Sultanate of Oman
Ministry of Transport, Communications
& Information Technology
Minister's Office
Muscat

سلطنة عمان
وزارة النقل والاتصالات وتقنية المعلومات
مكتب الوزير
مسقط

بسم الله الرحمن الرحيم

تعميم رقم (٨ /٢٠٢٢م)

حول الدليل الإسترشادي لإنترنت الأشياء

إستناداً إلى إختصاصات وزارة النقل والاتصالات وتقنية المعلومات الصادرة بالمرسوم السلطاني رقم (٢٠٢٠/٩٠) المتعلقة بالعمل على نقل وتوطين التكنولوجيا المتقدمة في صناعة تقنية المعلومات وتحقيق الإستفادة منها، قامت الوزارة بإعداد هذه الوثيقة بهدف دعم الإبتكار وتحفيز الإنتقال من الحلول التقنية التقليدية إلى النماذج القائمة على إنترنت الأشياء، إلى جانب تبني إطار مرجعي موحد للفئات المستهدفة بسلطنة عُمان لتصميم وتخطيط وتنفيذ حلول إنترنت الأشياء.

عليه، يُرجى من جميع الجهات ذات العلاقة بسلطنة عُمان الأخذ بما ورد في الدليل الإسترشادي (المرفق). ولمزيد من المعلومات يمكن التواصل مع المُختصين في هذه الوزارة من خلال البريد الإلكتروني (governance@mtcit.gov.om)

والله ولي التوفيق ،،،

م. سعيد بن حمود بن سعيد المعولي
وزير النقل والاتصالات وتقنية المعلومات

صدر في : ١٤ شوال ١٤٤٣هـ
الموافق : ١٥ مايو ٢٠٢٢م

س: ١١٨٠

Sultanate of Oman
Ministry of Transport, Communications
& Information Technology
Minister's Office
Muscat

بسم الله الرحمن الرحيم

سلطنة عمان
وزارة النقل والاتصالات وتقنية المعلومات
مكتب الوزير
مسقط

الدليل الإسترشادي لإنترنت الأشياء

مايو ٢٠٢٢م

وزارة النقل والإتصالات وتقنية المعلومات	الدليل الإسترشادي لإنترنت الأشياء	النسخة 1	تاريخ الإصدار أبريل ٢٠٢٢	الصفحة 1

الإصدار والتوزيع:

جهة الإصدار	البريد الإلكتروني	تاريخ الإصدار
المديرية العامة للسياسات والحوكمة وزارة النقل والإتصالات وتقنية المعلومات	Governance@mtcit.gov.om	٢٠٢٢

سجل الوثيقة:

النسخة	التاريخ	جهة الإصدار	الملاحظات
0.1	٢٠٢٢	وزارة النقل والإتصالات وتقنية المعلومات	

قائمة النشر:	
١.	جميع وحدات الجهاز الإداري للدولة
٢.	الموقع الإلكتروني للوزارة

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050

ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

جدول المحتويات

١. المقدمة :

يتكون إنترنت الأشـــياء من مليارات الأشـــياء (الأجهزة) المتصـــلة مع بعضـــها البعض عبر بروتوكول الإنترنت، مثل أجهزة الإستشعار والحساسات وأدوات الذكاء الإصطناعي وغيرها من الوحدات التي تستخدم التكنولوجيا اللاسلكية للإتصال بالإنترنت، والتي أحدثت تحولاً جذرياً في نماذج الاتصال والتواصل وتطوير الحلول الإبتكارية.

إلا أن نشـــر وإســـتخدام أجهزة إنترنت الأشـــياء الغير محمية في كل مكان قد يجعلها عرضـــة بشـــكل متزايد للهجمات الســـيبرانية والجرائم الإلكترونية، الأمر الذي قد يهدد أمن البيانات أو يعرض خصـــوصـــية مالكيها للخطر، حيث يعد أمن إنترنت الأشـــياء معقداً كونه يتضـــمن مجموعة كبيرة من المهام مثل تضمين البيانات اللازمة للتشفير أثناء عمليات تصنيع الجهاز، و توفير بيانات تشفير جديدة أثناء التشغيل، ووضع سياسات التحكم للوصول الى الخدمات والشـــبكات، وتأمين عمليات تطوير البرمجيات، ونشـــر وحدات أمان الأجهزة و إدارة عمليات تطوير البرامج.

عليه إرتأت وزارة النقل والاتصـــالات وتقنية المعلومات تبني نموذج مرجعي موحد للفئات المســـتهدفة بســـلطنة عُمان لتصـــميم وتخطيط وتنفيذ حلول إنترنت الأشـــياء، حيث يمكن إســـتخدام هذا الدليل الإســـترشـــادي من قبل هذه الفئات لتطوير حلول آمنة واتباع أفضـــل الممارسات في تخطيط وتنفيذ مشاريع حلول إنترنت الأشياء.

٢. التعاريف والمصطلحات :

الوزارة: وزارة النقل والاتصالات وتقنية المعلومات.

الهيئة : هيئة تنظيم الإتصالات .

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

مزود الخدمة : الشخص الطبيعي أو المعنوي الذي حصل على ترخيص لتقديم خدمات إنترنت الأشياء.

إنترنت الأشـــياء: مجموعة من الأجهزة القابلة للعنونة في بروتوكول الإنترنت التي تتفاعل مع البيئة المادية، والتي عادة ما تحتوي على عناصـــر للإســـتشـــعار والتواصـــل والمعالجة والتشغيل.

منظومة إنترنت الأشياء: جميع الأشياء والأجهزة والمعدات والبرمجيات والتطبيقات بما فيها أجهزة المراقبـة والتحكم وأجهزة ووســـائـل معـالجـة وتخزين البيـانـات وأجهزة المرســـلات والمستقبلات وأية معدات مساعدة.

الشـــئ " الأشـــياء " : هو جهاز من العالم المادي (أشـــياء مادية) أو تطبيق عن عالم المعلومات (أشـــياء افتراضـــية) ، يتســـم بإمكانية دمجه في شـــبكات الإتصـــالات ويحتوي عادة على البرمجيات وإمكانية الاتصال بشبكات الاتصالات وتقنية المعلومات، والقدرة على جمع ونقل البيانات عبر شـبكات الاتصـالات من خلال تقنيات مضـمنة فيه تسـاعد على تفعيل أنظمته الداخليه والتواصل مع البيئة الخارجية.

المستخدم: هو مستخدم تطبيقات إنترنت الأشياء المقدمة من قبل مزود الخدمة.

معرفات إنترنت الأشـــياء: هي مجموعة أرقام أو رموز تســـتخدم لتعريف الأشـــياء لتســـهيل الوصول إليها، وتستخدم معرفات الاتصال لتحديد نقاط النهاية (المصدر والوجهة النهائية) .

إطار النوذج المرجعي لإنترنت الأشـــياء : مخطط عريض لنظام أو حل لإنترنت الأشـــياء (IoT) البيئي، والذي يعمل كدليل مرجعي لتمكين الجهات الفاعلة من إستخدام لغة مشتركة وهيكل متعدد الطبقات لمناقشة الجوانب المتعلقة بالنظام مثل الأمان والخصوصية.

٣. الأهداف :

١. دعم الإبتكار وتحفيز الإنتقال من الحلول التقنية التقليدية إلى النماذج القائمة على إنترنت الأشياء.

٢. توفير إطار واضح لتطوير حلول إنترنت الأشياء في سلطنو عُمان.
٣. توجيه الفئات التي يغطيها نطاق تطبيق هذه الدليل إلى النظر في النموذج المرجعي لإنترنت الأشياء كنموذج أساسي عند اتخاذ قرارات إستثمار جديدة في إنترنت الأشياء.
٤. المساهمة في تعزيز نمو السوق المحلي في تقديم الحلول القائمة على إنترنت الأشياء وتعزيز مشاركته في السوق الإقليمي والعالمي.
٥. توفير الآليات التي تضمن توفير الإستخدام الآمن لخدمات إنترنت الأشياء.

٤. الغرض :

تبني نموذج مرجعي موحد للفئات المستهدفة بسلطنة عُمان لتصميم وتخطيط وتنفيذ حلول إنترنت الأشياء، و تشجيع الإبتكار بإستخدام حلول إنترنت الأشياء.

٥. النطاق :

ينطبق هذا الدليل على جميع المعنيين بإنترنت الأشياء داخل سلطنة عُمان بما في ذلك على سبيل المثال وليس الحصر:

- مزودي خدمات الاتصالات.
- مزودي خدمات إنترنت الأشياء.
- مطوري حلول وأجهزة إنترنت الأشياء.
- مزودي أجهزة وأنظمة إنترنت الأشياء.
- مستخدمي إنترنت الأشياء (الأفراد، الشركات ، وحدات الجهاز الإداري للدولة).

٦. الدليل الإسترشادي لإنترنت الأشياء :

٦.١ النموذج المرجعي لأنترنت الأشياء :

يتضمن النموذج المرجعي لإنترنت الأشياء من جميع المكونات التي تمكن الشركات، الحكومات والمستخدمين من الإتصال بأجهزتهم الخاصة المتصلة بإنترنت الأشياء، ويتكون من أربع طبقات إلى جانب قدرات الإدارة و القدرات الأمنية التي ترتبط بهذه الطبقات وهي كالتالي:

الطبقة المادية: وهي تشمل الأجهزة التي تشكّل جهاز إنترنت الأشياء، بما في ذلك أجهزة الإستشعار ومعدات الشبكات.

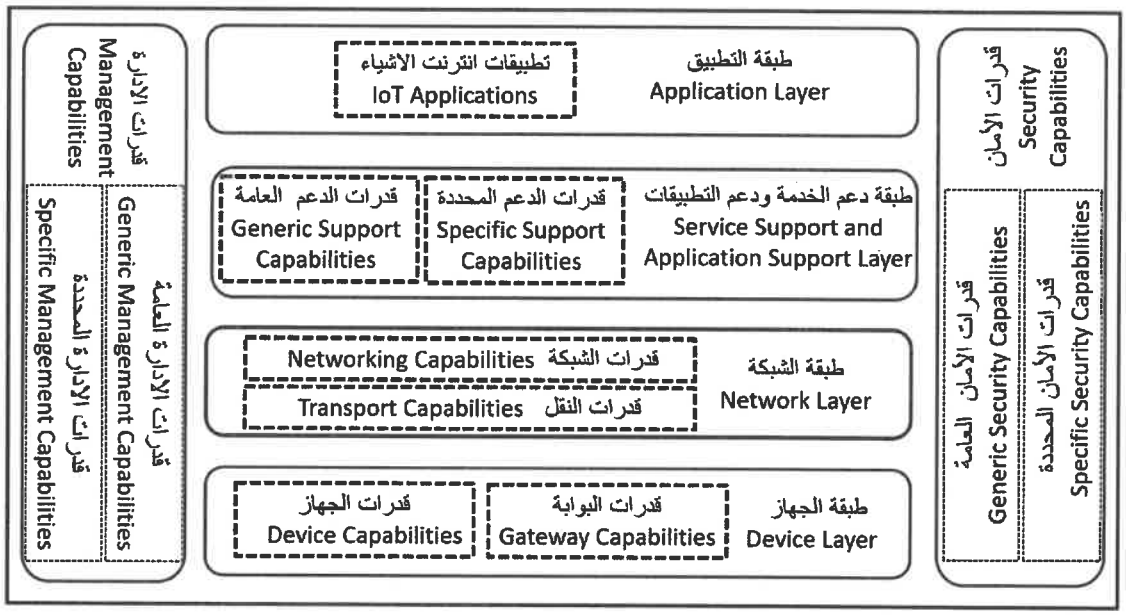
طبقة الشبكة: وهي مسؤولةٌ عن نقل البيانات التي تجمعها الطبقة المادية إلى أجهزةٍ مختلفةٍ.

طبقة التطبيقات: ويشمل ذلك البروتوكولات والواجهات التي تستخدمها الأجهزة للتعرف والتواصل مع بعضها البعض.

طبقة دعم الخدمة و ودعم التطبيقات : وتتضمن أجهزة التحكم عن بعد والتي تُمكن الاجهزة المستخدمة من إستقبال الأوامر وغيرها من البيانات عن طريق لوحة التحكم التى تعرض المعلومات عن البيئة المحيطة بالمستخدم وتتيح للجهاز التحكم فيها ومن ثم تعرض كل تلك البيانات للتحليل من قبل أنظمة برمجية مخصصة قبل حفظها، وفيما يلي شرح مفصل لكل طبقة من هذه الطبقات وفقاً للنموذج المرجعي المعتد به من قبل الإتحاد الدولي للاتصالات.

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050

ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠



النموذج المرجعي لأنترنت الأشياء

(المصدر: الإتحاد الدولي للاتصالات)

طبقة التطبيق (Application Layer) : تحتوي على تطبيقات إنترنت الأشياء.

طبقة دعم الخدمة و دعم التطبيقات (Service support and Application Support layer) :

تتضمن نوعين من القدرات :

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

- **قدرات الدعم العامة (Generic Support Capabilities)** : هي قدرات عامة من الممكن استخدامها مع تطبيقات مختلفة من تطبيقات إنترنت الأشياء مثل معالجة البيانات وتخزينها كما بإلامكان إستخدامها إذا إستدعت الحاجة مع قدرات الدعم المحددة على سبيل المثال عند بناء قدرات دعم محددة إضافية .
- **قدرات الدعم المحددة (Specific Support Capabilities)** : هي قدرات تلبي متطلبات التنوع في التطبيقات بهدف توفير الدعم لمختلف تطبيقات إنترنت الأشياء.

طبقة الشبكة (Network Layer) : تتضمن الطبقة نوعين من القدرات كالتالي:

- **قدرات الشبكة** : توفر وظيفة التحكم ذات الصلة بتوصيل الشبكة (**Network Connectivity**) مثل وظائف التحكم في موارد الوصول والنقل ، والإدارة أو المصادقة ، والتفويض والمحاسبة .
- **قدرات النقل** : توفر وظيفة التوصيل ذات العلاقة بنقل خدمة إنترنت الاشياء ومعلومات البيانات الخاصة بالتطبيق إلى جانب معلومات التحكم والإدارة الخاصة إنترنت الأشياء.

طبقة الجهاز (Device Layer) : تصنف عملياً إلى نوعين من القدرات تشمل قدرات الجهاز (**Device Capabilities**) و قدرات البوابة (**Gateway Capabilities**) كالتالي :

- **قدرات الجهاز(Device Capabilities)**: قد تتضمن على سبيل المثال الإمكانيات التالية:

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

- التفاعل المباشر مع شبكة الإتصال: تستطيع الأجهزة جمع وتحميل البيانات بشكل مباشر إلى شبكة الإتصال (من غير إستخدام قدرات البوابة) ويمكن أن تتلقى المعلومات مباشرة من شبكة الإتصال.
- التفاعل الغير مباشر مع شبكة الاتصال: الأجهزة تستطيع جمع وتحميل البيانات بشكل غير مباشر الى شبكة الاتصال عبر قدرات البوابة، في المقابل تستطيع الأجهزة بشكل غير مباشر من تلقي المعلومات من شبكة الاتصال.
- شبكات مخصصة: قد تكون الأجهزة قادرة على بناء شبكات على طريقة الشبكات المخصصة في بعض السيناريوهات التي تحتاج زيادة في قابلية التوسع وسرعة النشر.
- حفظ الطاقة: قد تدعم إمكانات الجهاز "السكون" وآليات "الاستيقاظ" لتوفير الطاقة.

- قدرات البوابة (Gateway Capabilities) : لا تعد بوابات إنترنت الأشياء ضرورية دائمًا، إعتمادًا على نوع تقنية الاتصال و / أو أنواع الأجهزة المستخدمة ، حيث ستتصل بعض الأجهزة مباشرةً بمنصة إنترنت الأشياء.

تُستخدم البوابات لعدد من الأغراض مثل:

- **دعم واجهات متعددة :** في طبقة الجهاز تدعم قدرات البوابة الأجهزة المتصلة من خلال أنواع مختلفة من التقنيات السلكية واللاسلكية مثل (Controller Area Network) و (Bluetooth) و (Wi-Fi)، في حين في طبقة الشبكة تستطيع قدرات البوابة الاتصال عبر تقنيات مختلفة مثل شبكة الهاتف العامة (PSTN) وشبكات الجيل الثاني، والجيل الثالث، والجيل الرابع، والجيل الخامس (2G, 3G, 4G,5G) أو الشبكات طويلة المدى (LTE) أو Ethernet أو خطوط المشترك الرقمية (DSL)، وشبكات الاتصال عبر الأقمار الإصطناعية (VSAT).

- **تحويل البروتوكولات :** يصبح وجود قدرات البوابة ضروري في حالتين:

الحالة الاولى: الاتصـــالات في طبقة الجهاز تســـتخدم بروتوكولات مختلفة لطبقة الجهاز.

الحالة الثانية : الاتصالات التي تتضمن طبقة الجهاز وطبقة الشبكة تستخدم بروتوكولات مختلفة.

قدرات الإدارة (Management Capabilities): بطريقة مماثلة لشـــبكات الاتصـــال التقليدية، تغطي قدرات إدارة إنترنت الأشـــياء فئات منها: الأخطاء التقليدية والتكوين والمحاســـبة والأداء والأمن (FCAPS)، أي إدارة الأعطال وإدارة التكوين وإدارة المحاســـبة وإدارة الأداء وإدارة الأمن، وتصـــنف الى قدرات ادارة عامة (Generic Management Capabilities) وقدرات إدارة محددة (Specific Management Capabilities).

قدرات الإدارة العامة : تشمل قدرات الإدارة العامة الأساسية في إنترنت الأشياء ما يلي:

- إدارة الجهاز ، مثل تنشـــيط الجهاز عن بُعد وإلغاء التنشـــيط والتشـــخيص والبرامج الثابتة و / أو تحديث البرامج وإدارة حالة عمل الجهاز.
- إدارة مكونات الشبكة المحلية (Local Network Topology).
- إدارة حركة المرور والازدحام (Traffic and congestion management) مثل الكشف عن حالة تجاوز الشبكة وحجز الموارد لتدفق البيانات الحرجة.
- قدرات الإدارة المحددة: ترتبط قدرات الإدارة المحددة ارتباطًا وثيقًا بالمتطلبات الخاصة بالتطبيق، على سبيل المثال، متطلبات مراقبة خط نقل طاقة الشبكة الذكية.

القدرات الأمنية: (Security Capabilities) يوجد نوعين من القدرات الأمنية تشمل قدرات أمنية عامة (Generic Security Capabilities) وقدرات أمنية محددة (Specific Security Capabilities).

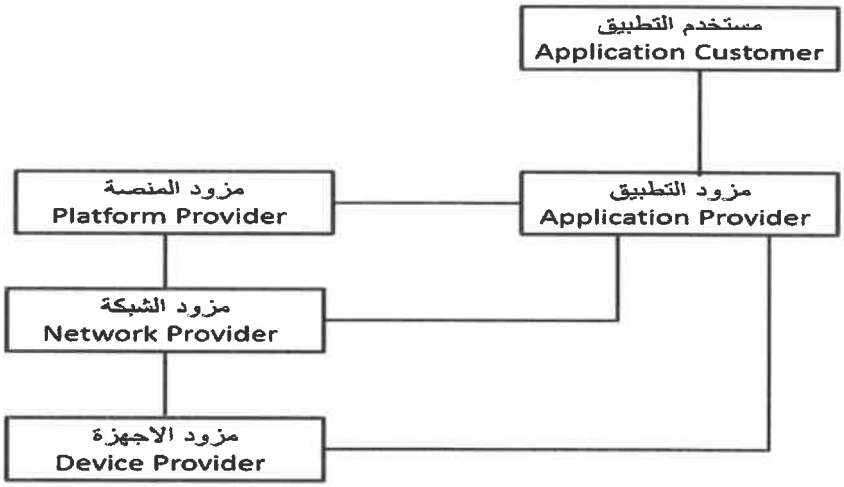
قدرات الأمان العامة (Generic Security Capabilities) مستقلة عن التطبيقات وتشمل:

- في طبقة التطبيق: التفويض والمصادقة وسرية بيانات التطبيق وحماية سلامتها وحماية الخصوصية والتدقيق الأمني ومكافحة الفيروسات.
- في طبقة الشبكة: التفويض والمصادقة، سرية بيانات الإشارة و استخدام البيانات (Use data and Signaling data confidentiality) و حماية سلامة الإشارة (Signaling integrity protection).
- في طبقة الجهاز: المصادقة، التفويض، التحقق من سلامة الجهاز، التحكم في صلاحية الوصول، وسرية البيانات وحماية سلامتها.

قدرات الأمان المحددة (Specific Security Capabilities): ترتبط إمكانات الأمان المحددة إرتباطًا وثيقًا بالمتطلبات الخاصة بالتطبيقات، مثل الدفع عبر الهاتف المحمول ومتطلبات الأمان.

٦.٢ النظام البيئي لإنترنت الأشياء (IoT ecosystem):

يضم نظام إنترنت الأشياء مجموعة متنوعة من أصحاب المصلحة ، يؤدي كل صاحب مصلحة دور واحد على الأقل وبالإمكان أن يقوم بأكثر من دور حسب نموذج العمل كما يتضح من النظام البيئي لإنترنت الأشياء أدناه:



النظام البيئي لإنترنت الأشياء (IoT ecosystem)

(المصدر: الإتحاد الدولي للاتصالات)

مزود الجهاز (Device Provider) : يكون مزود الجهاز مسؤولاً عن الأجهزة التي توفر البيانات الأولية و / أو المحتوى لمزود الشبكة ومزود التطبيق وفقًا لنوع الخدمة، والتي قد تشمل بدءًا من المستشعرات البسيطة، إلى الأجهزة المستقلة الأكثر تعقيدًا مثل أجهزة التتبع، والعدادات الذكي، وما إلى ذلك، إلى الأجهزة المضمنة في الأنظمة المعقدة مثل تلك الموجودة في أنظمة التحكم، والمركبات ذاتية القيادة، وما إلى ذلك.

مزود الشبكة (Network Provider) : يقوم بدور أساسي في النظام البيئي لإنترنت الأشياء، حيث يؤدي الوظائف الرئيسية التالية:

- الوصول إلى الموارد التي يوفرها مزودي الخدمات الآخرون وتكاملها.
- دعم البنية الأساسية لقدرات إنترنت الأشياء والتحكم فيها.

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

- عرض إمكانيات إنترنت الأشياء، بما في ذلك قدرات الشبكة والتعرض للموارد لمزودين آخرين.

مزود المنصة (Platform Provider): أحد أهم جوانب حل إنترنت الأشياء هو قدرة المؤسسة على "تشغيل وإدارة" حلول وأجهزة إنترنت الأشياء الخاصة بها من خلال مجموعة متنوعة من الأنشطة بما في ذلك: إدارة اتصال الجهاز، وتخزين البيانات ومعالجتها، ومراقبة الأحداث ومعالجتها، والتحليلات وواجهات الأنظمة الخارجية.
نظرًا لأن تعريف منصة إنترنت الأشياء يمكن أن يعني العديد من الأشياء المختلفة في سياقات مختلفة، فإن هذا الإطار يفصل "منصة إنترنت الأشياء" إلى ثلاث أجزاء كالتالي:

- **تمكين التطبيق:** مجموعة من الوظائف التي غالبًا ما يتم تجميعها تحت مصطلح انترنت الاشياء الأساسي الشامل ، وتستخدم لوصف العديد من وظائف إنترنت الأشياء الأساسية بما في ذلك: بوابة التكامل API ، وتخزين قاعدة البيانات ، والتصور، وإدارة الجهاز، وخادم التطبيقات وغيرها.
- **تمكين الذكاء:** يشير إلى إستخدام التقنيات (الناشئة) مثل التحليلات والذكاء الإصطناعي (AI) والتعلم الآلي (ML) والتعلم العميق (DL) الذي يضيف قيمة من خلال التحليل الذكي لكمية هائلة من البيانات التي يتم جمعها من أجهزة إنترنت الأشياء وغيرها من الأجهزة الخارجية.
- **إدارة الاتصال :** تشير إدارة الاتصال إلى الوظائف التي تدير اتصالات الأجهزة وهوية الجهاز وتكوين الجهاز.

مزود التطبيق (Application Provider): يستخدم مزود التطبيق القدرات أو الموارد التي يوفرها مزود الشبكة ومزود الجهاز ومزود المنصة، من أجل توفير تطبيقات إنترنت الأشياء

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

لعملاء التطبيق، حيث يمثل العلاقة بين مالك / مشغل حلول إنترنت الأشياء وأصحاب المصلحة الذين يقدمون خدمات أو منتجات لهذه الحلول.

مستخدم التطبيق (Application Customer): هو مستخدم تطبيقات إنترنت الأشياء المقدمة من قبل مزود التطبيقات، حيث يمكن أن يحتوي حل إنترنت الأشياء على أنواع متعددة من المستخدمين ، ويمكن أن يكون لكل نوع من المستخدمين متطلبات إستخدام أو إستهلاك مختلفة.

٦,٣ اطار أمن إنترنت الأشياء:

يقدم هذا الإطار المتطلبات العالية المستوى المتعلقة بالأمن والخصوصية حسب توصية الإتحاد الدولي للاتصالات رقم (ITU-T X.١٣٦١) وهي كالتالي:

أمن الاتصالات:

توفر قدرة للاتصالات الآمنة والموثوقة ومحمية الخصوصية بهدف حظر كل نفاذ غير مرخص به إلى محتوى البيانات، ولكي يتسنى ضمان سلامة البيانات وحماية محتويات البيانات المتعلقة بالخصوصية أثناء إرسال البيانات أو نقلها في تقنية إنترنت الأشياء.

أمن إدارة البيانات:

توفر قدرة لإدارة البيانات الآمنة والموثوقة ومحمية الخصوصية لكي يُحظر كل نفاذ غير مرخص به إلى محتوى البيانات، ولكي يتسنى ضمان سلامة البيانات وحماية محتويات البيانات المتعلقة بالخصوصية أثناء تخزين البيانات أو معالجتها في تقنية إنترنت الأشياء.

أمن توفير الخدمات :

توفير قدرة لتوفير الخدمة الآمنة والموثوقة والمحمية الخصوصية لكي يُحظر كل نفاذ غير مرخص به إلى الخدمة وتقديم الخدمات الاحتيالية، ولكي يتسنى حماية المعلومات المتعلقة بخصوصية مستعملي إنترنت الأشياء.

تكامل السياسات والتقنيات الأمنية:

توفر القدرة على دمج مختلف السياسات والتقنيات الأمنية، لكي يتسنى ضمان التزامن في المراقبة الأمنية على مجموعة متنوعة من الأجهزة وشبكات المستعملين في إنترنت الأشياء.

التحقق والتخويل المتبادل :

قبل أن يتمكن أي جهاز / أو مستعمل لإنترنت الأشياء من النفاذ إلى إنترنت الأشياء، يتطلب إجراء التحقق وتخويل متبادل بين الجهاز أو مستعمل إنترنت الأشياء وفقاً للسياسات الأمنية المحددة سلفا.

التدقيق الأمني:

توفر قدرة لدعم التدقيق الأمني في إنترنت الأشياء ،بحيث يتسم كل نفاذ إلى البيانات أو محاولة النفاذ إلى تطبيقات إنترنت الأشياء بالشفافية وإمكانية التتبع بشكل كامل وفقاً للوائح والقوانين ذات الصلة. وبوجه خاص يلزم أن تدعم تقنية إنترنت الأشياء التدقيق الأمني لأغراض إرسال البيانات وتخزينها ومعالجتها والنفاذ إلى التطبيقات.

٦،٤ الإلتزامات والحقوق:

الإلتزامات العامة :

١. التقيد بكافة القوانيين والأنظمة السارية المفعول في سلطنة عُمان كسياسة الحوسبة السحابية، قانون مكافحة جرائم تقنية المعلومات.
٢. الحفاظ على سرية بيانات الخدمة الخاصة بالمستفيد وعدم الإفصاح عن تلك البيانات إلا بموافقة مسبقة من قبل المستخدم أو بناءاً على طلب رسمي من الجهات القضائية أو الجهات المصرح لها.
٣. الحصول على الموافقات الفنية اللازمة لجميع الأجهزة والأنظمة والوحدات المقرر إستخدامها قبل تشغيلها وفقاً للتعليمات والإجراءات المتبعة لدى هيئة تنظيم الاتصالات
٤. الإلتزام بأي إجراءات / قرارات تنظيمية معتمدة من قبل الجهات المعنية المتعلقة بإستخدام معرفات انترنت الأشياء مثل عناوين بروتوكول الإنترنت (IPv4/IPv6) أو أي معرفات أخرى مثل (MAC address).

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

٥. الإلتزام بتوفير الخوادم (servers) المستخدمة لتقديم خدمات إنترنت الأشياء داخل سلطنة عُمان وتخزين البيانات فيها.
٦. الإلتزام بتوفير الإمكانيات الفنية في أجهزة ومعدات شبكات إنترنت الأشياء لحفظ البيانات للرجوع اليها عند الحاجة وذلك لمدة لا تقل عن أثنى عشر شهراً أو حسب ما تقرره الجهات المصرح لها بهذا الشأن.
٧. الإلتزام بالإجراءات / القرارات التنظيمية المنشورة أو المستقبلية الصادرة عن الجهات المعنية في سلطنة عُمان المتعلقة بإدارة البيانات ، أمن الشبكات وأمن وخصوصية بيانات المستخدمين.
٨. الإلتزام بما يستجد على الخطط الوطنية الخاصة بالترقيم واستخدام الموارد النادرة والمواصفات الفنية في سلطنةعُمان لمواكبة المستجدات في قطاع الاتصالات وتقنية المعلومات مع الأخذ في الحسبان التوصيات الصادرة من المنظمات الدولية ذات العلاقة.

إلتزامات مزود الخدمة:

١. الحصول على رخصة تقديم خدمات إنترنت الأشياء لدى الجهات المعنية في سلطنة عُمان قبل البدء بتقديم الخدمة.
٢. اشعار صاحب البيانات بالطرق والوسائل لجمع ومعالجة ومشاركة بياناته وكذلك التدابير الأمنية لضمان خصوصية البيانات حسب الأنظمة واللوائح والسياسات المعمول بها في سلطنة عُمان.
٣. اشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات انفاذ القانون والمجتمع المدني).
٤. أن يكون جمع/ معالجة / مشاركة البيانات مقتصراً على الحد الأدنى من البيانات لتحقيق الغرض الذي قدم صاحب البيانات موافقته الضمنية أو الصريحة.

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

٥. أن يقتصر إستخدام البيانات على الغرض الذي جمعت من أجله.
٦. إعداد وتوثيق سياسات واجراءات الاحتفاظ بالبيانات وفقاً للسياسات واللوائح المعمول بها.
٧. الإلتزام بتخزين البيانات ومعالجتها داخل الحدود الجغرافية لسلطنة عُمان لضمان المحافظة على السيادة الرقمية للبيانات الوطنية ولا يجوز معالجتها أو تخزينها إلا بعد الحصول على موافقة الجهات المختصة.
٨. وضع خطة واضحة لإدارة البيانات تتضمن (آلية جمع البيانات/إلية تحليل البيانات / آلية تصنيف البيانات / النشر والمشاركة / الإستخدام / حماية البيانات / ملكية البيانات/ الإحتفاظ بالبيانات / إتلاف البيانات).
٩. بناء أنظمة الأمن ودعم الخصوصية كجزء أساسي ورئيسي عند تصميم منظومة إنترنت الأشياء والتأكد من توافرها وتوافق الأجهزة المستخدمة بها.
١٠. تحديد أنواع المخاطر الأمنية عالية المستوى على المنظومة والتي تستوجب تطبيق أسس حماية عالية واتخاذ تدابير أمنية نحوها بمستويات مختلفة.
١١. إتخاذ كافة التدابير الأمنية لمراقبةوالحد من الوصول غير المصرح له من قبل شخص / أشخاص / جهات إلى أنظمة وبيانات المستخدم.

حقوق صاحب البيانات:

- الحق في الحصول على موافقته على معالجة البيانات ما لم يكن هناك أغراض مشروعة تتطلب عكس ذلك.
- الحق في الوصول إلى بياناته لدى مزود الخدمة وذلك للإطلاع عليها وطلب تعديلها أو تحديثها وطلب اتلاف البيانات التي إنتهت الحاجة إليها والحصول على نسخة منها.

٧. **الإدارة :**

١. تعود ملكية هذا الدليل إلى وزارة النقل والاتصالات وتقنية المعلومات وسيخضع للمراجعة كلما اقتضت الحاجة ذلك.

٢. يدخل الدليل حيز التطبيق إعتبارا من تاريخ إعتماده وتعميمه من وزارة النقل والاتصالات وتقنية المعلومات.

٨. **الإصدارات ذات الصلة:**

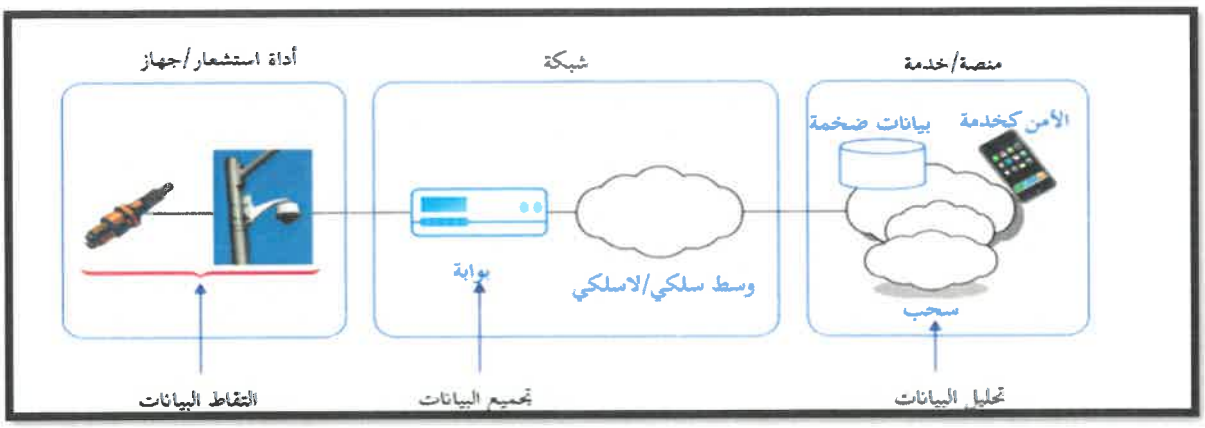
١. الإطار الأمني لإنترنت الأشياء القائم على نموذج البوابة الإتحاد الدولي للاتصالات (٢٠١٨).
٢. إطار عمل التوافق الأمني لإنترنت الأشياء للإتحاد الأوروبي (٢٠١٦).
٣. الإطار المرجعي لإنترنت الأشياء – استراليا (٢٠١٨).
٤. الإطار التنظيمي لإنترنت الأشياء للاتحاد الدولي للاتصالات (٢٠١٧) .
٥. إطار عمل الحكومات الذكية للانترنت الأشياء (دراسة سياسات الأمن السيبراني لإنترنت الأشياء في الحكومة الفيدرالية الأمريكية (٢٠٢٠).
٦. سياسة إنترنت الأشياء – الجمهورية الهندية (٢٠١٨).
٧. مشاورات العموم الخاصة بإنترنت الأشياء – هيئة تنظيم الاتصالات سلطنة عمان (٢٠٢٠).
٨. الإطار التنظيمي لإنترنت الأشياء – هيئة تنظيم الاتصالات السعودية (٢٠١٩).
٩. متطلبات منظومة إنترنت الأشياء – هيئة تنظيم الاتصالات الأردنية (٢٠٢١).

إنتهى،،،،

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي – الرمز البريدي: ١١٢ – هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

ملحق (١)

بعض التهديدات الأمنية التي تواجه إنترنت الأشياء



المعمارية الوظيفية لإنترنت الأشياء

(المصدر: الإتحاد الدولي للاتصالات)

التهديدات التي تصيب أدوات الاستشعار / أجهزة انترنت الأشياء :

- **الإستيلاء على الجهاز: يشير الى الإنتهاك المادي لجهاز أو فقدانه لمفاتيحه.**
- **هجمة الثقب الأسود (Sinkhole) : يضع الشخص الدخيل جهازاً مزيفاً داخل الشبكة بحيث يجتذب جميع حركة البيانات عن طريق إرسال معلومات تسيير مزيفة إلى الأجهزة المجاورة لجذب حركة الشبكة إليه.**
- **الهجمات بهويات مزورة (Sybil): ينتحل فيها جهاز خبيث هويات متعددة بصورة غير مشروعة وتعرف الهوية الإضافية للجهاز الخبيث بعقدة الهوية المزوره وتشن هذه الهجمة بالاقتران مع هجمات أخرى للحد من فعالية آليات تحمل الأعطال.**
- **هجوم الإغراق: هو شكل من هجمات رفض الخدمة (DoS) يرسل فيها المهاجم سلسلة متعاقبة من رزم (hello) إلى الجهاز المستهدف في محاولة لإستهلاك قدر كاف من موارد الجهاز لجعل الجهاز لا يستجيب للحركة المشروعة.**

- هجمة الثقب الدودي (Wormhole): يحدث في المسار البيني (مسار البيانات بين جهازين على بنية شبكية قائمة) حيث تحصل الشبكة التي تمرر البيانات إلى شبكة أخرى على البيانات من شبكة ما وتستنسخها في شبكة أخرى من خلال المسار البيني وقد يختلط الأمر على تلك الشبكة بعينها بسبب هذا الإجراء.
- إنتحال هوية أداة الاستشعار/ الجهاز: تحدث هذه الهجمة عندما ينجح مهاجم في إنتحال هوية إدارة استشعار مشروعة / جهاز مشروع.

التهديدات التي تواجه بوابات انترنت الأشياء:

- **النفاذ غير المرخص به :** قد يتسبب في إفشاء معلومات حساسة، وتغيير البيانات، ورفض الخدمة والإستخدام غير المشروع للموارد، على سبيل المثال نفاذ مهاجم الي بوابة يمكن أن يؤدي إلى رصد البيانات غير المشفرة مثل أسماء المنتفعين وكلمات المرور.
- **البوابة الإحتيالية:** حتى وإن كانت جميع البوابات اللاسلكية آمنه فمن السهل على المهاجمين أن يطلقوا بوابة إحتيالية خاصة بهم، فمثلاً للمهاجم تثبيت نقطة نفاذ لا سلكية احتيالية بصوره مقصودة وسرية لتمكين مهاجم أخر من النفاذ بسهولة إلى الشبكة سواءا محليا أو عن بعد لإستبدال نقطة النفاذ اللاسلكية بنقطة أخرى يمكن تشكيلها ومراقبة النفاذ اليها بشكل كامل أو حتى تشكيل نقطة نفاذ لاسلكية احتيالية بإعدادات مماثلة، ولكن بنسبة أعلى من القدرة اللازمة للتغلب على إشارة نقطة النفاذ اللاسلكية المشروعة.
- **هجمة رفض الخدمة :** تكون أجهزة الإستشعار اللاسلكية معرضه بوجه خاص لهجمات رفض الخدمة بسبب سماتها التي تشمل الوسط المفتوح ومكونات الشبكة المتغيرة.

التهديدات الامنية التي تواجه الشبكة :

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050
ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

- **النفاذ غير المرخص به:** يمكن أن يتسبب النفاذ غير المرخص به إلي شبكة استشعار لاسلكية في الكشف عن معلومات حساسة وتغيير البيانات ورفض الخدمة والاستخدام غير المشروع للموارد، على سبيل المثال يستطيع المهاجم أن يرصد البيانات غير المشفرة مثل أسماء المنتفعين وكلمات المرور الخاصة بهم من عبر النفاذ إلى شبكة من شبكات الإستشعار.
- **إستشفاف الرزم :** في شبكات الاستشعار اللاسلكية الغير مزودة بقدرات التشفير من السهل على المهاجم التنصت على اتصالات الشبكة، وجهاز إستشفاف رزم الشبكة هو اداة تضبط بطاقة الشبكة على " الأسلوب المشوش" ويعني ذلك أن السطح البيني سيتقبل ويعالج كل الحركة وليس فقط الحركة الموجهه إليها.
- **سطو ببلوتوث (bluejacking):** هذه النوع من الهجمات تستهدف الأجهزة المتنقلة المزودة بإمكانية البلوتوث مثل الهواتف الخلوية ويبدأ فيها المهاجم بإرسال رسائل غير مرغوب بها الى مستعملي الأجهزة المزودة بخاصية البلوتوث بهدف إستدراج المنتفع إلى الرد بصورة ما أو إضافة بيانات اتصال جديدة الى مجلد عناوين الجهاز.
- **إلتهام ببلوتوث (Bluesnarfing) :** يقصد به النفاذ الغير مرخص به إلى المعلومات من جهاز لاسلكي مستهدف عن طريق توصيل بلوتوث ويحدث غالبا بين الهواتف أو الحواسيب المكتبية أو الحواسيب المحمولة أو المساعدات الرقمية الشخصية (PDA).

التهديدات التي تواجه المنصة / الخدمات :

تكون المهمة الرئيسية لطبقة التطبيقات هي جمع ومعالجة عدد كبير من بيانات المنتفعين بما فيها المعلومات الشخصية للمنتفعين أو المعاملات السرية لمختلف المعاملات وهذه البيانات

P.O. Box : 338 Ruwi, Postal Code : 112 ,Tel. : 24685550/24685552, Fax : 24685050 ص.ب : ٣٣٨ روي - الرمز البريدي: ١١٢ - هاتف : ٢٤٦٨٥٥٥٠/٢٤٦٨٥٥٥٢، فاكس : ٢٤٦٨٥٠٥٠

التهديدات التي تواجه المنصة / الخدمات :

تكون المهمة الرئيسية لطبقة التطبيقات هي جمع ومعالجة عدد كبير من بيانات المنتفعين بما فيها المعلومات الشخصية للمنتفعين أو المعاملات السرية لمختلف المعاملات وهذه البيانات هي الهدف الرئيسي للمهاجم بغرض سرقتها أو العبث بها أو إتلافها ومن الضروري حماية البيانات عبر إستعمال آليات حماية الخصوصية وتشمل التهديدات التي تواجه طبقة التطبيقات معالجة البيانات الضخمة، الأجهزة الذكية الخارجة عن السيطرة، والتدخل البشري غير المرخص به وعدم قدرة الاجهزة المستهدفة على التعافي من الكوارث.

التهديدات الخاصة التي تواجه المنصات / الخدمات:

- **تحديد المواصفات :** عملية إستكشافية تستخدم لجمع معلومات عن المنصة / الخدمات.
- **رفض الخدمة:** هجمة تصبح فيها المنصة/ الخدمة مشغولة بطلبات كثيفة على الخدمة لدرجة يتعذر فيها الإستجابة لطلبات المنتفعين.
- **تنفيذ شفرة خبيثة:** تتم في أي جزء من نظام البرمجيات أو نص الغرض منه إحداث تأثيرات غير مرغوب بها إنتهاكات للأمن أو للمعلومات المحددة لهوية الشخص أو الإضرار بنظام.
- **التنصت على الشبكة:** هجمة تلتقط الرزم المرسلة من الشبكة وتقرأ محتوى البيانات بحثاً عن المعلومات المهمة مثل كلمات المرور.
- **هجمة بالتخمين:** تحدث هذه الهجمة كلما تمكن المهاجم من تخمين المعلومات منخفضة التصنيف التي يمكن النفاذ إليها بطريقة مشروعة.

إنتهى،،،