الاتحاد الدولي للاتصالات
قطاع التقييس

ITUPublications
التوصيات

التوصية

ITU-T X.1815 (03/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن شبكات الاتصالات المتنقلة الدولية–2020

المبادئ التوجيهية والمتطلبات الأمنية لخدمات حوسبة الحافة في الاتصالات المتنقلة الدولية–2020

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
القياس الحيوي عن بُعد	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن شبكة الويب (1)	X.1140–X.1149
أمن التطبيقات (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن تكنولوجيا السجلات الموزعة (DLT)	X.1400–X.1429
أمن التطبيقات (2)	X.1450–X.1459
أمن شبكة الويب (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1500–X.1519
تبادل معلومات بشأن مواطن الضعف/الحالة	X.1520–X.1539
تبادل معلومات بشأن الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل معلومات بشأن السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولِّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن شبكات الاتصالات المتنقلة الدولية–2020	**X.1800–X.1819**

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1815

المبادئ التوجيهية والمتطلبات الأمنية لخدمات حوسبة الحافة في الاتصالات المتنقلة الدولية–2020

ملخص

ستمكّن شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020) مجموعة متنوعة من الخدمات، منها خدمات النطاق العريض المتنقل المعزَّز (eMBB) والخدمات القائمة على الاتصالات الآلية الكثيفة (mMTC) والخدمات القائمة على الاتصالات منخفضة الكمون فائقة الموثوقية (URLLC)، في بنية تحتية لموارد الشبكة والحوسبة. وتماشياً مع الميزات الرئيسية والمتطلبات المحددة لشبكة الاتصالات المتنقلة الدولية–2020، من اللازم أن تتسم هذه الشبكة بمزيد من الكفاءة والتكيف والذكاء والموثوقية والمرونة.

ولدعم الخدمات النموذجية في شبكة IMT-2020، خاصة خدمات eMBB والخدمات القائمة على الاتصالات URLLC، يُعترف بأن حوسبة الحافة تمثل إحدى التكنولوجيات الرئيسية للوفاء بمؤشرات الأداء الرئيسية (KPI) المتطلّبة لشبكة IMT-2020، خاصة فيما يتعلق بالكمون المنخفض وكفاءة عرض النطاق.

وتمكّن حوسبة الحافة المشغل والطرف الثالث المتمثل في مقدم الخدمة من نشر الخدمات بالقرب من نقطة نفاذ المستعمل، ومن ثم تحقيق كفاءة عالية في تقديم الخدمة من خلال الكمون والحمولة المنخفضين على شبكة النقل من طرف إلى طرف.

ومن أجل ضمان الأمن في عمليات نشر وتطبيقات خدمات حوسبة الحافة، يتعين تحليل التهديدات الأمنية والمتطلبات الأمنية ذات الصلة الخاصة بخدمات حوسبة الحافة ووضع إطار أمني شامل لهذه الخدمات.

ويسعى مشروع التوصية هذا إلى تحليل مخطط النشر وسيناريوهات التطبيق النموذجية لخدمات حوسبة الحافة، ويحدد التهديدات والمتطلبات الأمنية الخاصة بخدمات حوسبة الحافة في الاتصالات IMT-2020، ومن ثم يحدد القدرات الأمنية للمشغل على حماية تطبيقاته.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1815	2023-03-03	17	11.1002/1000/15113

مصطلحات أساسية

خدمات حوسبة الحافة، شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020)، مبادئ توجيهية أمنية.

* للنفاذ إلى توصية، يُرجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات/حقوق تأليف ونشر برمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قواعد البيانات ذات الصلة لقطاع تقييس الاتصالات (ITU-T) في موقع قطاع تقييس الاتصالات http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

المبادئ التوجيهية والمتطلبات الأمنية لخدمات حوسبة الحافة في الاتصالات المتنقلة الدولية–2020

1 مجال التطبيق

تقدم هذه التوصية مخطط نشر محتملاً وسيناريوهات تطبيق نموذجي لخدمات حوسبة الحافة، وتحدد التهديدات والمتطلبات الأمنية لخدمات حوسبة الحافة في الاتصالات المتنقلة الدولية–2020 (IMT-2020)، ومن ثم تقدم مبادئ توجيهية بشأن القدرات الأمنية للمشغل من أجل حماية تطبيقاته.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، فإن مستعملي هذه التوصية يرجى منهم بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T Y.3101] التوصية ITU-T X.3101 (2018)، *متطلبات شبكة الاتصالات المتنقلة الدولية–2020*.

[3GPP TS 23.501] المعيار 3GPP TS 23.50 (2022)، *معمارية نظام الجيل الخامس (5GS) (الإصدار 17، النسخة 0.4.17)*.

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

تُستعمل في هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الاتصالات المتنقلة الدولية–2020 (IMT-2020) [b-ITU-T Y.3100]: (بناءً على التوصية [b-ITU-R M.2083]): الأنظمة ومكونات النظام والتكنولوجيات ذات الصلة التي توفر قدرات أكثر تعزيزاً بكثير من تلك الوارد وصفها في التوصية [b-ITU-R M.1645].

2.1.3 حصان طروادة (Trojan horse) [b-ITU-T E.800]: جزء من برمجية يبدو كأنه لا خطر منه بل قد يبدو مفيداً. وبهذا المظهر يخفي الغرض الحقيقي من البرمجية التي تهدف إلى إعطاب النظام أو سرقة المعلومات.

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 خدمة حوسبة الحافة في الاتصالات المتنقلة الدولية–2020 (IMT-2020 edge computing service): خدمة مقدمة عبر نظام الاتصالات المتنقلة الدولية–2020 تمكّن من استضافة خدمة بالقرب من نقطة النفاذ لمعدات المستعمل، لتحقيق الكفاءة في تقديم الخدمة من خلال الكمون والحمولة المنخفضين على شبكة النقل من طرف إلى طرف.

2.2.3 نظام الاتصالات المتنقلة الدولية-2020 (IMT-2020 system): نظام لمشروع شراكة الجيل الثالث (3GPP) يتكون من شبكة النفاذ إلى الاتصالات المتنقلة الدولية–2020 (AN) والشبكة الرئيسية للاتصالات المتنقلة الدولية–2020 ومعدات المستعمل (UE).

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

AF وظيفة التطبيق *(Application Function)*

AMF وظيفة إدارة النفاذ والتنقلية *(Access and Mobility Management Function)*

AN شبكة النفاذ *(Access Network)*

CDN شبكة إيصال المحتوى *(Content Delivery Network)*

EASDF وظيفة اكتشاف مخدِّم تطبيق الحافة *(Edge Application Server Discovery Function)*

DDoS رفض الخدمة الموزَّع *(Distributed Denial of Service)*

DC مركز البيانات *(Data Centre)*

DN شبكة البيانات (*Data Network*)

DNN اسم شبكة البيانات *(Data Network Name)*

DNS نظام أسماء الميادين *(Domain Name System)*

eMBB النطاق العريض المتنقل المعزَّز *(enhanced Mobile Broadband)*

EHE بيئة مضيفة للحافة *(Edge Hosting Environment)*

GW-C مستوي التحكم في البوابة *(Gateway-Control Plane)*

GW-U مستوي مستعمل البوابة *(Gateway-User Plane)*

IMS نظام فرعي متعدد الوسائط لبروتوكول الإنترنت *(Internet protocol Multimedia Subsystem)*

IP بروتوكول الإنترنت *(Internet Protocol)*

KPI مؤشر أداء رئيسي *(Key Performance Indicator)*

MEC حوسبة الحافة المتنقلة *(Mobile Edge Computing)*

mMTC *الاتصالات الآلية الكثيفة (massive Machine Type Communications)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

NEF وظيفة كشف الشبكة *(Network Exposure Function)*

NB IoT إنترنت الأشياء ضيقة النطاق *(Narrow Band Internet of Things)*

NFVO منسِّق التمثيل الافتراضي لوظائف الشبكة *(Network Functions Virtualization Orchestrator)*

NRF وظيفة مستودع الشبكة *(Network Repository Function)*

VNFM مدير وظيفة الشبكة الافتراضية *(Virtualized Network Function Manager)*

OSS أنظمة دعم التشغيل *(Operation Support Systems)*

PDU وحدة بيانات البروتوكول *(Protocol Data Unit)*

PSA مثبِّت دورة وحدة بيانات البروتوكول *(Protocol data unit Session Anchor)*

QoS جودة الخدمة *(Quality of Service)*

RAN شبكة النفاذ الراديوي *(Radio Access Network)*

SBA معمارية قائمة على الخدمة *(Service Based Architecture)*

SIM وحدة تعرف هوية المشترك *(Subscriber Identification Module)*

SMF وظيفة إدارة الدورة *(Session Management Function)*

TLS أمن طبقة النقل *(Transport Layer Security)*

UE معدات المستعمل *(User Equipment)*

UPF وظيفة مستوي المستعمل *(User Plane Function)*

URLLC الاتصالات منخفضة الكمون فائقة الموثوقية *(Ultra-reliable Low Latency Communications)*

V2X الاتصالات من مركبة إلى كل شيء *(Vehicle to Everything)*

5 الاصطلاحات

تستخدم هذه التوصية الاصطلاحات التالية:

كلمة "**يُشترط**" تدل على متطلب يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

وتدل كلمة "**ينبغي**" على متطلب يوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

6 نظرة عامة على حوسبة الحافة في الاتصالات المتنقلة الدولية–2020

ستمكّن شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020) مجموعة متنوعة من الخدمات، منها خدمات النطاق العريض المتنقل المعزَّز (eMBB) والخدمات القائمة على الاتصالات الآلية الكثيفة (mMTC) والخدمات القائمة على الاتصالات منخفضة الكمون فائقة الموثوقية (URLLC) [ITU-T Y.3101]، في بنية تحتية لموارد الشبكة والحوسبة. وتماشياً مع الميزات الرئيسية والمتطلبات المحددة في شبكة الاتصالات المتنقلة الدولية–2020، من اللازم أن تتسم هذه الشبكة بمزيد من الكفاءة والتكيف والذكاء والموثوقية والمرونة.

ولدعم الخدمات النموذجية في شبكة IMT-2020، خاصة خدمات eMBB والخدمات القائمة على الاتصالات URLLC، يُعترف بأن حوسبة الحافة هي واحدة من التكنولوجيات الرئيسية للوفاء بمؤشرات الأداء الرئيسية (KPI) المتطلِّبة لشبكة IMT-2020، خاصة فيما يتعلق بالكمون المنخفض وكفاءة عرض النطاق.

وتمكّن حوسبة الحافة في الاتصالات IMT-2020 المشغل والطرف الثالث المتمثل في مقدم الخدمة من نشر الخدمات بالقرب من نقطة نفاذ المستعمل من خلال النظام IMT-2020، ومن ثم تحقيق كفاءة عالية في تقديم الخدمة من خلال الكمون والحمولة المنخفضين على شبكة النقل من طرف إلى طرف.

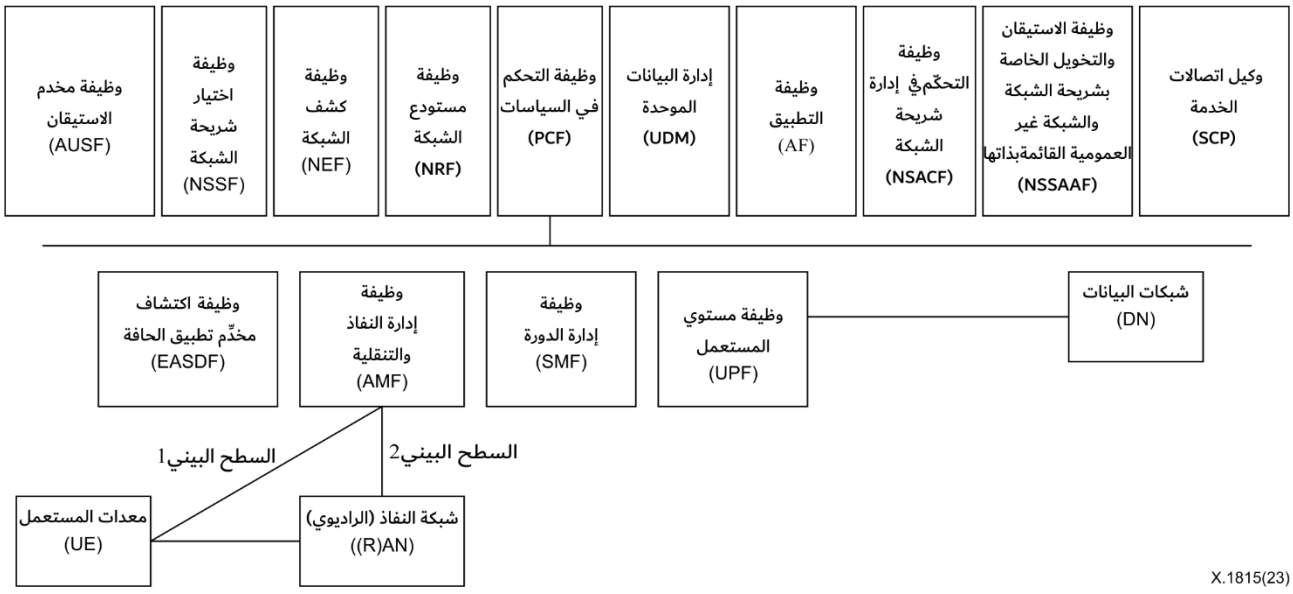
1.6 مخطط النشر

يتاح لمعمارية النظام IMT-2020 التي حددها مشروع شراكة الجيل الثالث (3GPP) في النظام IMT-2020 خياران، ينطوي أحدهما على النهج التقليدي القائم على السطح البيني والنقطة المرجعية، وأما الآخر، فتتفاعل فيه وظائف الشبكة الأساسية فيما بينها باستعمال معمارية قائمة على الخدمة (SBA).

ويصف الشكل 6-1 معمارية للنظام IMT-2020 قائمة على المعيار [3GPP TS 23.501].

ومن منظور المشغل، قد يشمل مخطط نشر خدمات حوسبة الحافة في الاتصالات IMT-2020 باستعمال المعمارية SBA الوظائف التالية لشبكة الاتصالات IMT-2020:

- (UPF) وظيفة مستوي المستعمل: هذه الوظيفة واحدة من وظائف الشبكة (NF) للشبكة الأساسية للاتصالات IMT-2020. وهي المسؤولة عن تسيير الرزم وإعادة إرسالها، والتفتيش عن الرزم، ومعالجة جودة الخدمة (QoS)، ودورة وحدة بيانات البروتوكول (PDU) الخارجية من أجل التوصيل البيني لشبكة البيانات (DN)، في معمارية الاتصالات IMT-2020.
- (AMF) وظيفة إدارة النفاذ والتنقلية: تتلقى هذه الوظيفة من معدات المستعمل (UE) جميع المعلومات المتعلقة بالتوصيل والدورة من خلال السطح البيني N1، وشبكة النفاذ (الراديوي) ((R)AN) من خلال السطح البيني N2 (انظر الشكل 1)، ولكنها مسؤولة فقط عن التعامل مع المهام المتعلقة بإدارة التوصيل والتنقلية.
- (SMF) وظيفة إدارة الدورة: هذه الوظيفة عنصر أساسي في معمارية SBA للاتصالات IMT-2020. وهي المسؤولة الأولى عن التفاعل مع مستوي البيانات المنفصلة، واستحداث دورات PDU وتحديثها وحذفها، وإدارة سياق الدورة مع الوظيفة UPF.
- (EASDF) وظيفة اكتشاف مخدِّم تطبيق الحافة: تشمل هذه الوظيفة واحدة أو أكثر من الوظائف التالية: التسجيل في وظيفة مستودع الشبكة (NRF) من أجل اكتشاف وظيفة EASDF واختيار ومعالجة رسائل نظام أسماء الميادين (DNS) وفقاً للتعليمات الصادرة من وظيفة SMF. وتتمتع وظيفة EASDF بتوصيلية مباشرة لمستوي المستعمل (أي دون أي ترجمة لعنوان الشبكة (NAT)) مع مثبِّت دورة PDU (PSA) على السطح البيني N6 من أجل إرسال إشارات النظام DNS المتبادلة مع معدات المستعمل (UE).



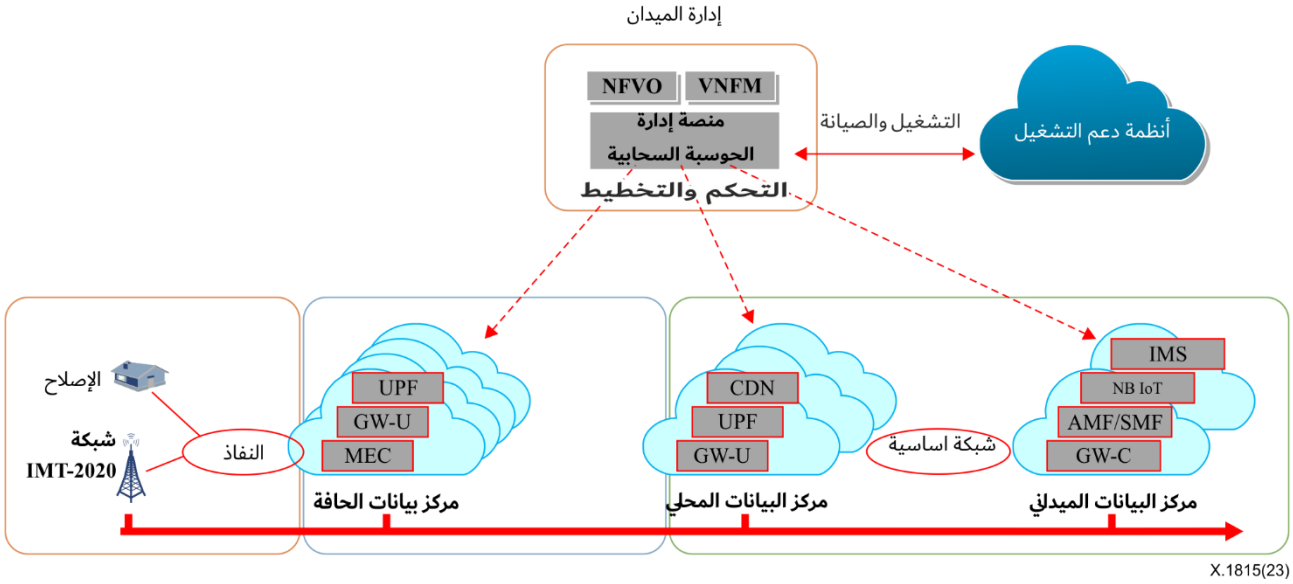
الشكل 6-1 معمارية نظام الاتصالات المتنقلة الدولية–2020

يصف الشكل 6-2 مخطط نشر لخدمات حوسبة الحافة في الاتصالات IMT-2020.

ويدعم نظام IMT-2020 البيئة المضيفة للحافة (EHE) التي يتم نشرها في شبكة البيانات خارج وظيفة مستوي المستعمل لمثبِّت دورة وحدة بيانات البروتوكول (PSA UPF). ويمكن أن تكون البيئة EHE تحت تحكم المشغل أو أطراف ثالثة [b-3GPP TS 23.548]. ويمكن أن يتمتع الجزء المحلي من شبكة البيانات الذي تنشر فيه البيئة EHE بتوصيلية مستوي المستعمل مع مثبِّت دورة PSA يتم نشره مركزياً ومع مثبِّت دورة PSA يتم نشره محلياً لاسم شبكة البيانات (DNN) نفسه.

ومن وجهة نظر المشغل، يكون مخطط نشر خدمات حوسبة الحافة في الاتصالات IMT-2020 على النحو المبين في الشكل 6-2.

- **مركز بيانات الحافة:** يوفر وظيفة حوسبة الحافة المتنقلة (MEC) التي تمكن خدمات حوسبة الحافة في الاتصالات IMT-2020 ووظيفة مستوي مستعمل البوابة (GW-U) ووظيفة مستوي المستعمل (UPF).
- **مركز البيانات المحلي:** يوفر وظائف GW-U وشبكة إيصال المحتوى (CDN) وUPF.
- **مركز البيانات الميداني:** يوفر وظائف مستوي التحكم في البوابة (GW-C) وإدارة النفاذ والتنقلية/إدارة الدورة (AMF/SMF) وإنترنت الأشياء ضيقة النطاق (NB IoT) والنظام الفرعي متعدد الوسائط لبروتوكول الإنترنت (IMS)، ووظائف أخرى.
- **إدارة الميدان:** تشمل منصة إدارة الحوسبة السحابية، ومنسِّق التمثيل الافتراضي لوظائف الشبكة (NFVO)، ومدير وظيفة الشبكة الافتراضية (VNFM).



الشكل 6-2 مخطط نشر خدمات حوسبة الحافة في الاتصالات المتنقلة الدولية–2020

2.6 سيناريو التطبيق النموذجي

1.2.6 الاتصالات من مركبة إلى كل شيء (V2X)

في سيناريو الاتصالات من مركبة إلى كل شيء (V2X)، يجلب حجم الأجهزة الموصولة ذات التطبيقات المتعددة عدداً متزايداً من متطلبات نقل البيانات إلى جانب الشبكة. والشبكة مطلوبة لإتاحة نطاق عريض معزز وقدرات حسابية معززة من أجل استخدام البيانات وتخزينها.

وبتطبيق تكنولوجيا حوسبة الحافة للاتصالات IMT-2020 في سيناريو V2X، أصبح من الممكن نشر تطبيقات في عقدة الحافة، ومن ثم تقليل التأخير الزمني من طرف إلى طرف وزيادة الموثوقية بما يتماشى مع المتطلبات المحددة لخدمات V2X المختلفة (على سبيل المثال، تحتاج خدمة القيادة الآمنة إلى متطلبات صارمة فيما يتعلق بالكمون والموثوقية على السواء) من خلال الاستفادة من مسار الإرسال الأقصر وتوفير موارد أقوى للحوسبة والتخزين.

وتشمل الخدمات في تكنولوجيا حوسبة الحافة للاتصالات IMT-2020 القائمة على الاتصالات V2X ما يلي دون الاقتصار عليه:

- **خدمة المعلومات:** توفر خدمة حوسبة الحافة وظائف التحديد والتحميل والتحديث، والترفيه السمعي والفيديوي، والكشف عن بُعد عن المركبة. وتتطلب هذه الوظائف خدمة حوسبة حافة توفر قدرة معززة للنطاق العريض المتنقل، مثلاً، 25 Mbps على الأقل لخدمة فيديوية عالية الوضوح 4K.

- **خدمة القيادة الآمنة:** تساعد خدمة حوسبة الحافة السائق في اتخاذ قرارات التحكم (مثلاً، عن طريق إصدار إنذار بالاصطدام) من خلال معلومات المركبة ومعلومات الراجلين والحصول على معلومات وحدة جانب الطريق. ومن المطلوب أن توفر خدمة حوسبة الحافة قدرات كمون منخفض وموثوقية عالية (بشكل عام، يقل التأخير عن 20 ms ولا تقل موثوقية الاتصالات عن 99%).
- **خدمة كفاءة القيادة المعززة:** تحقق خدمة حوسبة الحافة المستوى الأمثل لكفاءة مرافق حركة المرور استناداً إلى تكنولوجيات V2X وتحليل البيانات الضخمة للاتصالات IMT-2020، مثلاً التحكم في إشارات حركة المرور، ودليل سرعة المركبة.

2.2.6 إنترنت الأشياء (IoT)

بتطبيق تكنولوجيا حوسبة الحافة للاتصالات IMT-2020 في إنترنت الاشياء، أصبح من الممكن نشر تطبيقات في عقدة الحافة، ومن ثم تقليل التأخير الزمني من طرف إلى طرف من خلال الاستفادة من مسار الإرسال الأقصر وعرض خدمة أكثر كفاءة عبر حوسبة البيانات المحلية.

وتشمل سيناريوهات الخدمة في تكنولوجيا حوسبة الحافة للاتصالات IMT-2020 القائمة على إنترنت الأشياء ما يلي دون الاقتصار عليه:

- المدينة الذكية؛
- المبنى الذكي؛
- المنزل الذكي.

3.2.6 الإنترنت الصناعية

تدعم تكنولوجيا حوسبة الحافة للاتصالات IMT-2020 خدمات الإنترنت الصناعية (خاصة بالنسبة لحالة تطبيقات إنترنت الأشياء في الوقت الفعلي، حيث تُعالج البيانات عادةً بعيداً عن مركز البيانات المركزي ويكون الكمون المنخفض مطلباً إلزامياً) من خلال تنسيق شبكة الاتصالات IMT-2020 مع المتحكِّم في الحافة وبوابة الحافة والحوسبة السحابية للحافة.

ويكون المتحكِّم في الحافة مسؤولاً عن تنسيق المهام ونشر التطبيقات وإدارة دورة الحياة من بوابة الحافة، ويتحكم في الأجهزة الصناعية، وما إلى ذلك.

وتنفذ بوابة الحافة عمليات تنسيق المهام وتسجيل الأجهزة الصناعية ونشر التطبيقات وإدارة دورة الحياة من الحوسبة السحابية للحافة، وتحلِّل بيانات الحافة، وما إلى ذلك.

وتكون الحوسبة السحابية للحافة مسؤولة عن تنسيق المهام وتسجيل الأجهزة الصناعية ونشر التطبيقات وإدارة دورة الحياة من بوابة الحافة، وتنسق مخدمات الحافة، وتحلل بيانات الحافة، وما إلى ذلك.

7 التهديدات الأمنية

يشمل عرض خدمة حوسبة الحافة للاتصالات المتنقلة الدولية–2020، من وجهة نظر متعددة الطبقات، طبقة البنية التحتية وطبقة الشبكة وطبقة التطبيق، ولذلك يجب النظر في التهديدات الأمنية من جميع وجهات النظر هذه. ومن المهم الإشارة إلى أنه على الرغم من أن حوسبة الحافة المتنقلة (MEC) تتمتع بخاصية الأمن وحماية الخصوصية لأن نقل البيانات يتم مباشرة إلى مخدّمات حوسبة الحافة المتنقلة (MEC) بدلاً من المخدّمات المركزية، مما يقلل من مخاطر تسرب البيانات في عملية نقل البيانات في الشبكة، فإن استخدام عدد كبير من الأجهزة المحمولة ونشر مخدمات سحابية متطورة يؤدي إلى تحديات أمنية جديدة. وتحديداً، قد لا تكون حلول أمن الحوسبة السحابية التقليدية مناسبة لحوسبة الحافة المتنقلة (MEC) نظراً إلى أن بيئات أجهزة إنترنت الأشياء على الحافة تواجه عدداً من التهديدات الجديدة التي تختلف تماماً عن تلك الموجودة في الإدارة التقليدية للحوسبة السحابية. ومن الناحية العملية، يستحيل تطبيق أساليب أمن البيانات الحالية على أجهزة الحافة لأن معظمها مقيد بالموارد وتصبح الشبكة ضعيفة بسبب البيئة الدينامية للغاية لحوسبة الحافة المتنقلة (MEC). وأجرت وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) تقييماً شاملاً لمواطن

الضعف فيما يتعلق بحوسبة الحافة المتنقلة (MEC) [b-ENISA] مع مراعاة مواصفات الجيل الخامس (5G) وفقاً للإصدار 16 للمواصفات التقنية التي وضعها مشروع شراكة الجيل الثالث (3GPP). لذلك، فإن تهيئة بيئة لحوسبة الحافة المتنقلة (MEC) لتطبيقات الجيل الخامس (5G) المستقبلية مع ضمان الأمن، لا يزال يمثّل مشكلة تتطلب مزيداً من البحث في المستقبل القريب.

1.7 طبقة البنية التحتية

1.1.7 منصة إدارة الحوسبة السحابية

قد يحتاج نشر خدمة حوسبة الحافة للاتصالات IMT-2020 إلى منصة لإدارة الحوسبة السحابية. وإلى جانب التهديدات الأمنية العامة التي تواجهها هذه المنصة، يمكن أن يستعمل المهاجم السطح البيني بين منصة إدارة الحوسبة السحابية وشبكة IMT-2020 لشن هجمات أخرى على شبكة IMT-2020.

2.1.7 البنية التحتية الافتراضية

قد لا تكون البنية التحتية الافتراضية متاحة في حالة تعرض الموارد المادية لهجمات أو عطل. ويمكن أن يستغل المهاجم هشاشة النظام المحتملة هذه للنفاذ الإداري غير المخول إلى نظام إدارة الموارد الافتراضي وتغيير معلومات التشكيل.

3.1.7 عمليات حقن معدات/برمجيات خبيثة

يمكن حقن مكونات برمجيات ومعدات غير مرخصة معروفة باسم "أحصنة طروادة" في البنية التحتية للنيل من فعالية مخدمات وأجهزة الحافة القائمة، بل السماح باستغلال مقدم الخدمة [b-Daniel]. وقد يسمح هذا الأمر للكيانات التي تقدم حلول البرمجيات والمعدات لخدمة حوسبة الحافة بتنفيذ أنشطة خبيثة عن غير قصد نيابةً عن المهاجم.

4.1.7 العبث المادي بالأجهزة

يزيد احتمال إمكانية العبث المادي بالأجهزة مع زيادة اقتراب مكان وجود موارد الحوسبة في معمارية حوسبة الحافة من المهاجمين المحتملين. وقد يُتلف المهاجم عُقد الحافة، مما يؤدي بدوره إلى الإضرار بفعالية الشبكة بأكملها.

2.7 طبقة الشبكة

1.2.7 تحليل تدفق الشبكة

قد يقوم المهاجم بمراقبة و/أو سرقة بيانات الوصلات وتحليل خصائص التدفق للحصول على معلومات عن الخدمات، ويبادر من ثم إلى مواصلة الهجوم على الشبكة.

2.2.7 التقاط طوبولوجيا الشبكة

يمكن أن يلحق المهاجم ضرراً بعقدة الخدمة التي قد يتم نشرها في البيئات المفتوحة لشن هجوم يلتقط من خلاله طوبولوجيا الشبكة.

3.2.7 هجوم رفض الخدمة الموزَّع (DDoS)

يمكن أن يلحق المهاجم ضرراً بالمستعملين المشتركين و/أو عُقد الخدمة التي قد يتم نشرها في البيئات المفتوحة لشن هجوم رفض الخدمة الموزَّع (DDoS). وعند حدوث هجمات DDoS، يكون مورد الشبكة الحالي منشغلاً بالحركة الناجمة عن موارد أخرى ألحق بها الضرر داخل الشبكة، وهو خطر أمني آخر يهدد حوسبة الحافة.

4.2.7 التنصت على بيانات الاتصالات أو التلاعب بها

تعتمد الخدمات التي تستعمل حوسبة الحافة للاتصالات IMT-2020 على الشبكة اللاسلكية المفتوحة. ويمكن أن يتنصت المهاجم على بيانات الاتصالات أو يتلاعب بها؛ ففي بعض السيناريوهات، على سبيل المثال، قد تتضمن بيانات الاتصال الخاصة بالصناعة

والمصنع والمدينة الذكية معلومات بالغة الأهمية من قبيل معرفات هوية المستعمل وبيانات اعتماده، ومعلومات الأعمال ومعلومات السلامة العامة.

5.2.7 الهجوم العابر للميادين

نظراً إلى أن خدمة حوسبة الحافة في شبكة IMT-2020 تحتاج إلى تنسيق الوظائف بين شبكة النفاذ والشبكة الأساسية ومنصة إدارة الحوسبة السحابية، فإن نقطة التوافق الوحيد قد تتسبب في هجوم عابر للميادين يؤدي على عدم توفر الشبكة والخدمة.

6.2.7 النفاذ غير المخول

يتطلب تمكين معدات المستعمل من التوصيل بأفضل خدمة لحوسبة الحافة تفاعلات تشوير بين معدات المستعمل وشبكة IMT-2020 الأساسية. وإذا عبث مهاجم بوظيفة التشوير، فإنه قد يجعل النفاذ غير المخول إلى خدمة حوسبة الحافة، بل شن هجوم DDoS، أمراً ممكناً.

7.2.7 كشف الشبكة لتطبيق الحافة

يمكن أن تكشف الحوسبة السحابية لشبكة IMT-2020 معلومات الشبكة لوظيفة التطبيق (AF) المحلية مع احتمال سيناريوهات من قبيل وظيفة مستوي المستعمل لمثبِّت دورة وحدة بيانات البروتوكول (PSA UPF) المحلية التي تكشف معلومات الشبكة للوظيفة AF المحلية من خلال وظيفة كشف الشبكة (NEF) المحلية أو بشكل مباشر.

8.2.7 هجمات معلومات التسيير

يحدث هجوم معلومات التسيير، أو ببساطة هجوم التسيير، في طبقة الشبكة لشبكة الحافة. وتتداخل هجمات التسيير مع الطريقة التي يتم بها نقل الحركة داخل الشبكة، مما قد يؤثر على الصبيب والكمون ومسارات البيانات.

9.2.7 اختطاف الدورة

يقوم القرصان باعتراض دورة المستعمل واختطافها للنفاذ إلى بيانات المستعمل وخدماته.

3.7 طبقة التطبيق

1.3.7 هشاشة الإطار التقني

في خدمات حوسبة الحافة للاتصالات IMT-2020، حيث يستخدم كم هائل من العُقد نفس الإطار التقني بين مختلف السيناريوهات والصناعات الرأسية، فإن تعرض عقدة واحدة للخطر من شأنه أن يؤثر على العقد الأخرى.

2.3.7 الاستعمال غير المرخص

يحدث التهديد المتمثل في الاستعمال غير المرخص عندما يتمكن مستعمل غير قانوني أو غير مشترِك من النفاذ إلى خدمات حوسبة الحافة للاتصالات IMT-2020 من خلال التنكر في هيئة كيان مخول.

3.3.7 أحصنة طروادة والفيروسات

تحدث الهجمات باستخدام أحصنة طروادة والفيروسات عندما تقوم خدمة خبيثة لحوسبة الحافة للاتصالات **IMT-2020** أو مهاجم بانتحال صفة مقدم خدمة قانوني وحقن أحصنة طروادة أو فيروسات في تطبيق، مما قد يلحق ضرراً بأجهزة المستعمل وبياناته، بل يشن هجوماً إضافياً على شبكة الاتصالات المتنقلة.

4.3.7 الكشف عن البيانات

يحدث الكشف عن البيانات عندما ينتحل المهاجمون صفة كيان قانوني للحصول على بيانات أثناء عمليات خدمة حوسبة الحافة المتمثلة في ترحيل بيانات التطبيق وإرسالها وتخزينها وتبادلها وإتلافها.

8 المتطلبات الأمنية

1.8 طبقة البنية التحتية

ينبغي أن تشمل المتطلبات الأمنية لمنصة إدارة الحوسبة السحابية ما يلي:

أ) أن تدعم منصة إدارة الحوسبة السحابية الاستيقان والتخويل لبوابة مستوي البيانات وإدارة منصة حوسبة الحافة وتطبيق حوسبة الحافة.

ب) حماية البيانات الحساسة من أجل مقاومة النفاذ غير المخول والعبث بالبيانات (على سبيل المثال، في السيناريوهات الصناعية، يلزم حماية بيانات الإنتاج الحساسة من أجل الأداء السليم للعمليات الصناعية، ولتجنب أي انقطاع بسبب هجمات الشبكة).

ج) عزل منصة إدارة الحوسبة السحابية بشكل آمن مع عناصر الشبكة الأساسية IMT-2020 (مثلاً، وظيفة كشف الشبكة (NEF)، وظيفة مستوي المستعمل (UPF)).

د) إجراء تحليلات القنوات الجانبية للكشف عن معدات أحصنة طروادة باستخدام تحليلات الوقت والطاقة ودرجة حرارة المكان. وتكشف هذه الطريقة أساساً عن البرمجيات الثابتة الخبيثة أو البرمجيات المثبتة على عُقد الحافة من خلال تحديد سلوكيات النظام غير العادية، مثل الزيادات في وقت التنفيذ أو استهلاك الطاقة.

هـ) استخدام طرق الكشف عن معدات أحصنة طروادة التي تقارن المعدات المصابة بأحصنة طروادة مع المعدات غير المصابة بأحصنة طروادة للكشف عن الهجمات الخبيثة.

و) إنفاذ الأمن المادي لأي عُقد حافة غير موضوعة في مراكز بيانات الحافة ذات مستوى أمني عال، مثل استخدام تقنيات حماية مادية إضافية خلال التصنيع أو تنفيذ آليات إقفال وغير ذلك من الضمانات المادية في الميدان.

ز) بصرف النظر عما سبق، ضرورة حماية أجزاء نظام الحافة التي تتعامل مع مواد التجفير من هجمات القنوات الجانبية، وذلك مثلاً باستخدام بطاقات SIM محصَّنة ومقاوِمة.

وينبغي أن تشمل المتطلبات الأمنية للبنية التحتية الافتراضية ما يلي:

أ) ضرورة عزل وحدة المعالجة المركزية الافتراضية (vCPU) والذاكرة والدخل/الخرج (I/O) للآلة الافتراضية بشكل آمن، في حالة نشر الآلة الافتراضية للبنية التحتية لخدمة حوسبة الحافة للاتصالات IMT-2020.

ب) دعم البنية التحتية الافتراضية للعزل الآمن بين الحاويات.

ج) دعم البنية التحتية الافتراضية لنسخ المستودعات والتوقيع.

د) فصل الحركة وعزل موارد الحوسبة من خلال التجزئة بتقسيم الشبكة [b-ENISA].

2.8 طبقة الشبكة

ينبغي أن تشمل المتطلبات الأمنية لاتصالات الشبكة ما يلي:

أ) دعم سرية وحماية سلامة إرسال البيانات.

ب) استخدام بروتوكول أمنياً (مثلاً TLS v1.2) لإنشاء قناة آمنة بين عناصر الشبكة.

ج) استخدام تجفير حركة البيانات بين الأطراف باستعمال بروتوكول نقل آمن من طرف إلى طرف، واستخدام رقم عشوائي طويل أو سلسلة عشوائية طويلة كمفتاح للدورة، وإعادة إنشاء معرف الدورة بعد كل تسجيل دخول ناجح.

د) دعم قدرة حماية رفض الخدمة الموزع (DDoS) عن طريق ترشيح الحركة بعناية بحيث لا يُسمح للطلبات غير المشروعة بالمرور، بينما تمر الطلبات المشروعة دون تأخير كبير.

وينبغي أن تشمل المتطلبات الأمنية لإدارة الشبكة ما يلي:

أ) أن تدعم أنظمة دعم التشغيل (OSS) الاستيقان والتخويل من أجل التفاعل مع منصة إدارة الحوسبة السحابية.

ب) أن يتم عزل الوظائف بين إدارة خدمة حوسبة الحافة والأنظمة OSS بشكل آمن.

ج) أن يتم باستمرار رصد ما إذا كانت الشبكة بطيئة أو معيبة، وإصدار الإنذارات بالهجمات والمشاكل المتعلقة بالشبكة في الوقت المناسب.

د) أن يتم إنشاء بروتوكولات تسيير موثوقة.

3.8 طبقة التطبيق

ينبغي أن تشمل المتطلبات الأمنية لتطبيق الحافة ما يلي:

أ) تنفيذ تقييم أمني يشمل التحقق من الامتثال الأمني وإدارة الأصول ومسح الفيروسات، وما إلى ذلك.

ب) أن يدعم تطبيق الحافة الاستيقان والتخويل من أجل التفاعلات بين منصة إدارة الحوسبة السحابية وتطبيقات الحافة الأخرى.

ج) حماية البيانات الحساسة من أجل مقاومة النفاذ غير المخول والعبث بالبيانات.

د) دعم التحقق من سلامة تطبيق الحافة.

هـ) التحقق من هوية المسؤول وسلطته أثناء تحميل تطبيق الحافة وتثبيته.

و) دعم السرية وحماية السلامة في عمليات نقل البيانات وإرسالها وتخزينها وتبادلها وإتلافها.

ز) دعم وظيفة تعرف تلقائي وتشديد أمني تستند إلى تمديد أمن لغة البرنامج وتحليل البرنامج الساكن.

ح) دعم وظائف الرصد والتحليل والإنذار في الوقت الفعلي فيما يتعلق بأداء التطبيق والحركة وقناة المصدر وبيئة العميل.

ط) دعم مراجعة التطبيق، والمواظبة على جمع السجلات الأمنية لأجهزة الحافة وتطبيقاتها، وتخزينها وتحليلها، ثم التنبيه وتعقب الانتهاكات والتجاوزات والسلوكيات غير الطبيعية للتطبيق.

9 مبادئ توجيهية بشأن القدرات الأمنية لخدمة حوسبة الحافة

1.9 طبقة البنية التحتية

للوفاء بالمتطلبات الأمنية لطبقة البنية التحتية، ينبغي توفير القدرات الأمنية الضرورية التالية:

أ) رصد مخاطر أمن البيانات والإنذار المبكر بها لمنع العبث بالبيانات وتسريبها.

ب) تخزين أمن البيانات، بما في ذلك قدرات التخزين المجفر للبيانات الحساسة وتغليفها.

ج) قدرات حماية أمن المنصة الافتراضية من خلال تعزيز أمن النظام والعزل الأمني والتحكم الأمني وتجفير البيانات وغير ذلك من القدرات لضمان أمن البيانات في الشبكة الافتراضية.

د) الوظائف الأمنية الكفيلة بضمان أمن التمثيل الافتراضي لوظائف الشبكة، بما فيها:

- ضوابط الاستيقان؛

- ضوابط النفاذ؛
- التحقق عن بُعد لأغراض أمن النظام؛
- أمن الاتصالات؛
- الشهادة؛
- الاستنساخ؛
- التوقيع؛
- العزل الأمني؛
- أقسام التنفيذ بوساطة العتاد؛
- جذر الثقة القائم على العتاد؛
- تجفير العتاد؛
- بيئة التنفيذ الموثوقة؛
- التخزين ذاتي التجفير؛
- النفاذ المباشر إلى الذاكرة؛
- الوحدات النمطية لأمن العتاد؛
- حماية سلامة البرمجيات والتحقق منها.

2.9 طبقة الشبكة

تشمل القدرات الأمنية لطبقة الشبكة التي ينبغي توفيرها ما يلي دون الاقتصار عليه:

أ) قدرات لحماية سرية وسلامة إرسال البيانات، مثل الختم الزمني والرقم التسلسلي وتجفير الوصلة، وآليات أخرى.

ب) دعم القدرات لمنع اختطاف الدورة، مثل تجفير حركة البيانات بين الأطراف، باستخدام رقم عشوائي طويل أو سلسلة عشوائية طويلة كمفتاح للدورة، وإعادة إنشاء معرف الدورة بعد نجاح تسجيل الدخول.

ج) التحكم في أمن البيانات المتعلقة بعُقد الحافة، بما في ذلك استيقان الهوية والعزل الأمني والرصد المستمر والإنذار المبكر وتجفير البيانات وإزالة حساسية البيانات والنسخ الاحتياطي.

د) بروتوكولات تسيير موثوقة.

3.9 طبقة التطبيق

تشمل القدرات الأمنية لطبقة التطبيق التي ينبغي توفيرها ما يلي دون الاقتصار عليه:

أ) التحكم في أذونات التطبيق لمختلف المستعملين والسيناريوهات، من أجل ضمان سرية وسلامة وتيسر بيانات طبقة التطبيق وخدماتها.

ب) الحماية من هجمات الفيروسات وتحديث قاعدة بيانات الفيروسات في الوقت المناسب لمنع تسريب البيانات أو سرقتها.

ج) تحديد البيانات الحساسة وتقييمها، بما يشمل الترخيص بإزالة الحساسية والتخزين المجفر والرصد والتعقب والتنبيه غير الطبيعي وإدارة المراجعة والإتلاف، وغير ذلك من القدرات.

د) استيقان الهوية والرصد المستمر والإنذار المبكر.

بيبليوغرافيا

[b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2021), *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2006), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-ITU-R M.2083] Recommendation ITU-R M.2083 (2015), *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

[b-3GPP TS 23.548] 3GPP 23.548 (2021), *5G system enhancements for edge computing (version 17.2.0 release 17)*.

[b-Daniel] B. Daniel, *Is edge computing secure? Here are 4 security risks to be aware of* 9 December 2020.
https://www.trentonsystems.com/blog/is-edge-computing-secure.

[b-ENISA] ENISA (European Union Agency for Cybersecurity), *ENISA Threat Landscape For 5G Networks*, December 2020. Available to:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2023