكن للمهاجمين، على سبيل المثال، أن يكون لديهم تقرير عن مصنع تصنيع يبلغ نصف طاقته (بينما هو العمل بنسبة ١٠٠ ٪) وسيحاول مشغل المحطة زيادة الحمل الذي يمكن أن يكون مدمراً لـ النباتي .

٢٠. بروتوكولات المصادقة رديئة

مع إغراق السوق بالعديد من الأجهزة المتصلة بإنترنت الأشياء، تغاضت الشركات المصنعة عن حقيقة أن كل جهاز يحتاج إلى بروتوكول مصادقة مناسب وقوي، غالباً ما تؤدي آليات الترخيص الضعيفة هذه إلى تزويد المستخدمين بإمكانية وصول أعلى من المفترض أن يحصلوا عليها.

تفتقر معظم الأجهزة إلى تعقيد كلمة المرور، وبيانات الاعتماد الافتراضية الضعيفة، ونقص التشفير، وعدم وجود مصادقة ثنائية، واستعادة كلمة المرور غير الآمنة، يمكن أن تؤدي هذه الثغرات الأمنية بسهولة إلى وصول المتسللين بسهولة إلى الأجهزة والشبكات.

٢١. مخاوف الخصوصية

تجمع معظم الأجهزة البيانات من جميع الأنواع، والتي تتضمن معلومات حساسة، تثار مخاوف الخصوصية عندما تبدأ الأجهزة في جمع المعلومات الشخصية دون وجود أي طرق حماية مناسبة لتلك البيانات .

في الوقت الحاضر، تتطلب جميع تطبيقات الهواتف الذكية تقريباً نوعاً من الأذونات وجمع البيانات على كل من iOS وAndroid تحتاج إلى مراجعة هذه الأذونات ومعرفة نوع البيانات التي يتم جمعها بواسطة هذه التطبيقات، إذا كانت البيانات التي تم جمعها ذات طبيعة شخصية وحساسة، فمن الأفضل التخلص من التطبيق بدلاً من المخاطرة ببياناتك الشخصية.

٢٢. الأمن المادي ضعيف

تحدثنا عن الأمن الرقمي حتى الآن، ولكن هذا ليس التهديد الوحيد لجهاز إنترنت الأشياء، إذا كان الأمن المادي ضعيفاً، فيمكن للقراصنة الوصول بسهولة إلى الأجهزة دون الحاجة إلى القيام بالكثير من العمل.

تتمثل نقاط الضعف المادية عندما يتمكن المتسلل من تفكيك الجهاز بسهولة والوصول إلى مساحة التخزين الخاصة به، حتى وجود منافذ USB مكشوفة أو أنواع أخرى من المنافذ يمكن أن يؤدي إلى وصول المتسللين إلى وسيط تخزين الجهاز وتعريض أي بيانات على الجهاز للخطر .

٢٣. RFID القشط

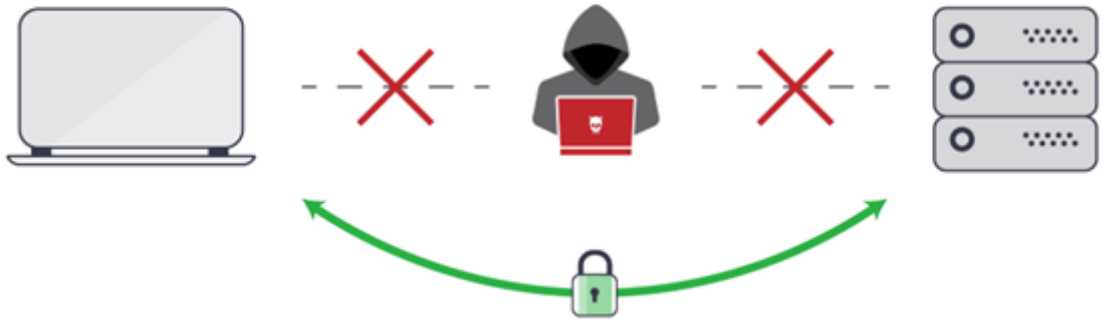
هذا هو نوع القشط حيث يعترض المتسللون المعلومات والبيانات اللاسلكية من شرائح RFID المستخدمة في بطاقات الخصم وبطاقات الائتمان وبطاقات الهوية / جوازات السفر والمستندات الأخرى .

شكل ١٧ رسم لهجوم RFID القشط

الغرض من التمويه على هذه البيانات هو سرقة المعلومات الشخصية المستخدمة لسرقة الهوية المتقدمة، يستخدم المتسللون الأجهزة التي تدعم NFC والتي تسجل جميع البيانات غير المشفرة من شرائح RFIDثم تبث عبر الإشارات اللاسلكية.

٢٤. هجمات رجل في الوسط

هذا نوع من الهجوم حيث يعترض المتسللون الاتصال بين طرفين من خلال جهاز إنترنت الأشياء غير الآمن أو ملف الضعف في الشبكة، ثم يغيرون الرسائل بينما يعتقد كلا الطرفين أنهما يتواصلان مع كل منهما آخر، يمكن أن تكون هذه الهجمات مدمرة للأطراف المعنية لأن جميع معلوماتهم الحساسة معرضة للخطر أثناء الاتصال.



شكل ١٨ رسم لهجوم الرجل في المنتصف

٢٥. مخططات بالوعة

يمكن للمتسلل جذب كل حركة المرور بسهولة من عقدة شبكة الاستشعار اللاسلكية (WSN) لبناء حفرة، هذا النوع من الهجوم يخلق حفرة مجازية تهدد سرية البيانات وترفض أيضاً أي خدمة للشبكة، يتم ذلك عن طريق إسقاط جميع الحزم بدلاً من إرسالها إلى وجهتها .

نظرة عامة على بروتوكولات وآليات الأمن في إنترنت الأشياء

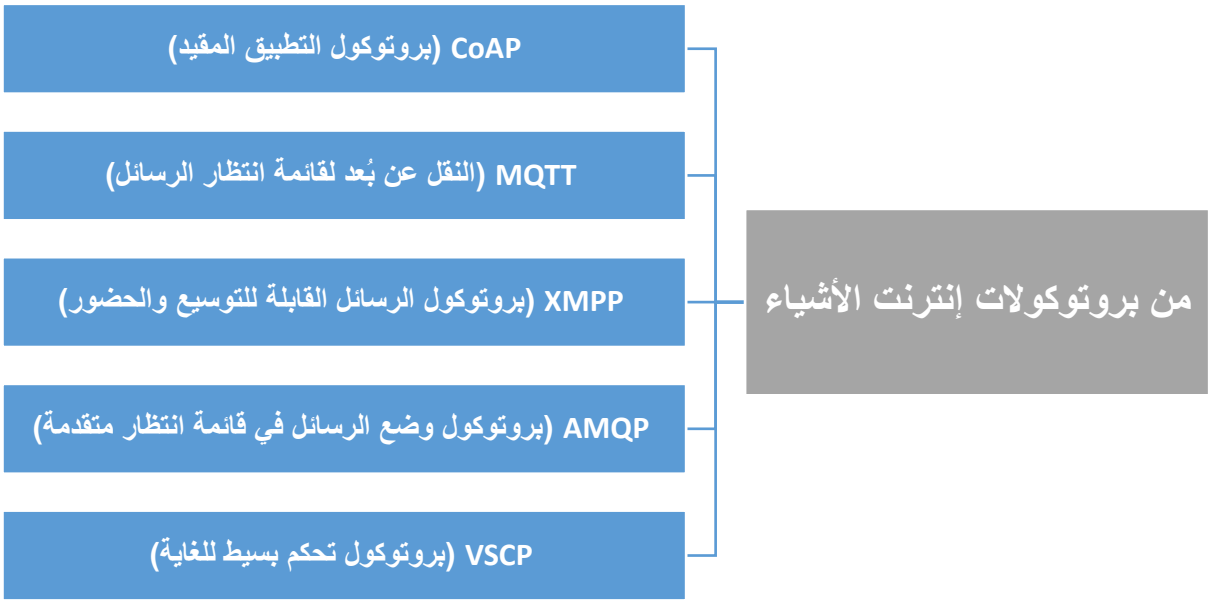
توسعت إنترنت الأشياء (IoT) من جهاز واحد مقيد إلى مجموعة كاملة من أنظمة السحابة، وكلها متصلة عبر سلسلة من البروتوكولات التي تسمح للأجهزة والخوادم بالتواصل مع بعضها البعض، دعونا نلقي نظرة على بعض بروتوكولات إنترنت الأشياء.

يُعرّف الاتحاد الدولي للاتصالات إنترنت الأشياء بأنه "البنية التحتية العالمية لمجتمع المعلومات الذي يدرك الخدمات المتقدمة من خلال ربط الأشياء (المادية والافتراضية) القائمة على المعلومات القائمة والمتطورة من المعلومات والاتصالات المتطورة" .

يحتوي مصطلح "إنترنت الأشياء" على كلمتين - الإنترنت والأشياء يشير مصطلح "إنترنت الأشياء" إلى العديد من أجهزة إنترنت الأشياء ذات الهويات الفريدة ، والتي لها وظائف أداء الاستشعار عن بُعد والبدء والمراقبة في الوقت الحقيقي لأنواع معينة من البيانات، يمكن لأجهزة IoT أيضاً تبادل البيانات بشكل مباشر أو غير مباشر في الوقت الفعلي مع الأجهزة والتطبيقات المتصلة الأخرى ، أو جمع البيانات من الأجهزة الأخرى ومعالجة البيانات وإرسالها إلى خوادم مختلفة، يعرف مصطلح آخر "إنترنت" بأنه شبكة اتصال عالمية تربط تريليونات من أجهزة الكمبيوتر حول العالم لتحقيق مشاركة المعلومات.

بروتوكول إنترنت الأشياء

قام IEEE معهد مهندسي الكهرباء والإلكترونيات وETSI المعهد الأوروبي لمعايير الاتصالات بتعريف بعض أهم البروتوكولات لإنترنت الأشياء، وهي موضحة في شكل ١٩



شكل ١٩ من بروتوكولات إنترنت الأشياء

أ. CoAP بروتوكول التطبيق المقيد

CoAP (Constrained Application Protocol) (بروتوكول التطبيق المقيد) هو بروتوكول طبقة تطبيق مصمم خصيصًا لبيئات إنترنت الأشياء. وتتمثل ميزتها الرئيسية في انخفاض التأثير الحسابي والطاقة على أجهزة إنترنت الأشياء، مما يجعلها مناسبة للغاية للبيئات المقيدة. تسمح بنية CoAP بالتحويل السهل إلى رسائل HTTP، مما يسهل التكامل مع الأنظمة القائمة على HTTP. بالمقارنة مع HTTP، فإن CoAP يقلل بشكل كبير من حجم الحزمة ومتطلبات الطاقة.
تتضمن تطبيقات CoAP ما يلي: CoAPthon (Python)، وCalifornium (Java)، وFreeCoAP (C).
يدعم CoAP نوعين فقط من الرسائل — الطلب والاستجابة — ويعمل بشكل غير متزامن عبر UDP، مما يقلل من المتطلبات الحسابية والطاقة. ومع ذلك، يفتقر UDP إلى معايير جودة الخدمة quality of service (QoS) الخاصة بـ TCP، لذا يتضمن CoAP آلية موثوقية بسيطة حيث يتم إعادة إرسال الحزم التي تم وضع علامة "ليتم تأكيدها" في حالة عدم تلقي تأكيد خلال فترة زمنية محددة.

يمكن لعقد CoAP تخزين الاستجابات مؤقتًا لتقليل وقت الاستجابة وعرض النطاق الترددي للشبكة للطلبات المماثلة المستقبلية. على عكس HTTP، تعتمد إمكانية التخزين المؤقت لـ CoAP على رمز الاستجابة بدلاً من طريقة الطلب.
للأمان، يستخدم CoAP بروتوكول DTLS عبر UDP لضمان السرية والنزاهة والمصادقة وعدم التنصل، على الرغم من أن هذا يضيف الحمل الحسابي. الجهود جارية لتقليل حجم رأس DTLS وخطوات المصافحة لجعلها أكثر ملاءمة للأجهزة المقيدة.

يحدد CoAP أربعة أوضاع أمان:

١- NoSec: لا توجد آلية أمنية.

٢- PreSharedKey: يستخدم مفاتيح محددة مسبقًا، ومناسب للأجهزة غير القادرة على التعامل مع تشفير المفتاح العام.

٣- RawPublicKey: يستخدم تشفير المفتاح العام، مع الأجهزة التي تم تكوينها باستخدام أزواج مفاتيح غير متماثلة.

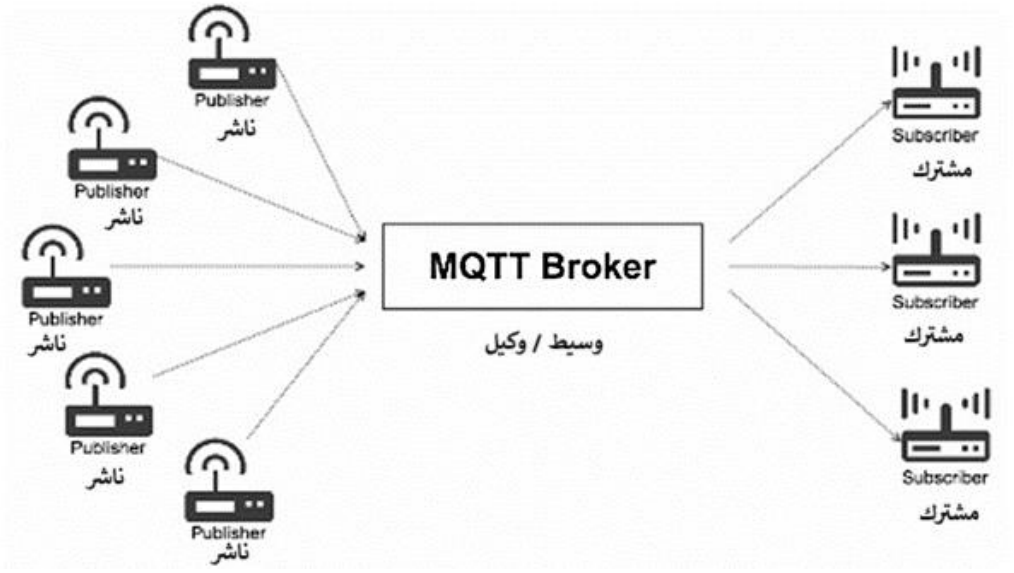
٤- الشهادات: يستخدم شهادات .X٥٠٩ للمصادقة والتواصل الآمن.

يمكن تشغيل بروتوكول LwM2M (Lightweight Machine to Machine) (آلة خفيفة الوزن إلى آلة) فوق بروتوكول CoAP، مما يوفر تقنية تطبيق عالية المستوى. يحدد M٢LwM بنية خادم العميل حيث يقوم عميل M٢LwM بالتسجيل في خادم M٢LwM. كما أنه يوفر واجهات برمجة تطبيقات الأمان للتمهيد والتسجيل والوصول إلى البيانات والأحداث.

ب. بروتوكول MQTT النقل عن بُعد لقائمة انتظار الرسائل

MQTT (Message Queue Telemetry Transport) (نقل القياس عن بعد لقائمة انتظار الرسائل) هو بروتوكول على مستوى التطبيق يعتمد على TCP، تم تقديمه في عام ١٩٩٩، وهو مصمم للتأثير المنخفض على الطاقة الحسابية وحالات النطاق الترددي المحدود.

تعمل MQTT على نظام النشر/الاشتراك، حيث تربط عقد عملاء متعددة (الناشرين والمشتركين) من خلال وسيط. يرسل الناشرون معلومات حول موضوعات محددة إلى الوسيط، ويتلقى المشتركون تحديثات من الوسيط حول هذه المواضيع. انظر شكل ٢٠. بالنسبة للشبكات الكبيرة، يمكن للوسطاء الموزعين موازنة الحمل، وتشكيل طبقة ضبابية لإدارة البيانات. إذا يتكون بروتوكول MQTTمن ثلاث مكونات رئيسية: المشتركون والناشرون والوسطاء (الوكلاء)، يقوم الناشر بإنشاء البيانات وإرسال المعلومات إلى المشترك عبر الوكيل، يضمن الوسيط الأمان من خلال التحقق من تفويض الناشرين والمشتركين. يمكن للأجهزة أن تعمل كناشرين ومشتركين، وتعمل بشكل غير متزامن دون اتصال مباشر.



شكل ٢٠ مخطط MQTT

تتضمن تطبيقات MQTT Mosquitto، وGridServer، وMqttools، وMoquette، وKMQTT، مع دعم بعضها لأدوار العميل والوسيط.

تضمن جودة خدمة (QoS) MQTT موثوقية الاتصال بثلاثة مستويات:

أ. جودة الخدمة صفر: لا توجد ضمانات للتسليم؛ يتم إرسال الرسائل مرة واحدة.

ب. جودة الخدمة ١: ضمان التسليم مع التأكيد؛ يتم إعادة إرسال الرسائل لجميع المشتركين في حالة عدم تلقي تأكيد.

ج. جودة الخدمة ٢: ضمان التسليم الفردي من خلال عملية تأكيد مزدوجة، مما يوفر أعلى موثوقية بأعلى تكلفة للموارد.

تعد جودة الخدمة ٢ أفضل من جودة الخدمة ١ من ناحية عدم تكرار الرسائل، حيث إن الرسائل التي وصلت لبعض المشتركين لا يعاد إرسالها ثانية لهم في حال عدم تلقي المشتركين الأخرين لهذه الرسائل. مثال، تم إرسال رسالة من الوسط للمشتركين أ و ب، وصلت الرسالة للمشترك أ بينما لم تصل الرسالة للمشترك ب. إن تم استخدام جودة الخدمة ١ فإنه سيتم إعادة إرسال الرسالة للمشتركَين (وهذا يجعل المشترك أ يستقبل الرسالة المكرر)، أما إن استخدمت جودة الخدمة ٢ فإن الرسالة سيتم إعادة إرسالها إلى المشترك ب فقط. يعتمد اختيار مستوى جودة الخدمة على عدة عوامل، مثل (١) موثوقية الشبكة ، (٢) أهمية محتوى الرسالة ، (3) تكرار الرسائل المرسلة.

يعد بروتوكول MQTT هو الخيار المفضل بناءً على أجهزة إنترنت الأشياء ويمكن أن يوفر توجيه معلومات فعال للأجهزة الصغيرة وغير المكلفة منخفضة الذاكرة والمستهلكة للطاقة في شبكات النطاق الترددي الضعيفة.

د. XMPP بروتوكول الرسائل القابلة للتوسيع والحضور

XMPP (Extensible Messaging and Presence Protocol) (بروتوكول الرسائل القابلة للتوسيع والحضور) هذا بروتوكول اتصال إنترنت الأشياء يعتمد على الوسيطة الموجهة للرسائل الموجهة XML وهو يدعم التبادل في الوقت الفعلي للبيانات المنظمة والقابلة للتطوير بين أي كيانين أو أكثر من كيانات الشبكة، تم تطوير البروتوكول من قبل مجتمع Jabber مفتوح المصدر في عام ١٩٩٩ ، ويستخدم بشكل رئيسي للمراسلة في الوقت الفعلي ومعلومات الحالة وصيانة قائمة جهات الاتصال، يتيح XMPP لتطبيقات المراسلة تنفيذ المصادقة ، والتحكم في الوصول ، والقفز خطوة بخطوة ، والتشفير من طرف إلى طرف، كبروتوكول أمان ، يجلس على رأس بروتوكول إنترنت الأشياء الأساسي ويربط العميل بالخادم من خلال تدفق أقسام XML يحتوي قسم XML على ثلاثة مكونات رئيسية: الرسالة والحالة و IQ.

ه. AMQP بروتوكول وضع الرسائل في قائمة انتظار متقدمة

AMQP (بروتوكول انتظار الرسائل المتقدم) هو معيار مفتوح من معايير (منظمة النهوض بمعايير المعلومات المنظمة) OASIS (Organization for the Advancement of Structured Information Standards)تم استخدامه في البداية في الأعمال المصرفية والمالية، ويمتد الآن ليشمل شبكات إنترنت الأشياء. مثل MQTT، فإنه يستفيد من بروتوكول TCP ويعتمد على آلية النشر والاشتراك غير المتزامنة. يتضمن النظام وسيطًا يستقبل الرسائل ويوزعها، وأجهزة تعمل كمنتجين (إرسال الرسائل) أو مستهلكين (الطلب والمعالجة رسائل).

يتكون الوسيط من:

- التبادل: فرز الرسائل من المنتجين إلى قوائم الانتظار بناءً على مفاتيح الربط.
- قوائم الانتظار: قوائم الرسائل المحددة بواسطة مفاتيح الربط، والتي يمكن أن تكون متقلبة أو مستمرة.

تسمح مرونة AMQP بالاتصال عبر الأنظمة الأساسية بين البنى المختلفة، مثل أنظمة Java وPython. من بين وسطاء AMQP المشهورين RabbitMQ، وApache Qpid، وAzure Service Bus.

يدعم AMQP ثلاثة مستويات لجودة الخدمة (QoS)، مشابهة لـ MQTT:

١- مرة واحدة على الأكثر: يتم إرسال الرسائل دون تأكيد استلامها.

٢- مرة واحدة على الأقل: يتم تخزين الرسائل وإعادة إرسالها حتى يتم تأكيد الاستلام، مما يضمن تسليمها.

٣- مرة واحدة بالضبط: نضمن تسليم الرسائل مرة واحدة بالضبط، مع آلية تأكيد مزدوجة تضمن عدم وجود تكرارات.

ومع ذلك، فهي ليست مثالية لأجهزة إنترنت الأشياء محدودة الطاقة، لأنها ترسل المزيد من البيانات وتستغرق وقتًا أطول من البروتوكولات الأخرى. يستخدم AMQP أيضًا TLS للأمان، ولكن يوصى باستخدام بروتوكولات أقل تكلفة للسيناريوهات ذات الطاقة المحدودة.

و. **STOMP (Simple Text Oriented Messaging Protocol) بروتوكول رسائل نصية بسيطة**

تم تطوير هذا البروتوكول الموجه بالنص مع الوسيطة الموجهة للرسالة، يوفر تنسيق اتصال قابلاً للتشغيل البيني يمكّن عملاء STOMP من التواصل مع أي وسيط رسائلSTOMP ، وبالتالي تحقيق إمكانية التشغيل البيني والواسع النطاق للرسائل بين اللغات والأنظمة الأساسية والوسطاء، مثل AMQP، يوفر STOMP سمات ونص إطار لرأس الرسالة.

ومع ذلك، لا يتعامل STOMP مع قوائم الانتظار والمواضيع - يستخدم دلالات SEND ودلالات "الهدف" يجب على الوكيل تعيينه لمحتوى مفهوم داخلياً، مثل المواضيع أو قوائم الانتظار أو التبادل ثم يشترك المستهلكون في هذه الوجهات، نظراً لأن هذه الوجهات غير محددة في المواصفات، فقد يدعم وسطاء مختلفون وجهات مختلفة، لذلك لا يكون رمز النقل بين الوكلاء واضحاً دائماً.

ومع ذلك، فإن STOMP بسيط وخفيف الوزن (على الرغم من أنه مطول إلى حد ما على الويب)، ولديه مجموعة متنوعة من الروابط اللغوية، كما يوفر بعض دلالات المعاملات RabbitMQ Web Stompهو أحد الأمثلة الأكثر إثارة للاهتمام، فهو يسمح لك بكشف الرسائل في المتصفح عبر Websockets.

ز. VSCP بروتوكول تحكم بسيط للغاية

إطار أكثر من الاتفاق VSCP .قابل للتطوير بدرجة كبيرة ويستهلك مساحة صغيرة، وهو حل مجاني ومفتوح المصدر لاكتشاف الجهاز وتحديده ، وتكوين الجهاز ، ووظائف الجهاز المستقلة ، وتحديثات البرامج الثابتة الآمنة، يتيح VSCP الأشياء للتفاعل في طبقة التطبيق،

يستخدم CAN و RS-232 و Ethernet و TCP/IPو MQTT و 6LowPan

يستخدم VSCP تنسيق الحدث ويدعم المعرف الفريد للعقدة، لذلك بغض النظر عن مكان تثبيت العقدة في العالم، يمكن تحديد العقدة بالإضافة إلى ذلك، يحتوي أيضاً على نموذج تسجيل لتوفير واجهة عامة مرنة لتكوين العقدة ونموذج للتحكم في وظيفة كل عقدة، لا يقوم VSCP بافتراضات حول النظام ذي المستوى الأدنى المستخدم لتحقيق الربط المادي مع العقد؛ وبالتالي ، فهو قابل للتطبيق على Ethernet و TCP / IP واللاسلكية و Zigbee و Bluetooth و CAN و GPRS و RS- 232 و USBآلية النقل.

يعتمد VSCP على الأحداث في كل مرة يقع فيها حدث، يتم بثه إلى جميع العقد الأخرى على الشبكة، من هناك تقرر كل عقدة ما إذا كانت تحتاج إلى معالجة الحدث المستلم أم لا يعتمد القرار النهائي على مصفوفة قرار العقدة، والتي تتكون من عدة <'if condition ثم <action خطوط'، حيث يتم تقييم الشرط <بناءً على الحقول الموجودة في مخطط بيانات VSCP الذي تم بثه على الشبكة.

الأمان في بروتوكولات وتقنيات إنترنت الأشياء

يتعين على موفري حلول إنترنت الأشياء إشراك قضايا الأمان في جميع مراحل دورة إنترنت الأشياء، يجب أن يكون التركيز على الأمن السيبراني، يبدأ الأمان في مرحلة التصميم مع التركيز بشكل خاص على نمذجة التهديدات، واختيار المكونات الآمنة، وقابلية المكونات للتكيف مع تدابير الأمان المستقبلية، وأخيراً، اختبار المرونة، تعد وظيفة FOTA أمراً ضرورياً للتحديثات عن بُعد وتصحيح الأعطال وحماية البيانات في حالة حدوث انتهاكات أمنية.

يمكن لخيارات العمليات المستقلة في حالة حدوث مشكلات في الاتصال أن تمنح ثقة أكبر للمستخدمين، يجب أن تقوم الشركة المصنعة أيضاً بتثقيف المستخدمين لإعداد تفضيلات مستخدم أقوى من خلال تكوينات المستخدم.

يمكن للمستخدمين من جانبهم تقليل مخاطر الاختراقات الأمنية باستخدام كلمات مرور قوية لحسابات الأجهزة وشبكات Wi-Fi ، واستخدام طريقة تشفير أقوى عند إعداد شبكات Wi-Fi مثلWPA2 ، وتعطيل الوصول عن بُعد إلى أجهزة إنترنت الأشياء عندما لا مطلوب ، وتعطيل الميزات غير المستخدمة حاليًا مثل معلومات الموقع.

مسؤوليات الأطراف عن الأمن السيبراني لأنظمة إنترنت الأشياء

يمكن لمطوري حلول إنترنت الأشياء، بما في ذلك الشركات المصنعة للمعدات، توفير تدابير الأمن السيبراني التالية :

أ. استخدام أدوات تطوير البرامج الحديثة والموثوقة API ، والمكتبات، والأطر، والبروتوكولات، وما إلى ذلك وحلول الأجهزة (اللوحات ، وأجهزة التحكم ، وما إلى ذلك).

ب. تقليل عدد المكونات اللازمة لتشغيل الجهاز، حيث إن كل عنصر إضافي مصدر محتمل للعديد من نقاط الضعف، بما في ذلك. الأعطال الجسدية، على سبيل المثال، لا يجب إضافة منافذ USB إلا إذا كانت هناك حاجة فعلية لها حتى يعمل الجهاز الذكي .

ج. تنفيذ المصادقة الآمنة، ومفاوضات الجلسة المشفرة، ومصادقة المستخدم.

د. ضمان الإصدار المنتظم لتحديثات البرامج للتخلص من الثغرات الأمنية التي تم العثور عليها والمحتملة .

ومع ذلك، لا يتحمل مطورو برامجها ومكوناتها فقط مسؤولية ضمان أمن المعلومات لإنترنت الأشياء، نظراً لأن مستخدمي أنظمة إنترنت الأشياء هم أول من يعاني من القرصنة أو فقدان البيانات، فإنهم هم الذين يجب أن يهتموا بحماية أجهزتهم وتطبيقاتهم، للقيام بذلك، **تحتاج إلى إجراء المعالجات التالية البسيطة إلى حد ما:**

- لا تستخدم معلومات تسجيل الدخول وكلمات المرور المثبتة مسبقًا من قبل الشركة المصنعة على أنها عاملة - يجدر إنشاء حساب مستخدم جديد بحقوق وصول محدودة.
- تعيين كلمة مرور "معقدة" لشبكة منزلك / شركتك وتمكين تشفير حركة مرور الشبكة.
- قم بتحديث برامج الأجهزة الذكية بانتظام من مصادر موثوقة.

الخصوصية هي جزء أساسي من الأمن

كانت قضايا الخصوصية مؤخراً في طليعة النقاش حول الشبكات، إنترنت الأشياء لديه القدرة على توفير كميات غير مسبوقة من المعلومات الشخصية، قد تقع هذه المعلومات في أيدي منتهكي المعلومات، سيحتاج مصنعي المعدات الأصلية إلى توفير سياسات خصوصية حول كيفية تعاملهم مع هذه البيانات، كما يجب عليهم تبني أفضل الممارسات لتجنب الإضرار بالسمعة والالتزام بالمتطلبات التنظيمية.

إنترنت الأشياء موجود لتبقى، وكلما جاء هذا الإدراك مبكراً – كان ذلك أفضل لكل من المستهلكين ومقدمي الحلول الذكية.

تحتاج الصناعة إلى إطار عمل قوي لضمان عدم إعاقة ثقة المستهلك في إنترنت الأشياء بأي شكل من الأشكال، بدلاً من ذلك، يجب أن يكون التركيز فقط على توفير أقصى درجات الراحة والراحة للعالم.

مشكلات الأمان وحلولها

نقاط الضعف والهجمات انترنت الأشياء IoT

في الآونة الأخيرة يضع المتسللون أنظارهم على أجهزة إنترنت الأشياء، يستفيدون بشكل عام من نقاط الضعف الموجودة بالإضافة إلى التكوين الخاطئ للمستخدم لتنفيذ هجماتهم، فهي لا تهدد فقط أمان وخصوصية المستخدمين، ولكن أيضاً على الأجهزة الأخرى التي قمت بتوصيلها على نفس الشبكة.

واحدة من أكبر المشكلات هي ما يعرف باسم ظل إنترنت الأشياء، في الأساس هو الاستخدام المعطى للأجهزة الشخصية لموظفي المؤسسة التي تكشف شبكات الشركة، هناك العديد من الأجهزة المتصلة بهذه الشبكات التي - وفقاً للخبراء- لم تكن مستعدة لمثل هذا التدفق، ما يفعله المتسللون هو استغلال واستغلال الثغرات الأمنية المحتملة على أجهزة الحاسب هذه.

أيضاً هجمات ضد أنظمة الوصول إلى المباني الذكية على وجه التحديد، أطلقوا في فبراير تنبيها يشير إلى وجود أكثر من 2,000 مبنى تم استغلالها من قبل المتسللين كان أحد الأهداف لتنفيذ هجمات DDoS.

سيارات تم استهدافهم أيضاً من قِبل المتسللين. إنها حقيقة أنه في كل مرة يكون لديهم تقنية أكثر تقدماً، وصلت إنترنت الأشياء أيضاً المركبات الحديثة، على وجه التحديد، تمكنوا من مهاجمة الكاميرا التي يحملها الكثيرون.

اكتشف Checkmarx أن Trifo Ironpie M6 فراغ ذكي كانت بها عيوب أمنية يمكن استغلالها لاختطاف الأجهزة ومقاطع الفيديو الخاصة بها.

مسألة أخرى مهمة تتعلق محاور ذكية، قامت ESET بتوثيق أجهزة محلية مختلفة عما نعرفه باسم إنترنت الأشياء، ومن بينها يمكننا تسمية المحاور التي تم استخدامها لتنفيذ الهجمات، وجدوا ثغرات كبيرة سمحت بتنفيذ التعليمات البرمجية عن بُعد وحتى اختطاف الجهاز تماماً.

الأحدث هو حالة Kaiji ظهر هذا الروبوت في مايو ويستهدف بشكل أساسي أجهزة إنترنت الأشياء و لينكس الخوادم، نفذ هجمات القوة الغاشمة لإنجاز هجمات.DDoS

باختصار، هذه هي الهجمات الرئيسية ونقاط الضعف التي أثرت على أجهزة إنترنت الأشياء في الأشهر الأخيرة، من المهم جدًا أن نهتم دائماً بالسلامة، من الضروري أن نحمي معداتنا بشكل صحيح بكلمة مرور جيدة، بحيث لا نحتفظ أبداً بالمعدات التي تأتي من المصنع ونقوم بتحديثها بشكل صحيح، في العديد من المناسبات تظهر نقاط ضعف يمكن استغلالها من قبل المتسللين لنشر هجماتهم، من الضروري تثبيت التصحيحات المتاحة.

منهجية اختراق انترنت الأشياء IoT

تأتي أهمية انتباه الشركات التي تقوم بتصنيع هذه الأجهزة كل اليوم إلى ضرورة وضع جدران حماية غاية في القوة، لحماية هذه الأجهزة من التعرض لأي هجمات إلكترونية، بل عليهم أن يراعوا عند تصميم هذه الجدران تصور وتخيل أسوأ السيناريوهات على الإطلاق.

للتعرف كيفية حماية أجهزتنا المعتمدة على تقنية إنترنت الأشياء، علينا أن نعرف أولاً الطرق التي من خلالها يمكن اختراق هذه الأجهزة من أكثر هذه الطرق شيوعاً.

١. استغلال الثغرات ونقاط الضعف

تشير بعض تقارير الأمن المعلوماتي إلى أن الأجهزة العاملة بتقنية إنترنت الأشياء تتعرض للهجمات الإلكترونية عبر الثغرات الإلكترونية حوالي ٨٠٠ مرة في الساعة الواحدة بواسطة مخترقون من كافة أنحاء العالم، حيث يقوم هؤلاء المخترقون بما يمكن وصفة بدق الأبواب الخلفية لهذه الأجهزة في محاولة لإيجاد وسيلة للدخول إليها.

وكشفت التقارير ذاتها إلى أنه يوجد أكثر من ٤٠٠ محاولة للدخول لكل جهاز، ٦٦ بالمائة منها تنجح بالفعل، وبمجرد نجاح المخترق في تنفيذ الاختراق الأولي سيتمكن من إحكام سيطرته على الجهاز في حدود ٦ دقائق فقط.

٢. الاختراق عبرuPNP

تقنية uPNP هي تقنية تسمح لبعض الأجهزة مثل كاميرات الفيديو على سبيل المثال، أن تتصل بالإنترنت وأن تقبل الاتصالات الخارجية بمجرد شبكها. وقد طورت هذه التقنية لتسمح للمستخدمين بالتحكم في أجهزتهم عن بعد عبر الإنترنت، ولكنها في الوقت ذاته تسمح لهذه الأجهزة بالتعرض المفتوح للعالم، وطالما تمكن الاتصال الخارجي من الوصول إلى هذه الأجهزة، فسيتمكن المخترقون من الوصول إليها أيضاً.

٣. اعتراض شبكات الهواتف

تعتمد بعض أجهزة إنترنت الأشياء على الاتصال الخليوي عبر شبكات الهاتف عوضاً عن الاتصال اللاسلكي عبر الواي فاي، وبينما يسمح الاتصال عبر الواي فاي بفتح بعض الثغرات، يسمح الاتصال عبر شبكات الهاتف بفتح ثغرات أكثر.

فعندما تقوم باستخدام هاتفك لإجراء اتصال لا يمكنك توقع أن هناك من يمكنه اختراق هذا الاتصال. ولكن الحقيقة هي أنه يمكن اختراق هذه الاتصالات عبر أجهزة قد لا تكلف أكثر من ٦٠٠ دولار، ومن بين الأجهزة التي تعمل بهذه الطريقة السيارات الحديثة على سبيل المثال، فلنفترض أن أحد المخترقين قد استطاع أن يخترق اتصال سيارة جيب جراند شيروكي التي تعتمد على الاتصال الخليوي، هل يمكنك تخيل مدى المخاطر التي سيمكنه التسبب فيها عبر التحكم الكلي في هذه السيارة.

استخدام VPN

ما هي شبكات VPN وكيف تعمل؟

تعني" VPN الشبكة الافتراضية الخاصة "وتقدم وصفا لكيفية إنشاء اتصال شبكي محمي عند استخدام الشبكات العامة، تقوم شبكات VPN بتشفير حركة البيانات الخاصة بك على الإنترنت وإخفاء هويتك الإلكترونية، مما يجعل تتبع أنشطتك عبر الإنترنت وسرقة بياناتك أمراً في غاية الصعوبة بالنسبة للغير، حيث يتم التشفير في الوقت الفعلي.

ما هي آلية عمل شبكات VPN ؟

تخفي شبكات VPN عنوان IP الخاص بك من خلال السماح للشبكة بإعادة توجيهه عبر خادم مهيأ خصيصا ويعمل عن بعد تحت إدارة مستضيف شبكة VPN ، وهذا يعني أنه إذا قمت بالتصفح عبر الإنترنت باستخدام شبكة VPN ، فإن خادم VPN يصبح مصدر بياناتك، هذا يعني أن مزود خدمة الإنترنت (ISP) والأطراف الثالثة الأخرى لا يمكنهم معرفة مواقع الويب التي تزورها أو البيانات التي ترسلها وتستقبلها عبر الإنترنت. تعمل شبكة VPN مثل عامل تصفية يحوّل جميع بياناتك إلى "بيانات مبهمة". ومن تم، حتى لو نجح أي طرف في الوصول إلى هذه البيانات، فستكون بلا فائدة.

ما هي فوائد اتصال VPN ؟

يخفي اتصال VPN حركة البيانات عبر الإنترنت ويحميها من الوصول الخارجي، فالبيانات غير المشفرة يمكن عرضها من قِبل أي شخص يمكنه الولوج إلى الشبكة ويريد رؤيتها، لكن عند استخدام VPNيصبح من الصعب على المخترقين ومجرمي الإنترنت فك تشفير هذه البيانات.

التشفير الآمن :تحتاج إلى مفتاح تشفير لقراءة البيانات، وبدون امتلاك مفتاح، سيستغرق الكمبيوتر ملايين السنين لفك الشفرة في حالة الهجوم المكثف بمساعدة VPN ، يتم إخفاء أنشطتك عبر الإنترنت حتى على الشبكات العامة.

إخفاء أماكن تواجدك :تعمل خوادم VPN بشكل أساسي كخوادم وكيلة لك على الإنترنت، ونظراً لأن بيانات الموقع الديموغرافي تأتي من خادم في دولة أخرى، لا يكون بالإمكان تحديد موقعك الفعلي، إضافةً إلى ذلك، فإن معظم خدمات VPN لا تخزن سجلات نشاطك، من ناحية أخرى، يقوم بعض مقدمي الخدمة بتسجيل سلوكك، لكنهم لا يمررون هذه المعلومات إلى أطراف ثالثة، وهذا يعني أن أي سجل محتمل لسلوكك كمستخدم يظل مخفياً بشكل دائم.

الوصول إلى المحتوى المحلي :لا يكون من الممكن دائماً الوصول إلى محتوى الويب المحلي من كل مكان، حيث تحتوي الخدمات والمواقع في كثيرٍ من الأحيان على محتوى لا يمكن الوصول إليه إلا من أجزاء معينة من العالم، وهنا تستخدم الاتصالات القياسية الخوادم المحلية في البلد لتحديد موقعك، وهذا يعني أنه لا يمكنك الوصول إلى المحتوى في بلدك أثناء السفر، ولا يمكنك الوصول إلى المحتوى الدولي من بلدك، هنا تتدخل خدمة تغيير الموقع عبر VPN لتسمح لك بتبديل الخادم إلى بلدان أخرى و"تغيير" موقعك بشكل فعّال.

النقل الآمن للبيانات :إذا كنت تعمل عن بُعد، فقد تحتاج إلى الوصول إلى الملفات المهمة على شبكة شركتك، ولأسباب أمنية، يتطلب هذا النوع من المعلومات اتصالًا آمناً، غالباً ما يلزم وجود اتصال VPNللوصول إلى الشبكة، حيث تتصل خدمات VPN بالخوادم الخاصة وتستخدم أساليب التشفير للحد من خطر تسرب البيانات.

ما الدور الذي ينبغي أن تقوم به شبكاتVPN ؟

يجب أن تكون شبكة VPN نفسها محمية من الاختراق، **من أهم المميزات التي تقدمها شبكةVPN :**

- **تشفير عنوان IP الخاص بك:** تتمثل المهمة الأساسية لشبكة VPN في إخفاء عنوان IP الخاص بك عن مزود خدمة الإنترنت الخاص بك والأطراف الثالثة الأخرى، ويسمح هذا لك بإرسال واستقبال المعلومات على الإنترنت دون التعرض لخطر رؤيتها بواسطة أي طرف بخلافك ومزود خدمة.VPN
- **تشفير البروتوكولات** :ينبغي لشبكات VPN كذلك أن تمنع بقاء أي أثر لاستخدامك، مثل تاريخ التصفح أو تاريخ البحث أو ملفات تعريف الارتباط، ويعد تشفير ملفات تعريف الارتباط مهماً بشكل خاص لأنه يمنع الجهات الخارجية من الوصول إلى المعلومات السرية مثل البيانات الشخصية والمعلومات المالية والمحتويات الأخرى على مواقع الويب.
- **إيقاف الاتصال :**إذا انقطع اتصال VPN الخاص بك فجأة، فسيتم أيضاً قطع اتصالك الآمن، يمكن لشبكات VPN الجيدة اكتشاف هذا التوقف المفاجئ وإنهاء البرامج المحددة مسبقاً، مما يقلل من احتمال تعرض البيانات للخطر.
- **المصادقة ثنائية العوامل :**من خلال استخدام مجموعة متنوعة من أساليب المصادقة، تقوم شبكات VPN القوية بفحص كل من يحاول تسجيل الدخول، على سبيل المثال، قد يُطلب منك إدخال كلمة مرور ومن ثم يتم إرسال رمز إلى جهازك المحمول، وهذا يزيد ما صعوبة وصول أي أطراف ثالثة غير مدعوة إلى اتصالك الآمن.

إذا يمكن للـ VPN أن توفير لإنترنت الأشياء: شبكة آمنة عن طريق تشفير البيانات، ويساعد في مصادقة الأجهزة، ويقلل من مخاطر اختراق البيانات.

تدريبات الفصل الثالث

س١: ضع كل من المصطلحات التالية أمام التعريف المناسب: (الوصول عن بعد، برامج الفدية، هجمات رجل في الوسط، عدم وجود تحديثات)

المصطلح	التعريف
	وهو أن يقوم المجرمون بتشفير نظامك بالكامل ويهددون بإزالة جميع بياناتك ما لم تعطيهم ما يطلبون
	وهو اختراق أجهزة إنترنت الأشياء والقيام بتشغيل الكاميرا/الميكروفونات دون علم أصحابها
	وهو أن يعترض المتسللون الاتصال بين طرفين ثم يغيرون الرسائل بينما يعتقد كلا الطرفين أنهما يتواصلان مع كل منهما آخر

س٢: اختار الإجابة الصحيحة للأسئلة التالية:

١. .....هو بروتوكول اتصال إنترنت الأشياء يعتمد على الوسيطة الموجهة للرسائل الموجهة ؟

أ. بروتوكولCoAP

ب. بروتوكولAMQP

ج. بروتوكولXMPP

د. بروتوكولMQTT

٢. .....هو بروتوكول تطبيق إنترنت للأجهزة المقيدة. وهي مصممة للاستخدام بين الأجهزة الموجودة في نفس الشبكة المقيدة، وبين الأجهزة الموجودة على الإنترنت. ؟

أ. بروتوكولCoAP

ب. بروتوكولAMQP

ج. بروتوكولXMPP

د. بروتوكولMQTT

٣. .....هو بروتوكول يتم استخدامه بشكل رئيسي للمراقبة عن بعد في إنترنت الأشياء. وتتمثل مهمته الرئيسية في الحصول على البيانات من العديد من الأجهزة ونقلها إلى البنية التحتية لتكنولوجيا المعلومات. ؟

أ. بروتوكولCoAP

ب. بروتوكولAMQP

ج. بروتوكولXMPP

د. بروتوكولMQTT

٤. .....يقوم/تقوم بتشفير حركة البيانات الخاصة بك على الإنترنت وإخفاء هويتك الإلكترونية؟

أ. بروتوكول رسائل نصية بسيطةSTOMP

ب. بروتوكول تحكم بسيط للغايةVSCP

ج. شبكاتVPN

د. المصادقة ثنائية العوامل

٥. .....من أدوات الأمن والاختراق IoT وتطبق من خلال استخدام مجموعة متنوعة من أساليب المصادقة ؟

أ. بروتوكول رسائل نصية بسيطةSTOMP

ب. بروتوكول تحكم بسيط للغايةVSCP

ج. شبكاتVPN

د. المصادقة ثنائية العوامل

٦. .....هو إطار (فريمورك) أكثر من كونه بروتوكول. قابل للتطوير بدرجة كبيرة ويستهلك مساحة صغيرة. ؟

أ. بروتوكول رسائل نصية بسيطةSTOMP

ب. بروتوكول تحكم بسيط للغايةVSCP

ج. شبكاتVPN

د. المصادقة ثنائية العوامل

٧. .....يوفر/توفر تنسيق اتصال قابلاً للتشغيل البيني؟

أ. بروتوكول رسائل نصية بسيطةSTOMP

ب. بروتوكول تحكم بسيط للغايةVSCP

ج. شبكاتVPN

د. المصادقة ثنائية العوامل

س٣: ضع علامة صح أمام العبارة الصحيحة وعلامة خطأ أمام العبارة الخاطئة.

١. استخدام كلمات المرور الافتراضية لا يعد من التهديدات المصاحبة لإنترنت الأشياء ( )

٢. تتمثل المهمة الأساسية لشبكة VPN في إخفاء عنوان IP الخاص بك عن مزود خدمة الإنترنت الخاص بك والأطراف الثالثة الأخرى ( )

حل تدريبات الفصل الثالث

حل السؤال الأول:

١- هجوم برنامج الفدية
٢- الوصول عن بعد
٣- هجمات الرجل في الوسط

حل السؤال الثاني:

١. بروتوكولXMPP (ج)
٢. بروتوكول CoAP (أ)
٣. بروتوكول MQTT (د)
٤. شبكات VPN (ج)
٥. المصادقة ثنائية العوامل (د)
٦. بروتوكول تحكم بسيط للغاية VSCP
٧. بروتوكول رسائل نصية بسيطة STOMP

حل السؤال الثالث:

١. خطأ
٢. صح

رابعاً: حلول الأمان القائمة على Blockchain لأنظمة إنترنت الأشياء

في هذا الفصل سنتعرف على المواضيع التالية:

- **المتطلبات التنظيمية**
- **تقنية Blockchain**
- **Blockchain وأنظمة إنترنت الأشياء**
- **أمثلة على حلول الأمان المستندة إلى Blockchain لأنظمة إنترنت الأشياء**

تمهيد

منذ ظهور شبكة الإنترنت، ارتفع عدد المستخدمين الذين يستخدمون الإنترنت للأغراض اليومية بشكل كبير. ومن الاحتياجات الشائعة الوصول إلى البيانات في أي وقت وفي أي مكان. واستجابة لذلك، بدأت العديد من الشركات في تقديم خدمات لتلبية هذا الطلب، وإدارة كميات هائلة من البيانات في مراكز البيانات. ويعد ضمان سلامة هذه البيانات مسؤولية بالغة الأهمية لهذه الشركات. وتعد تقنية البلوك تشين حلاً رائدًا يوفر تخزينًا ثابتًا للبيانات للمستخدمين.

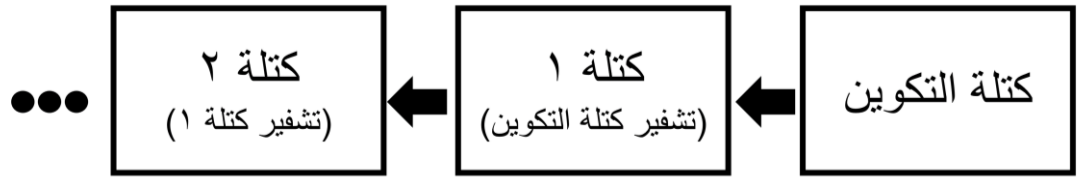
تُعَد تقنية البلوك تشين بمثابة سجل لامركزي وموزع يسهل تبادل البيانات بشكل شفاف وموثوق. ورغم أنها أثبتت فعاليتها بالفعل في القطاع المالي، فإن تطبيقاتها تتوسع في مجالات أخرى، ولا سيما سلاسل التوريد. ازداد الاعتماد على حلول البلوك تشين في إدارة سلسلة التوريد نظرًا لإمكاناتها في تعزيز مختلف العمليات التجارية والتنظيمية.

المتطلبات التنظيمية

تتيح تقنية البلوكشين طريقة مغايرة لعملية إنشاء البيانات وتخزينها تختلف عن قاعدة البيانات التقليدية حيث تتم بشكل لامركزي وموزع على جميع الأجهزة المرتبطة في الشبكة (Nodes) التي تقوم جميعها بالتحقق من صحة البيانات وتماثلها (Validation) بناء على قواعد التوافق الجماعي المحددة (Consensus)، ويتم حفظ البيانات في سجل معاملات موحد كنسخ متطابقة على جميع الأجهزة وليس كنسخة وحيدة في جهاز مركزي معين، ويضم السجل قائمة مستمرة من المعاملات التي تسمى كتل Blocks يتم ربطها بناء على قيمة Hash-value وتشفيرها لحماية السرية و تأمين صحة بياناتها باستخدام الخوارزميات ومنها قواعد التوافق الجماعي مثل (Proof of Work) و (Proof of Stake) و (Proof of Concept) و (Proof of Ownership) والتوقيع الإلكتروني (Digital Signature) وتشفير المفتاح العام والخاص (Public\Private Key Infrastructure encryption) وأنواع أخرى.

تسمح ميزة اللامركزية في تقنية البلوكشين بتبادل أي نوع من القيم بين أي طرفين دون الحاجة إلى تولي جهة مركزية معينة إدارة نظام المعاملات كمؤسسة مالية (بنك أو شركة مالية او غيره)، حيث يقوم عملها على شبكة "من النظير-إلى–النظير" (Peer-to-peer network) التي تتيح لجميع الأطراف والجهات ذات الصلة ولوج النظام في أي وقت وتوثيق منشأ وأصل كل معاملة وتسجيل بياناتها وتوصيلها إلى حالة التوافق الجماعي وتأكيد كل الأطراف عليها وثق عملية تسمى (Mining)، وبمجرد إجماع جميع الأطراف على المعاملة يتم إنشاء الكتلة (Block) المكونة من Header و Body ومن ثم إلحاقها بسلسلة باقي الكتل في الشبكة.

للتبسيط، يمكن مقارنة الكتل في سلسلة الكتل بورقة من مجموعة أوراق، حيث إنها قادرة على الاحتفاظ بأنواع مختلفة من البيانات. تُعرف الكتلة الأولى في سلسلة الكتل باسم كتلة التكوين، والتي يتم إنشاؤها عند إطلاق شبكة سلسلة الكتل لأول مرة. تحتوي الكتلة الثانية على المعاملات والتجزئة المشفرة لكتلة التكوين، وتتضمن كل كتلة لاحقة تجزئة سابقتها. يؤدي هذا إلى إنشاء بنية قائمة مرتبطة حيث يتم توصيل كل كتلة، باستثناء كتلة التكوين، بالكتلة التي تسبقها، كما هو موضح في شكل ٢١. يتم تعيين معرف فريد لكل كتلة، وتحمل كل عقدة في الشبكة نسخة كاملة من سلسلة الكتل. يمكن استخدام العقد من قبل المستخدمين الفرديين أو المستخدمين المتعددين.



شكل ٢١ مبدأ سلسلة الكتل

وتضمن تقنية البلوكشين درجة عالية من الثقة والأمان والشفافية في المعاملات، عبر تزويد المستخدمين ببيانات شاملة والقدرة على تعقب السجل التاريخي لكل المعلومات والمعاملات والتغيرات الطارئة عليها، ولا تسمح بأي حال مسح أي معاملة بعد إدخالها أو تعديل البيانات بدون سماح جميع الأطراف وتغيير جميع الكتل ذات الصلة، وذلك اعتماداً على عمل دالة الاختزال (Hash function) وعمليات التشفير التي تضمن تطابق البيانات في الكتل المترابطة بالسلسلة.

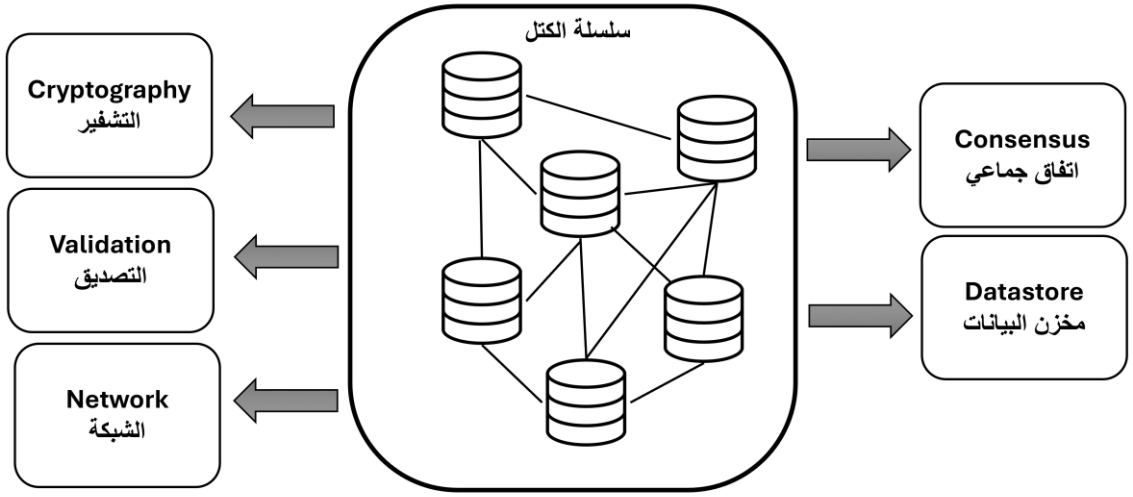
تنقسم شبكات البلوكشين إلى ثلاثة أنواع لكل منها استخدامات ومميزات مختلفة، وهي: شبكة البلوكشين العامة والبلوكشين الخاصة والاتحاد أو التحالف. يوضح جدول ٢ الفروقات بينها.

جدول ٢ الفروقات بين البلوكشين العامة والخاصة والاتحاد أو التحالف

	العامة	المتحدة	الخاصة
المستخدمون	إدارة غير مركزية بدون ترخيص هوية سرية/رموز قد يكون مصدرا ضارا	عدة مؤسسات ترخيص دخول هوية معرفة موثوقين	مؤسسة واحدة ترخيص دخول هوية معرفة موثوقين
آلية التوافق الجماعي والتأكيد	Proof of Stake, Proof of Work etc استهلاك كبير للطاقة	Consensus Algorithm أخف استهلاكا	Consensus Algorithm أخف استهلاكا
وقت تأكيد المعاملة	طويل Bitcoin: 10 min or more	قصير 100x msec	قصير 100x msec
أبرز الفوائد	لامركزية ولا حاجة لأي طرف وسيط لإتمام المعاملات.	الشفافية والأمان وتخفيض تكلفة المعاملات والوقت المستغرق وتقليل تكرار البيانات.	الشفافية والأمان وتخفيض تكلفة المعاملات والوقت المستغرق وتقليل تكرار البيانات.

ما المقصود بتقنية سلسلة الكتل؟

تقنية سلسلة الكتل هي آلية قاعدة بيانات متقدمة تسمح بمشاركة المعلومات الواضحة داخل شبكة الأعمال، تخزن قاعدة بيانات سلسلة الكتل البيانات في كتل مرتبطة ببعضها في سلسلة، وتعد البيانات متسقة زمنياً لأنه لا يمكنك حذف السلسلة أو تعديلها من دون توافق من الشبكة، ونتيجة لذلك، يمكنك استخدام تقنية سلسلة الكتل لإنشاء سجل حسابات غير قابل للتغيير أو ثابت لتتبع الطلبات والمدفوعات والحسابات والمعاملات الأخرى، يحتوي النظام على آليات مدمجة تمنع إدخالات المعاملات غير المصرح بها وتُنشئ تناسقاً في طريقة العرض المشتركة لهذه المعاملات. يوضح شكل ٢٢ العناصر الأساسية لبنية عمل البلوكشين.



شكل ٢٢ العناصر الأساسية لبنية عمل أنظمة البلوكشين

لماذا تعد سلسلة الكتل مهمة؟

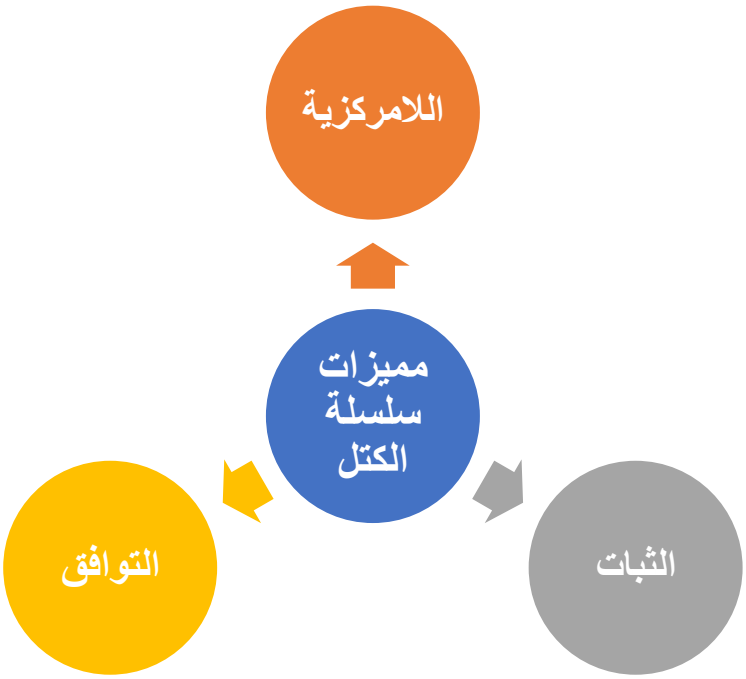
تقدم تقنيات قواعد البيانات التقليدية العديد من التحديات فيما يتعلق بتسجيل المعاملات المالية. على سبيل المثال، فكّر في بيع عقار، بمجرد تبادل الأموال، يتم نقل ملكية العقار إلى المشتري، بشكل فردي، يمكن لكل من المشتري والبائع تسجيل المعاملات النقدية، ولكن لا يمكن الوثوق بأي من المصدرين، يمكن للبائع أن يدعي بسهولة أنه لم يستلم الأموال بالرغم من حصوله عليها، كما يمكن للمشتري أن يجادل بالمثل بأنه قد دفع الأموال، حتى لو لم يكن قد دفعها.

لتجنب المشكلات القانونية المحتملة، يجب على طرف ثالث موثوق به الإشراف على المعاملات والتحقق من صحتها، لا يؤدي وجود هذه السلطة المركزية إلى تعقيد المعاملة فحسب، بل ينشئ كذلك نقطة ثغرة أمنية واحدة، إذا تم اختراق قاعدة البيانات المركزية، فقد يعاني كلا الطرفين، تخفف سلسلة الكتل من هذه المشكلات من خلال إنشاء نظام لامركزي ومقاوم للتلاعب لتسجيل المعاملات.

في سيناريو معاملة العقارات، تُنشئ سلسلة الكتل سجل حسابات واحداً لكل من المشتري والبائع، يجب أن تتم الموافقة على جميع المعاملات من قبل الطرفين ويتم تحديثها تلقائياً في سجل حسابات كل طرف في الوقت الفعلي، فأي فساد في المعاملات السابقة سيفسد سجل الحسابات بأكمله، وأدت خصائص تقنية سلسلة الكتل هذه إلى استخدامها في مختلف القطاعات، بما في ذلك إنشاء عملة رقمية مثل البيتكوين.

ما ميزات تقنية سلسلة الكتل؟

تتميز تقنية سلسلة الكتل بالميزات الرئيسية الآتي، انظر شكل **٢٣**.



شكل ٢٣ مميزات سلسلة الكتل

- **اللامركزية**

تشير اللامركزية في سلسلة الكتل إلى نقل التحكم وصنع القرار من منشأة مركزية (فرد أو منظمة أو مجموعة) إلى شبكة موزعة، تستخدم شبكات سلسلة الكتل اللامركزية الشفافية لتقليل الحاجة إلى الثقة بين المشاركين، كما تمنع هذه الشبكات المشاركين من ممارسة السلطة أو السيطرة على بعضهم بطرق تؤدي إلى تدهور وظائف الشبكة.

- **الثبات**

الثبات يعني أن شيئًا ما لا يمكن تغييره أو تعديله، لا يمكن لأي مشارك التلاعب بمعاملة بمجرد قيام شخص ما بتسجيلها في سجل الحسابات المشترك، إذا تضمن سجل المعاملة خطأ ما، فيجب عليك إضافة معاملة جديدة لعكس الخطأ، وتكون كلتا المعاملتين مرئيتان للشبكة.

- **التوافق**

يضع نظام سلسلة الكتل قواعد حول موافقة المشارك لتسجيل المعاملات، لا يمكنك تسجيل معاملات جديدة إلا بعد موافقة غالبية المشاركين في الشبكة.

Blockchain وأنظمة إنترنت الأشياء

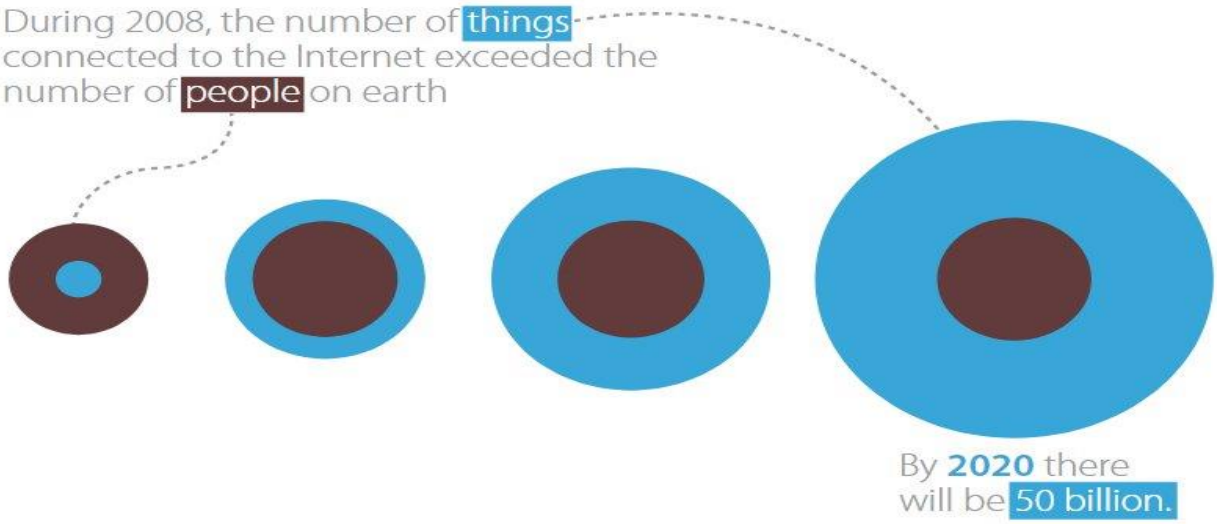
مما لا شك فيه أن استخدام انترنت الأشياء في تزايد مستمر، خصوصا مع تطور التكنولوجيا المتعلقة بالمباني الذكية والثورة الهائلة في مجال الهواتف الذكية، فأصبحت الحوسبة السحابية تعاني من تحديات عديدة في معالجة وتخزين الكم الهائل من البيانات.

أدى ذلك إلى الحاجة الملحة لاستخدام تقنية مساندة جديدة وهي الحوسبة الضبابية Fog Computing التي تدعم عمل الحوسبة السحابية، وذلك من خلال التعامل مع المعلومات الضخمة المتولدة من انترنت الأجهزة، فتقدم خدمة معالجة البيانات وتصفيتها قريبا من الأجهزة وقبل الوصول للسحابة، مما يخفض الوقت المستغرق للمعالجة وبالتالي تخفيف الضغط على الشبكة، فتصبح الحوسبة الضبابية كطبقة وسيطة بين الحوسبة السحابية وانترنت الأشياء في البنية الأساسية لها، فتضيف طبقة إضافية من الحماية والأمن في هذه المنظومة، وبما أنه تم تقليص انتقال المعلومات إلى السحابة، فبالتالي تصبح فرصة اعتراض المعلومات واختراقها أقل.

ولعل أكثر التقنيات فعالية في زيادة مستوى الأمان في شبكة انترنت الأشياء هي سلسلة الكتل Blockchain ، وقد اعتمدت العديد من الشركات هذه التكنولوجيا الجديدة لخلق بيئة أمنة لشبكتهم، فهي قاعدة بيانات ضخمة و موزعة تمتاز بقدرتها على إدارة قائمة من السجلات تسمى كتلا أو Blocks ، تضمن ميزة اللامركزية في Blockchain بتخزين البيانات الحساسة في أجهزة كمبيوتر موجودة في أماكن متفرقة، ومع إنشاء تدفق لامركزي للبيانات فإنه من الصعب اختراق الشبكة من قبل المتطفلين، ستعمل تقنية Blockchain على تحسين قابلية التوسع والأمان والخصوصية بحيث تصبح قادرة على تعزيز الأمن السيبراني للمؤسسات في أنحاء العالم.

غالباً ما يُعد الجمع بين blockchain و Internet of Things [IoT] أحد أكثر المجالات الواعدة لاستخدام التكنولوجيا خارج عملة التشفير نفسها، على وجه الخصوص، مع الإشارة إلى Internet of Things، يمكن لعناوين الحظر، والمعروفة باسم الارتباطات المفقودة، أن تعالج الإضافات والخصوصية ومشاكل الأمان في النظام البيئي.

في بداية عام ٢٠١١، توقعت شركة Cisco أن يكون هناك ما يقرب من ٥٠ مليار جهاز مختلف مترابط يتم تشغيله على الإنترنت العالمي بحلول عام ٢٠٢٠، لكن التوقعات المختلفة لعام ٢٠١٦ تشير إلى أن عددهم سيرتفع إلى ٥٠٠ بحلول عام ٢٠٣٠، إذا تم تنفيذ مثل هذه التنبؤات فعلياً ، فهذا يعني تكلفة غير مسبوقة لنقل البيانات، هذا لا يتطلب التحكم في الجهاز وضمان أمنه ، وهذا يثير مسألة اعتماد إنترنت الأشياء على نطاق واسع في ظل القضايا الرئيسية. انظر شكل ٢٤.



شكل ٢٤إحصائيات لحلول عام ٢٠٢٠

في الوقت نفسه، يجب أن نتذكر أن تقنية blockchain نفسها، مثل Internet of Things ، هي اختراع جديد نسبياً ، لأن التطبيقات التي تم إنشاؤها على هذا الأساس لها أيضاً مناطق مشاكل خاصة بها، على الرغم من ذلك ، لاتزال الطبيعة اللامركزية لـ blockchain لها العديد من المزايا ، وقد اعتمد مطورو أجهزة إنترنت الأشياء هذه المزايا بنجاح، وليس هناك الكثير من الأسباب للاعتقاد بأن هذه العملية ستتباطأ بشكل ما.

ما هي فوائد اللامركزية إنترنت الأشياء؟

على الرغم من أن صناعة إنترنت الأشياء تعتمد اليوم اعتماداً كبيراً على الخدمات المركزية، إلا أنه من الصعب أن نسميها حلولاً مناسبة طويلة الأجل لدعم تصميمات الأجهزة كبيرة الحجم المستقبلية، يمكن أن يكون نقل البيانات والخدمات الداخلية من خادم مركزي مفتاحاً لمساعدة إنترنت الأشياء في الوصول إلى إمكاناتها الكاملة.

أكثر أمانا

بالمقارنة مع الحلول السحابية، من المفترض أن توفر تقنية blockchain مستوى أعلى من الأمان للبنية التحتية بالكامل. لا توجد نقطة ضعف أو عيب واحد في الشبكة الموزعة، فتوقيع عملة التشفير على الطلب يجعل من الصعب غزو الشبكة، وأي رسالة تنشأ من أي موقع آخر غير الأصل ستكون غير صالحة.

منع الوصول غير المصرح به

باستخدام عملة مشفرة cryptocurrency غير المتماثلة [نوع العملة المشفرة، حيث يتم استخدام المفتاح لتشفير معلومات العملة، ولكنه ليس المفتاح المستخدم لفك تشفير المعلومات] لإنشاء طوابع زمنية وتخزين بيانات المعاملات، فإن التطبيق اللامركزي يقلل بدرجة كبيرة من خطر الوصول المصرح به إلى البيانات ومعالجتها.

خفض التكاليف

حالياً، هناك احتكار من قبل مقدمي خدمات إنترنت الأشياء، وهو ما ينطبق أيضاً على تكلفة المعدات المساعدة، من خلال تخزين البيانات في العقد دون إدارة مركزية. لا يقلل النموذج الموزع من تهديدات الأمان المختلفة فحسب، بل يجعل أيضاً إنترنت الأشياء أكثر فاعلية وإمكانية الوصول إليها. بالإضافة إلى ذلك، ستساعد اللامركزية على تقليل أو حتى تجنب تكلفة الضرر الناجم عن سلوك الدخيل، وكذلك القضاء على الوسطاء والتكاليف ذات الصلة.

لا حاجة للثقة

يستخدم السجل الموزع للتحقق من صحة البيانات، في حين أن العقد الذكي يقوم بأتمتة هذه العملية، لذلك، ليست هناك حاجة إلى الوثوق بمزود خدمة مركزي أو مشارك آخر لتخزين البيانات أو مراقبة توفر اتصالات الجهاز.

أتمتة

كما يتيح blockchain للأجهزة الذكية أن تعمل بشكل مستقل ومستقل عن التحكم في عملها. يمكن أن تكون "الشركة المستقلة الموزعة" هذه هي أساس النظام البيئي المستقبلي لإنترنت الأشياء ويمكن أن تعمل وفقًا للمنطق المحدد مسبقًا لمنزل أو صناعة معينة. يمكنه أيضًا أتمتة العمليات المختلفة تماماً، مثل توزيع الخدمات المالية أو مدفوعات التأمين.

أمثلة على حلول الأمان المستندة إلى Blockchain لأنظمة إنترنت الأشياء

أفضل الأمثلة والتطبيقات Blockchain وIoT

تعتبر اللامركزية وتبادل البيانات الآمن من خلال Blockchain مفيدة في تطبيقات إنترنت الأشياء المختلفة، **فيما يلي قائمة ببعض التطبيقات العديدة حيث يمكنهم إنشاء قيمة هائلة معاً:**

- **تتبع الأصول والامتثال**

يعد تتبع الأصول أحد أكثر تطبيقات إنترنت الأشياء شيوعاً، يمكن أن تكون مراقبة هذه الأصول والمكونات ذات قيمة كبيرة إذا تم إجراؤها بشكل صحيح، على سبيل المثال، يمكن استخدامه لتتبع المكونات في طائرة أو مركبات خدمات خاصة بصرف النظر عن المرافق، والأهم من ذلك، يجب أن تكون هذه التطبيقات آمنة ومتوافقة مع اللوائح.

تتيح بيانات بوابة إنترنت الأشياء المخزنة في دفاتر الأستاذ الخاصة بـ Blockchain مشاركة البيانات بسهولة، علاوة على ذلك، فهي الطريقة الأكثر فعالية من حيث التكلفة والتي يمكن الوصول إليها لجميع المستخدمين النهائيين للوصول إلى المعلومات وتبادلها في أي وقت، هذه الجوانب الرئيسية تجعل كلا التقنيتين زوجاً مثالياً لأي أصل أو حاجة لتتبع المكونات.

- **النقل والخدمات اللوجستية**

على غرار تتبع الأصول، تشمل سلاسل الإمداد واللوجستيات أيضاً أطرافاً مختلفة، يمكن لمثل هذا التطبيق أيضاً الاستفادة من استخدام هذه التقنيات معاً، جميع البيانات المرتبطة بالمنتج آمنة ويمكن الوصول إليها وجديرة بالثقة باستخدام نظام Blockchain البيئي الذي يدعم إنترنت الأشياء، يمكن للشركات تحقيق أقصى استفادة من الخدمات اللوجستية من خلال تتبع معلومات المنتج المقاوم للتلاعب بأمان وسرعة.

- **بيانات إنترنت الأشياء الصناعية**

يتطلب إنترنت الأشياء الصناعي قدرًا كبيرًا من المصداقية والكفاءة على عكس التطبيقات الأخرى. يعد استشعار البيانات ومراقبتها للأنظمة الصناعية عملية ذات أهمية قصوى في مجال السلامة، يمكن لدفتر الأستاذ Blockchain المناسب الذي يدعم إنترنت الأشياء أن يسمح بإجراء تحليلات فعالة وصيانة تنبؤية للآلات، نتيجة لذلك من خلال هذه التقنيات، يمكن أن يكون العمال والمشرفون وطاقم الصيانة على نفس الصفحة، وبالمثل يمكن للهيئات التنظيمية أيضاً الحصول على فكرة دقيقة عن المنشآت الصناعية.

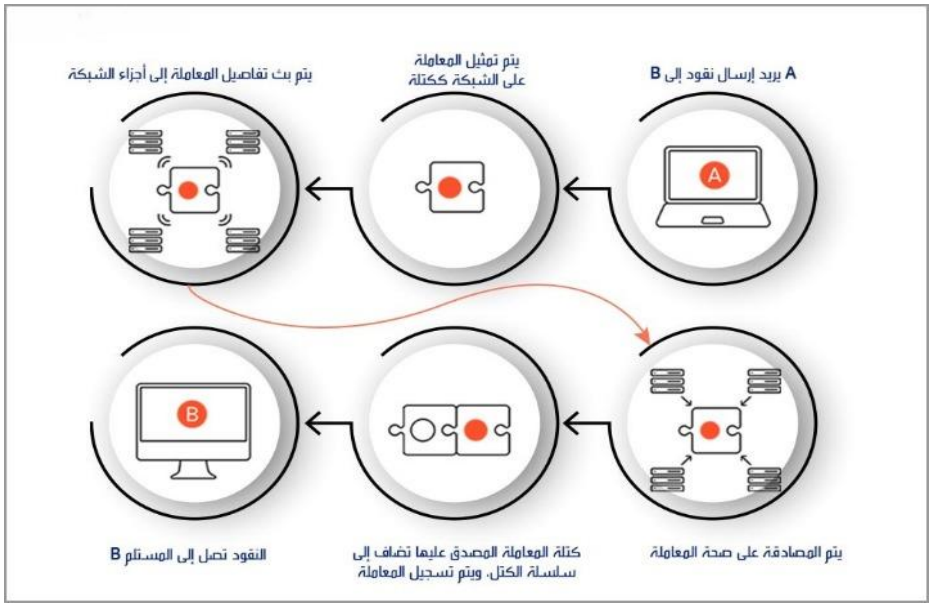
مثال على آلية عمل البلوكشين:

يمكن تعريف البلوكشين على أنه دفتر مشترك، يسمح للآلاف من أجهزة الحاسوب أو الخوادم المتصلة بالحفاظ على دفتر واحد مضمون وغير قابل للتغيير، يمكن للبلوكشين إجراء معاملات المستخدمين دون إشراك أي وسطاء تابعين لجهات خارجية. من أجل إجراء المعاملات، كل ما يحتاجه المرء هو أن يكون لديه محفظته.

إن محفظة البلوكشين هي برنامج يسمح للشخص بإنفاق عملات مشفرة مثل البيتكوين والايثيريوم وما إلى ذلك، ويتم تأمين هذه المحافظ بطرق التشفير (المفاتيح العامة والخاصة) بحيث يمكن للفرد إدارة معاملاته والتحكم فيها بشكل كامل.

أما عن الطريقة التي تعمل بها شبكة البلوكشين فهي كما يلي:

في البداية، عندما يقوم المستخدم بإنشاء معاملة عبر شبكة البلوكشين، سيتم إنشاء كتلة تمثل تلك المعاملة، وبمجرد إنشاء كتلة، يتم بث المعاملة المطلوبة عبر شبكة نظير إلى نظير، والتي تتكون من العديد من أجهزة الكمبيوتر التي تشغل نفس البرنامج، والتي تُعرف باسم العقد، والتي تقوم بعد ذلك بالتحقق من صحة المعاملة، ويمكن أن تتضمن المعاملة التي تم التحقق منها عملة مشفرة، أو عقود أو سجلات أو أي معلومات أخرى ذات قيمة. انظر شكل ٢٥.



شكل ٢٥ طريقة عمل البلوكشين

بمجرد التحقق من المعاملة، يتم دمجها مع الكتل الأخرى لإنشاء كتل جديدة من البيانات لدفتر الأستاذ، ومن المهم هنا ملاحظة أنه مع كل معاملة جديدة، يتم إنشاء كتلة مؤمنة، مربوطة مع بعضها البعض باستخدام مبادئ التشفير، وعندما يتم إنشاء كتلة جديدة، تتم إضافتها إلى شبكة البلوكشين الحالية لتأكيد أنها مؤمنة وغير قابلة للتغيير.

تطبيقات البلوكشين

البتكوين

لعل أهم تطبيقات البلوكشين على الإطلاق هو البتكوين (bitcoin)، الذي شغل العالم في السنوات القليلة الماضية.

قبل عدة سنوات، توصّل شخص مجهول (أو عدة أشخاص) تحت اسم ساتوشي ناكاموتو (Satoshi Nakamoto) إلى بروتوكول البتكوين، وهكذا بدأت ثورة مالية وتقنية جديدة، أحدثت رجّة (وما تزال) في النظام الاقتصادي العالمي، هذا البروتوكول سمح بالاستغناء عن الوسطاء والأطراف الثالثة، ووفّر نظاماً امنا للمصادقة والتخويل.

البتكوين كما يعرّفها أصحابها هي شبكة دفع مبتكرة وشكل جديد للأموال فهي عملة مشفرة (cryptocurrency)، وتعد شكلا من أشكال النقد الرقمي، إنها عملة رقمية لامركزية لا تتحكم فيها أي سلطة أو بنك مركزي، ويمكن إرسالها من مستخدم إلى آخر دون الحاجة إلى وسطاء، وتستخدم تكنولوجيا البلوكشين.

البتكوين مفتوحة المصدر، لا أحد يملك أو يدير شبكة البتكوين ويمكن لأي أحد المشاركة فيها.

العقود الذكية (Smart contracts)

العقد الذكي هو شيفرة حاسوبية يمكن تضمينها في البلوكشين لكتابة عقد أو التحقق منه والتفاوض عليه، تعمل العقود الذكية بموجب مجموعة من الشروط التي يوافق عليها المستخدمون، وعندما يتم استيفاء تلك الشروط، يتم تنفيذ الاتفاقية تلقائياً.

لنقل، على سبيل المثال، أنك تريد أن تستأجر مني شقة باستخدام عقد ذكي الاتفاق هو أني سأعطيك رمز الدخول إلى الشقة بمجرد أن تدفع لي أجر شهر، سنقوم بكتابة الصفقة في عقد ذكي، والذي سيُبادل رمز الدخول الخاص بالشقة تلقائياً بمبلغ الاستئجار عندما يحين وقت الدفع، بالطبع، ما زالت العقود الذكية في بدايتها، حالياً، يمكن برمجة عقود ذكية لأداء الوظائف البسيطة وحسب.

إيثيريوم (Ethereum) هي إحدى أشهر المنصات الخاصة بالعقود الذكية، وهي عبارة عن مشروع مفتوح المصدر يستخدم تكنولوجيا البلوكشين.

تخزين الملفات

تخزين الملفات على شبكة الإنترنت بشكل لامركزي له العديد من الفوائد، إذ يؤدي توزيع البيانات عبر الشبكة إلى حماية الملفات وتحصينها من الاختراق أو الضياع.

نظام الملفات الكوكبي (IPFS) أو (Inter Planetary File System) هو بروتوكول تم تأسيسه على هذه الفكرة، يتخلّص بروتوكول IPFS من الحاجة إلى علاقات مركزية بين العميل والخادم (كما هو شائع في شبكة الويب الحالية) هذا البروتوكول اللامركزي لديه القدرة على تسريع نقل الملفات، وقد تكون مثل هذه البروتوكولات الموزّعة مستقبل الشبكة، وهذا كله بفضل تكنولوجيا البيتكوين.

حماية الملكية الفكرية

في عالم الإنترنت، يمكن إنتاج ونسخ المعلومات الرقمية بلا حدود، وتوزيعها على نطاق واسع، وقد وفّر هذا لمستخدمي الويب منجم ذهب من المحتوى المجاني على مستوى العالم، لكن بالمقابل، فقد عانى الكثير من أصحاب حقوق الطبع والنشر، فقد فقدوا السيطرة على ملكيتهم الفكرية، وقد تضرّر الكثير منهم مالياً نتيجة لذلك.

يمكن للعقود الذكية حماية حقوق الطبع والنشر وأتمتة بيع الأعمال الإبداعية عبر الإنترنت، والتقليل من خطر نسخ الملفات وإعادة توزيعها عبر إلغاء الحاجة إلى الوسطاء، وبيع المنتجات مباشرة إلى المستهلكين.

إنترنت الأشياء (Internet of Things)

التشبيك، أو إنترنت الأشياء، هي إدارة أنواع معينة من الأجهزة الإلكترونية عبر الشبكة، مثل أجهزة مراقبة درجة حرارة الهواء في منشآت التخزين، العقود الذكية تجعل أتمتة إدارة هذه الأنظمة عن بعد ممكنة ،من أمثلة استخدام البلوكشين في التشبيك، شبكات الطاقة الذكية، لنفترض أنّ هناك أشخاصاً في المدينة يُنتجون الطاقة بأنفسهم (عبر خلايا الطاقة الشمسية مثلاً)، ويريدون بيع فائض الطاقة إلى جيرانهم، يمكن مثلاً للعقود الذكية المبنية على إيثيريوم أن توزّع تلك الطاقة تلقائياً وتتكفّل بتحويل الأموال من المشترين إلى البائعين، وقد بدأت شركة Consensys ، وهي شركة أمريكية، بمشروع قائم على العقود الذكية يقوم بمراقبة وإعادة توزيع الطاقة الكهربائية في شبكة الطاقة تلقائياً.

تسجيل الملكية

باعتبارها سجلات مفتوحة أمام الجميع، يمكن للبلوكشين أن تسهّل عملية حفظ السجلات، وتجعلها أكثر كفاءة، تسجيل الملكية هو أحد الأمثلة على ذلك، لأنه يكثر فيها الاحتيال، كما أنّها مكلفة وتحتاج إلى عمالة كثيفة لإدارتها.

أطلقت عدة دول مشاريع لتسجيل الملكية باستخدام البلوكشين، هندوراس كانت أول دولة تعلن عن مثل هذه المبادرة في عام ٢٠١٥، كما أبرمت جمهورية جورجيا صفقة مع مجموعة Bitfury لتطوير نظام بلوكشين لتسجيل الملكية، وأعلنت السويد أنها في طور اختبار تطبيق البلوكشين في نظامٍ لتسجيل الملكية.

لقد تبنّت الكثير من البنوك والشركات تقنية البلوكشين لتحويل الأموال والأصول والبيانات، كما دخلت تكنولوجيا البلوكشين في مجالات المال والأعمال، والرعاية الصحية، وسلاسل التوريد، والتأمين والخدمات اللوجستية، ويُتوقّع أنه بحلول عام ٢٠٢٧، فإنّ كل الشركات ستستخدم البلوكشين.

مع وجود العديد من التطبيقات العملية لتكنولوجيا البلوكشين، والتي تُستخدم بالفعل في العديد من القطاعات، فإن مستقبل البلوكشين يبدو واعداً.

تفتح لنا تكنولوجيا البلوكشين عالماً من الاحتمالات، وقد أصبحت الشركات والمؤسسات في كل المجالات، من المالية والطاقة إلى الذكاء الاصطناعي، تستكشف وتبحث عن طرق جديدة ومبتكرة للاستفادة من هذه التكنولوجيا الثورية.

أبرز مجالات تطبيق أنظمة البلوكشين

لقد تخطى استخدام البلوكشين من مجرد الخلفية التقنية التي يقوم عليها عمل نظام البتكوين (Bitcoin) لتبادل العملات الرقمية، إلى نظام يمكن الاستفادة من تطبيقاته العديدة والمتطورة في جميع القطاعات والمجالات العملية والتجارية والصناعية دون استثناء.
وكأمثلة على أبرز المجالات المستفيدة حالياً من البلوكشين هي، حماية "انترنت الأشياء" (IOT)، وتوفير الخدمات والمعاملات الحكومية والمؤسسية، وإدارة سلاسل المداد/التوريد واللوجستيات، وإجراء المعاملات المالية، وفي مجال الرعاية الصحية، وما يخص حفظ حقوق الملكية الفكرية والتوزيع والنشر في المجالات البحثية والأدبية والموسيقى والفنون وغيره.

إنترنت الأشياء

يشكل توفير الحماية الأمنية أحد أهم التحديات الرئيسية في مجال إنترنت الاشياء، خاصة في ظل تزايد التهديدات الإلكترونية وضرورة حماية الأشياء ذاتها وما تصدره وتجمعه من بيانات أثناء عملها، وتوفر تقنية البلوكشين حماية أمنية في عملية التواصل حيث تضمن هوية الأجهزة المرسلة والمستقبلة وفحص بياناتها المجمعة والمصادقة عليها وتسجيل التحديثات والمعاملات التي تتم فيما بينها، على سبيل المثال، إتمام معاملات شحن عدادات الكهرباء المنزلية أو السيارات الكهربائية وغيرها باستخدام العقود الذكية في البلوكشين لفحص بيانات الأجهزة ومصادقتها وتسجيل معاملات الشحن ودفوعاتها المالية بشكل أتوماتيكي وفوري.

الخدمات الحكومية والمؤسسية

يمكن الاستفادة من مزايا البلوكشين وخاصة سرعة المعاملات والشفافية والثقة في توفير وتحسين خدمات القطاع الحكومي والمؤسسات بشكل عام، مثل إصدار المستندات الرسمية بكل أنواعها وأغراضها كشهادات الميلاد والزوج والشهادات الجامعية ورخص القيادة، وتسجيل الملكيات كالأراض ي والعقارات والمركبات المرورية والمجوهرات الثمينة وكل ماله قيمة مادية، وإصدار بطاقات الهوية والتحقق من البيانات، وصرف العانات الحكومية للمستحقين، والتصويت الرقمي في الانتخابات الوطنية وغيرها.

سلاسل المداد/التوريد واللوجستيات

ستلعب أنظمة البلوكشين في السنوات القليلة القادمة دورا حيويا في توسيع العلاقات التجارية وتخطي المعوقات في حركة التجارة العالمية، حيث يجري العمل حاليا على توظيف البلوكشين في إنشاء منصات لوجستية تهدف إلى ربط الموانئ بالأطراف التجارية كالمصانع والشركات والموردين والمصدرين بهدف تسهيل التعاملات بينها وتسريع عمليات تصدير واستيراد السلع، وتمكن هذه المنصات وبشكل خاص الموانئ من معالجة وتتبع معلومات مختلفة لملايين من الحاويات وشحناتها الأسعار والفواتير وتواريخ النتاج وغيره، واعتماد نسخ إلكترونية لمستندات وبوليصات الشحن، ما يلغي التعقيدات الجرائية ويقلل من تكاليف الشحن والتعامل مع الأوراق، بالإضافة إلى زيادة معدلات الأمان والشفافية والحماية من البضائع المزيفة والتلاعب بالأسعار.

المعاملات المالية

يعتبر القطاع المالي أكثر وأسرع القطاعات تأثرا بالبلوكشين وغيرها من التكنولوجيا المالية التي أحدثت تحولات جذرية في هيكلية وأنظمة الخدمات المالية، وتتم الاستفادة حاليا من ميزة اللامركزية في البلوكشين من قبل الأفراد والمؤسسات في خدمات الدفع الفوري وتداول العملات والأصول الرقمية بشكل مباشر وآمن بين الأفراد او الأطراف دون الحاجة لوسيط من السوق المالي أو البنوك، بالضافة إلى استخدام البلوكشين في تنفيذ الحوالات المصرفية وخاصة الخارجية والتسويات مع البنوك والمؤسسات المالية المتراسلة فوريا، ما يختصر الخطوات والمدة الزمنية اللازمة لجراء الحوالات ويخفض تكلفة لنفقات المصاحبة لها.

الرعاية الصحية

يستفاد من البلوكشين في المجال الصحي في إعداد منصة لتسجيل بيانات الرعاية الصحية وفق المعايير والمقاييس الطبية العالمية مع مراعاة خصوصية المرض ى وبياناتهم، وذلك لتوفير المعلومات اللازمة لعمل التحليلات والدراسات والبحوث الصحية، وما يخدم عمل طاقم المستشفيات والمؤسسات المالية والتأمين الصحي والمدادات والأدوية وغيرهم من المخولين على قراءة دفتر سجلات الرعاية الصحية.

حماية الحقوق الفكرية

تتيح تقنية البلوكشين إنشاء منصات لتسجيل وتوثيق أوراق البحوث والدراسات ومجموعات الانتاج الأدبي والفني للكتب والمؤلفات والأفلام والقطع الموسيقية والفنون التصويرية والتشكيلية وغيره، بهدف حماية حقوق الملكية الفكرية والمالية، كاستخدامها في التحقق من مراعاة أحكام وضوابط الاقتباس من المصادر العلمية المنشورة، والتحكم في الانتاج وضمان حقوق النشر والتوزيع في أي من المجالات.

تدريبات الفصل الرابع

س١: اختار الإجابة الصحيحة فيما يلي:

١. .....هي آلية قاعدة بيانات متقدمة تسمح بمشاركة المعلومات الواضحة داخل شبكة الأعمال. ؟

أ. سلسلة الكتل(Blockchain)

ب. البتكوين(Bitcoin)

ج. إنترنت الأشياء(IoT)

د. الحوسبة السحابية(Cloud Computing)

٢. تعد الرعاية الصحية من ..... ؟

أ. تطبيقات تقنية سلسلة الكتل(Blockchain)

ب. مميزات تقنية سلسلة الكتل(Blockchain)

ج. عيوب تقنية سلسلة الكتل(Blockchain)

د. عملات تقنية سلسلة الكتل(Blockchain)

٣. الثبات اللامركزية والتوافق تعد من ..... ؟

أ. تطبيقات تقنية سلسلة الكتل(Blockchain)

ب. مميزات تقنية سلسلة الكتل(Blockchain)

ج. عيوب تقنية سلسلة الكتل(Blockchain)

د. عملات تقنية سلسلة الكتل(Blockchain)

٤. .....هي عملة رقمية لا مركزية لا تتحكم فيها أي سلطة أو بنك مركزي، ويمكن إرسالها من مستخدم إلى آخر دون الحاجة إلى وسطاء ؟

أ. سلسلة الكتل(Blockchain)

ب. البتكوين(Bitcoin)

ج. إنترنت الأشياء(IoT)

د. الحوسبة السحابية(Cloud Computing)

س٢: ضع علامة صح أمام العبارة الصحيحة وعلامة خطأ أمام العبارة الخاطئة

١. تعد حماية الملكية الفكرية من تطبيقات ومجالات تقنية سلسلة الكتل (Blockchain) ( )

٢. في تقنية سلسلة الكتل :(Blockchain) لا يمكن لأي مشارك التلاعب بمعاملة بمجرد قيام شخص ما بتسجيلها في سجل الحسابات المشترك ( )

٣. تنقسم شبكات البلوكشين إلى ثلاثة أنواع وهي: شبكة البلوكشين العامة البلوكشين الخاصة والاتحاد أو التحالف ( )

٤. في تقنية سلسلة الكتل :(Blockchain) يمكنك تسجيل معاملات جديدة بدون موافقة غالبية المشاركين في الشبكة ( )

٥. النقل والخدمات اللوجستية من الأمثلة على حلول الأمان المستندة إلى Blockchain لأنظمة إنترنت الأشياء ( )

حل تدريبات الفصل الرابع

حل السؤال الأول:

١. سلسلة الكتل(Blockchain) (أ)
٢. تطبيقات تقنية سلسلة الكتل(Blockchain) (أ)
٣. مميزات تقنية سلسلة الكتل(Blockchain) (ب)
٤. البتكوين(Bitcoin) (ب)

حل السؤال الثاني:

١. صح
٢. صح
٣. صح
٤. خطأ
٥. صح

أكاديمية التعلم
Academy Of Learning

تحت إشراف
المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

9 2 0 0 0 3 1 3 7

a o l . e d u . s a

aolksa