تحسين زمن الاستجابة باستخدام إطار جديد لإدارة الهوية في إنترنت الأشياء

د. ألفت جولحة*

عبير ابراهيم**

(تاريخ الإيداع 3 / 1 / 2021. قُبِل للنشر في 10/ 6 / 2021)

□ ملخّص □

يعتبر إنترنت الأشياء IoT مفهوماً متطوراً لشبكة الإنترنت التقليدية بحيث تمتلك الأشياء قابلية الاتصال بالإنترنت أو ببعضها البعض لإرسال واستقبال البيانات لأداء وظائف محددة من خلال الشبكة. يقدِّم نظام إدارة الهوية IdM (Identity Management)، خدمة المصادقة وتفويض النفاذ في شبكة الإنترنت، لذلك من المهم استخدامه مع إنترنت الأشياء IoT (Internet of Thing). يقترح هذا البحث تصميم إطار جديد لتحديد الهوية في إنترنت الأشياء في ظلِّ مُراعاة كل من تحقيق قناة اتصال آمنة، ومعرفة أنَّ أجهزة إنترنت الأشياء، هي أجهزة ذات موارد محدودة، ممّا فرض إيجاد آليَّات جديدة لتقليل استهلاك هذهِ الموارد. تمَّ التحقّق من أداء الإطار المقترح بإجراء سيناريوهات باستخدام برنامج المُحاكاة Cooja، وذلكَ وفقاً لمجموعةٍ من البارامتراتِ المؤثرةِ على الأداء، وقد قدَّم الإطار المُقترح تحسيناً في زمن الاستجابة.

الكلمات المفتاحية: إنترنت الأشياء، نظام إدارة الهوية، المصادقة، تفويض النفاذ، خدمة تسجيل الدّخول الموحّد.

* مدرسة– قسم هندسة الحاسبات والتحكم الآلي– كلية الهندسة الميكانيكية و الكهربائية– جامعة تشرين– اللاذقية– سورية.

** – طالبة ماجستير– قسم هندسة الحاسبات و التحكم الآلي– كلية الهندسة الميكانيكية و الكهربائية – جامعة تشرين– اللاذقية– سورية.

Improvement of Response Time Using a New Identity Management Framework in Internet of Things

Dr. Oulfat Jolaha[*]
Abeer Ebraheem[**]

(Received 3 / 1 / 2021. Accepted 10 / 6 / 2021)

□ ABSTRACT □

The Internet of Things (IoT) is an advanced concept of the traditional Internet so that objects have internet connectivity or each other to send and receive data to perform specific functions through the network. Identity Management (IdM) provides authentication and internet access authorization, so it is important to use it with Internet of Things (IoT). This research suggests designing a new identity management (IdM) framework in Internet of Things (IoT) taking into account both the realization of a secure communication channel and the fact that IoT devices are only devices with limited resources, forcing mechanisms to reduce the consumption of these resources. The performance of the proposed framework is verified by conducting scenarios using Cooja, according to a set of performance-impact parameters. The proposed identification framework provides an improvement in response time.

Keywords: Internet of Things (IoT), Identity Management (IdM) System, Authentication, Authorization, Single Sign On Service.

***Assistant Professor, Department of Computers and Automated Control, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**
****Postgrtaduate (Master), Department of Computers and Automated Control, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**

مقدمة:

تمثل إنترنت الأشياء Internet of Things (IoT)، شبكة مؤلفة من أغراضٍ (أشياء) مترابطة. ومن هذه الأشياء حسّاسات، محركات، أجهزة يمكن التعرف عليها من خلال عنوان شبكي فريد وتملك اتصال شبكي من أجل التفاعل. عادةً ما تكون هذه الأشياء محدودة الموارد من حيث قدرة المعالجة، الذّاكرة، وقابلية الاتصال (مدى الاتصال والنطاق الترددي) [1]،[2]. وإنّ عددَ الأجهزة (الأشياء) يزداد بشكل مستمر وأصبحت معظم هذه الأشياء منتجاتٍ بسيطة متوفرة في الأسواق الاستهلاكية مع حمايةٍ ضعيفةٍ ضد معظم الهجمات الالكترونية الشّائعة [3]، [4]. تتواجد أجهزة إنترنت الأشياء في مجالات عدة منها الصّحية، النقل، السّكنية، وغيرِها. على سبيل المثال، السّيناريو الذّي يُوضّح تواجد إنترنت الأشياء في المناطق السّكنية، هو امتلاك عدّة أجهزة (مثل الغسّالات والثّلاجات)، تقومُ بمراقبةِ عاداتِ الناس أو مساعدتِهم في مهام حياتهم اليوميَّة، كإبلاغِ الشّركة المصنعة للجهاز بوجود عطلٍ ما فيه. في هذه الحالة، يحتاج المصنعون إلى الوصول لهذه الأجهزة عن بعدٍ، إما للإصلاح والتحسين، أو لتحديث البرامج الثابتة الخاصة بالجهاز[1]،[3]. هنا يبرز مفهوم عزل الأجهزة بشكل مهم، بحيث يُمنع الوصول المباشر لهذه الأجهزة من خلال الإنترنت، ممّا يضمن عدم الوصول غير المصرح به وعدم انتهاك الخصوصية [1]. تشكّل كلاً من المصادقة، وتفويض النفاذ تحدَياً لإنترنت الأشياء، لاختلافها عن مكونات الإنترنت التقليدية، حيثُ أنَّ أجهزة إنترنت الأشياء ذات غرض محدد بمعظمها، وعادةً ما تكون ذات موارد محدودة [1].

لقد تركّزت جهود الباحثين نحو تقديمِ العديد من المُقترحاتِ التّي من شأنِها أن تستخدم نظام إدارة الهوية IdM مع إنترنت الأشياء IoT، ولكن لكلٍّ منها سلبياتُها، ممّا يجعل تلك السّلبيات قضايا مفتوحة أمامَ الباحثين. ففي [6] تمَّ اقتراح بنية مصادقة وتحكُّم بالوصول للمستخدمين وأجهزة إنترنت الأشياء، حيثُ اعتُبِرت الأجهزة عقداً نهائيةً في بنية الإنترنت، تتواصل مع بعضها من خلال عناوين عالميَّة فريدة IPV6 باستخدام البروتوكول Open ID من أجل المصادقة، والبروتوكول RBAC من أجل تفويض النفاذ، إلاَّ أنَّ هذا البحث لم يتطرَّق إلى قضايا تسجيل الدّخول الموحّد Single Sign On (SSO)، كما أنّه لم يُقدّم نتائج يُمكن من خلالِها التحقّق من البنية المقترحَة. بينما في [7] تمَّ التحكم بالوصول إلى الأجهزة عن طريق البروتوكول AOuth، وبروتوكول آخر يعتمد على قائمة انتظار يفعّل في مكّون وسيط بين سياقي الإنترنت وإنترنت الأشياء. واستخدمت الدّراسة [8] مكّون خدمات الويب بين الإنترنت وإنترنت الأشياء، في سبيل توافر سريَّة وسلامة المعلومات المُرسلة بين السّياقين. لابُدَّ من التَّنويه إلى أنَّه لا تعتبر الأنظمة في كل من [7] و[8] قادرة على تأمين تفاعل أمني نهاية لنهاية (بين الإنترنت وإنترنت الأشياء)، أو قنوات اتصال آمنة، أو حتّى خدمة تسجيل دخول موحَّد. قدمت الدراسة [9] خدمة تفويض خارجيَّة مستندة على البروتوكول AOuth، والتّي تسمَّى IoT-AOS، حيثُ تمَّ تناول تكامل إنترنت الأشياء مع مخطَّط التفويض الخاص بالإنترنت، وذلك باستخدام قناة اتصال آمنة، مع ذلك فإنَّ هذا العمل لا يملك تفاعل أمني نهاية إلى نهاية بين الإنترنت وإنترنت الأشياء، علاوةً على ذلك فإنّهُ لا يتناول خدمة تسجيل الدّخول الموحّد. على النقيض من ذلك، فإنَّ الدّراسة [3] عملِت على تصميم نظام إدارة هويَّة لإنترنت الأشياء في السّياق الصِّحي، إلاّ أنّها لم تقمُ بتوفير أي اتصال آمن، ممّا يجعل أجهزة إنترنت الأشياء قابلةً للوصول المُباشر من الإنترنت. تُقدمّ الدّراسة [10] منهجَ مُصادقة استناداً إلى الشّهادات، باستخدام DTLS، بحيث تهدف إلى تخفيض التَّكلفة النّاتجة عن الاتِّصال المطلوب لعمليَّة المُصادقة، هذهِ الدّراسة مِثل سابقاتِها لم تضع في اعتبارِها إضافة ميّزة تسجيل الدّخول الموحّد إلى إنترنت الأشياء. ولقد استخدم في الدّراسة [11] كل من بروتوكول LDAP وKerberos لإنجازِ كل من عمليةِ المصادقة وخدمة تسجيل الدّخول الموحّد في إنترنت الأشياء،

ولم يُؤخذ بالاعتبار وجود عنصر وسيط يقوم بملائمة الرّسائل المُرسلة بين الإنترنت وإنترنت الأشياء (أي تحويلُها لشكل مفهومٍ من قبل كل من مكدِّسي البروتوكولات الخاص بالإنترنت وإنترنت الأشياء). تم في الدّراسة [12] تصميم بروتوكول مصادقة مُوحّد FLAT، يجمع بين أنظمة التَّشفير المتماثلة والشّهادات الضّمنيَّة، مع تجاوز مبادئ التشفير غير المتناظر المُستخدمة في نظام FIDM التقليدي، ولم يؤخذ بالحسبان عمليَّات تفويض النَّفاذ، واكتشاف الخدمة، قدّمت الدّراسة [1] نموذجاً يقوم بدمج نظام إدارة الهويَّة IdM مع إنترنت الأشياء IoT محققاً خدمة تسجيل الدّخول الموحّد SSO استناداً لمفتاح تشفير محققاً تشفير البيانات بين طرفي الاتصال، لكنَّها لم تأخذ بالاعتبار محدوديَّة الموارد لإنترنت الأشياء. أما الدراسة [13] فقد قدمت إطاراً لإدارة الهوية من أجل تطبيقات الرعاية الصحية، بحيث يعتمد هذا الإطار على القياسات الحيوية لإجراء عملية المصادقة، وهذا من شأنه التخفيف من المشكلات التي يواجهها القطاع الصحي مع المرضى المسنين الذين يفتقرون إلى الخبرة في استخدام التقنيات الحديثة، إلا أن الإطار اختبر مع عدد قليل من المستخدمين بلغ فقط 25 مستخدماً. وأخيراً صممت الدراسة [14] معمارية لنظام إدارة الهوية الموزع استناداً إلى الشبكات المعرفة بالبرمجة، حيث استطاعت هذه المعمارية التخلُّص مما يدعى بمشكلة نقطة الفشل الوحيدة في النظام المركزي، كما وساهمت هذه الدراسة في حل مسألة الهوية الفريدة في شبكات انترنت الأشياء غير المتجانسة، لكنَّ مسألة تحديث المتحكمات دون مقاطعة عملية إجراء المصادقة لا تزال بحاجة إلى مزيد من الاختبارات.

لذا يتم في هذا البحث تصميم إطار جديد لإدارة الهوية يتلافى نقاط الضّعف التي تم ذكرها وذلك بجعل المعرّف أكثر فاعليَّة بالاعتماد على طريقة مُصادقة فعالة تستند إلى مفتاح لإنجازِ تسجيل دخول موحّد في إنترنت الأشياء. وتمّ اعتماد المُحاكاة الحاسوبية باستخدام برنامج المحاكاة Cooja للتحقّقِ من أداءِ الإطار المُقترح.

أهمية البحث وأهدافه:

تأتي أهمية البحث من تطّور الخدمات عبر الإنترنت، والتّي كانَ لها بالغ الأثر على كمية البيانات والمعلومات الشّخصية المنشورة عبر الإنترنت. ونظراً لكبر حجم البيانات المتاحة على الإنترنت، وبشكل خاص تلك الناتجة عن تبادل البيانات في تطبيقات إنترنت الأشياء، فإنَّه يتولد احتمال تواجد كيان غير معروف قادر على الوصول إلى المعلومات الخاصَّة بإنترنت الأشياء. يتم في هذا البحثَ تصميم نظام جديد لإدارة الهوية IdM، يُزوَّد بخدمة المصادقة وتفويض النفاذ في شبكة الإنترنت، بحيث يتم مكاملته مع IoT، حيث يتم في جهاز IoT تخفيض البيانات المرسلة وفقاً لسياق الطلب مما يؤدِّي إلى تخفيض في زمن الاستجابة اللازم لإرسال الاستجابات، مما يحسِّن من جودة الخدمة.

طرائق البحث ومواده:

يوفر نظام إدارة الهوية IdM كلاً من المصادقة وتفويض النفاذ لمستخدمي الإنترنت (إدارة معلومات هوية المستخدمين) [1]،[4]،[12]. ويمتلك هذا النظام أربعَةَ مكوناتٍ [5]،[1] هي:

1- الكيانات: هم المستخدمون أو الأجهزة.

2- المعرّفات (معرفات الكيانات): قد تكون هذه المعرّفات عبارة عن معرّف المستخدم (User Id)، البريد الإلكتروني (E-mail)، عنوان Url... إلخ.

3- مزود المعرّف Identity Provider (IdP): يقوم بعملية إدارة معرفات المستخدمين (هوياتهم)، وواصفات التوثيق (الوظائف، المناصب، والامتيازات)، مزوداً بأوراق الاعتماد المطلوبة لأجل تفويض النفاذ (الشهادات، الرّموز، القياسات الحيوية ... إلخ).

4- مزود الخدمة Service Provider (SP): يزود بالخدمات لأجل المستخدمين المفوضين وفقاً لمعرفاتهم وأوراق اعتمادهم.

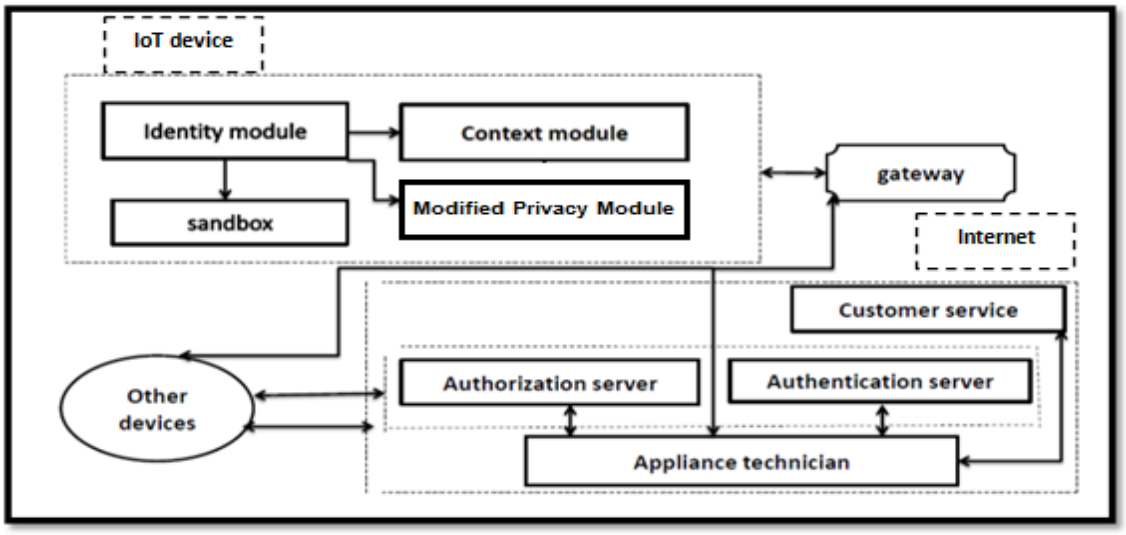
يتم في هذا البحث تقديم إطار جديد لإدارة الهوية قادر على جعل المعرّف أكثر فاعليَّة، حيث يتفادى الإطار المقترح سلبية تحميل جهاز إنترنت الأشياء المحدود الموارد عبء تطبيق السَّماحيات وذلك بتطبيق عملية مصادقة وتفويض نفاذ خارجية في سياق الإنترنت، عن طريق مخدّمات متخصّصة. ولقد تطلب تنفيذ التكامل الذي يقدمه إطار الهوية المقترح في هذا البحث القيام بالتعديل على وحدةِ الخصوصية.

نظام إدارة الهويَّة المقترح في انترنت الأشياء

يستند نظام إدارة الهويَّة المقترح على طريقة مصادقة مُشّفرة مع مراعاة عرض الحزمة في إنترنت الأشياء، بحيث يعمل الإطار الجديد لإدارة الهوية على تمكين إدارة التعريف من التمييز بين مستخدم الجهاز والجهاز بغرض عزل البيانات الشخصية على الأجهزة المشتركة، بحيث يتم تقييد استخدام الجهاز بالاعتماد على السياق المطلوب وتقليل المحتوى المرسل عبر الشبكة لتوفير عرض الحزمة المتاح. إذن فالإطار المقترح قائم على تكامُل ميِّزات الإنترنت مع إنترنت الأشياء بحيث يراعي هذا التكامل الإبقاء على خدمة تسجيل الدّخول الموحّد SSO، أي وراثتِها من نظام إدارة الهوية الموجود في شبكة الإنترنت، والتّي تمنح القدرة على نفاذٍ مؤقتٍ لعدّة أجهزة عن طريقِ عمليةِ مصادقةٍ واحدةٍ، بالإضافة لتحقيق اتصال آمن بين أطراف الاتصال (الإنترنت، وإنترنت الأشياء)، وهذا تم إنجازه في هذا البحث من خلال العمل على جعلِ الدّخول الموحّد يعتمد على مفتاح، وذلك بهدف تشفير البيانات بين طرفي الاتصال، أي بينَ سياقي الإنترنت وإنترنت الأشياء.

مكونات إطار إدارة الهويَّة المقترح

يتألَف إطار إدارة الهويَّة المُقترح وفقاً للشكل (1) من أربعة مُكوِّنات، بعضها يتواجد في شبكة الإنترنت وبعضها في شبكة إنترنت الأشياء. يتكون الجزء المُتواجد في شبكة الإنترنت من مجموعة عناصر تتفاعل مع بعضها البعض ومع شبكة إنترنت الأشياء والشَّبكات الأُخرى، وهي: خدمة الزَّبائن Customer Service (CS) فهي تزوَّد بواسطة المصنع، وتشكِّل واجهة اتِّصال بين التِّقني والجهاز، تقني الجهاز أو المصنع Appliance Technician يستجيب للطلبات مثل المراقبة، الصيانة، تحديث البرامج، أي أنَّهُ نظام مُدار من قبل المصنع لتلبية احتياجات الزبون بعد البيع، ولا يملك نفاذاً مباشراً إلى جهاز المستخدم، إنما يستخدم خدمة الزبون كوسيلة عبور أو نفاذ للجهاز ومخدِّم المصادقة Authentication Server الذي يتحقَّق من أوراق اعتماد تقني التَّطبيق ويوفِّر تسجيل دخول موحَّد لأجل المخطَّط المقترح، أمَّا مخدِّم تفويض النَّفاذ Authorization Server فيقدم رموزاً (tokens) لتقني التطبيق الذي تمت مصادقته، لكي ينفذ إلى كل من خدمة الزبون والبوابات.



الشكل (1): معمارية إطار إدارة الهوية المقترح في إنترنت الأشياء

أمَّا بالنِّسبة للجزء المتواجد في شبكة إنترنت الأشياء فهو يتكَّون من أربع وحدات أساسيَّة تعمل مع بعضها البعض على الجهاز المحدود الموارد كما تعمل مجتمعةً على استغلال مُعرِّف الجهاز الذي يمتلك القدرة على التَّمييز بين مُستخدم الجهاز والجهاز وذلك لانتقاء البيانات المَطلوبة وفق طلب الاتِّصال، حيث تجري عمليَّة الانتقاء هذه وفق خوارزميَّة تُطبَّق في وحدة الخصوصية. وهذه الوحدات هي: وحدة المعرِّف (الهويَّة) Identity Module والتي تتألَّف من معرف الجهاز وهو عبارة عن رقم تسلسلي ومفتاح تشفير متناظر (يُزودان من قبل المصنع خلال عمليَّة الإنتاج)، ومُعرِّف المستخدم وهو عبارة عن الرَّقم التسلسلي للجهاز ونوع المُستخدم، ويُخزَّن كل من المعرف والمفتاح المتناظر في خدمة الزَّبائن (CS). وتقوم وحدة العزل Sandbox Module بوظيفة العزل بين البيانات على الجهاز المُشترك، بمعنى أنَّ البيانات الشَّخصية لا يمكن أن يتم تشاركها أو النَّفاذ إليها من قبل المستخدمين الآخرين الَّذين يتشاركون ذات الجهاز، مما يؤمن وظائف أمن البيانات إلى الأشياء.

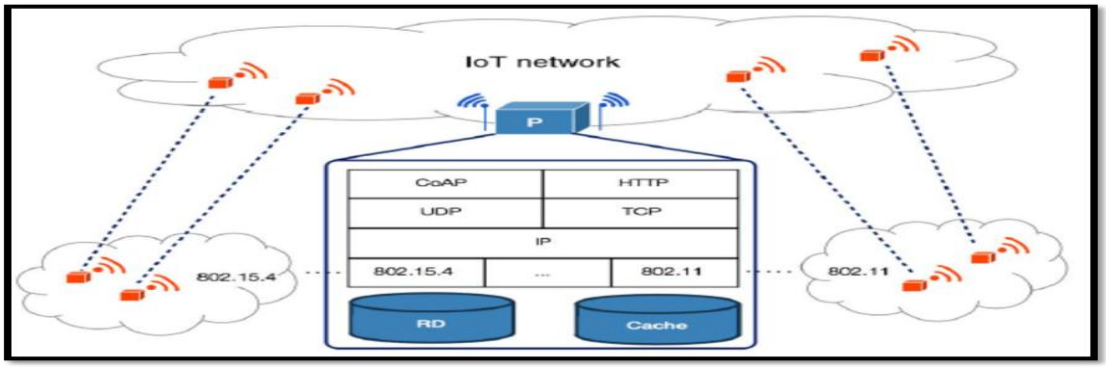
تعمل وحدة تتبُّع السِّياق Context Module على تتبُّع معرف الأشياء (الأجهزة) والمستخدمين بأسلوب ديناميكي، مقيدةً إمكانية استخدام الجهاز وفقاً للسياق الذي هو موجَّه لكي يُستخدم به. وقد تم استبدال وحدة الخصوصيَّة بوحدة الخصوصية المعَدلة Modified Privacy Module بحيث تتمكن من إرسال طلبات خدمة واستقبال استجابات، مما يتيح إزاحة حمل تطبيق سياسات الخصوصية (من توثيق وتفويض) من على عاتقِ جهاز إنترنت الأشياء إلى مخدّماتٍ خاصة خارجيَّة ممَّا يُحسِّن من أمن إدارة المعرِّفات IdM.

وتعمل البوابة Gateway كجسرٍ بين الإنترنت وإنترنت الأشياء، ممّا يعني أنّها تتعامل مع اثنين من المكدّساتِ البروتوكولية المختلفة، وفقاً للشكل (2)، وبما أنَّ لكل من المكدسين طبقة فيزيائية مختلفة، فإنَّ هذا يتطلب جهازي مرسل/مستقبل لهذهِ البوابة متعدّدة البروتوكولات [6].

أَما بالنِّسبة للمُكوِّن Other Devices فهو يمثِّل كلّ الأجهزة سَواءً أكانت محدودة الموارد أم لا والقابلة للنَّفاذ إلى الشَّبكة المقيَّدة IoT المدروسة.

آلية عمل إطار تحديد الهوية المُقترَح

إنَّ آليَّة عمل إطار تحديد الهويَّة المقترح تتمثَّل في التَّفاعُل بين مكونات الإطار المُقتَرَح وهي تتضمَّن عدة مراحل: أوَّلها تدفق البيانات للطّلب المُرسل من قبل الجهاز، أمَّا المرحلة الثانية فهي المصادقة وتفويض النفاذ لأجل التقني، المرحلة الثَّالثة تدعى تدفق بيانات الاتصال من جانب التقني، أما المرحلة الرَّابعة والأخيرة فهي تقوم على تخفيض البيانات المرسلة عبر الشَّبكة من خلال تطبيق خوارزمية توفير عرض الحزمة المُعدَّلة. وفيما يلي يتم توضيح تلك المراحل بالتَّفصيل.



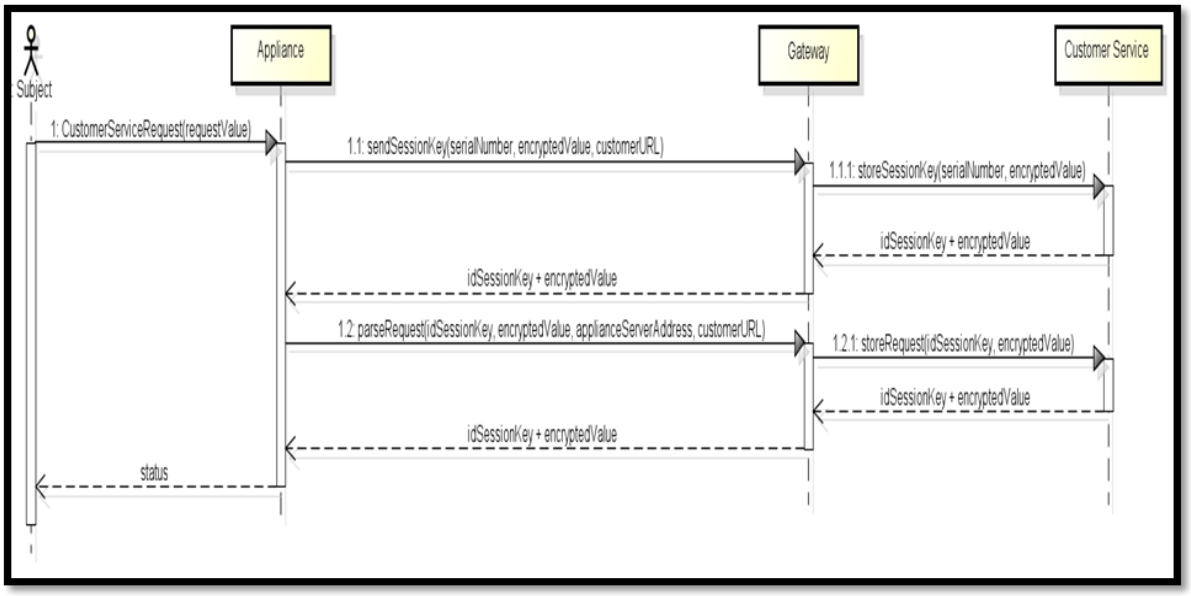
الشكل (2): معمارية بوابة إنترنت الأشياء مع الطبقات الدّاخلية [6]

في المرحلة الأولى الموضحة في الشّكل (3) يتم عرض تدفق البيانات للطلب المُرسل من قبل الجهاز، حيث أنَّ الطلب الذي يبدؤه الجهاز هو عبارة عن طلبِ خدمةٍ موجّه إلى خدمةِ الزّبون، وقد تكون الخدمة المضمّنة في طلب الخدمة عبارة عن تفعيل للتطبيق أو تنفيذ مهمة صيانة ... إلخ، حيث يطلب الزّبون (مُستخدم الجهاز) من التطبيق خدمةً مُزودةً بواسطة خدمة الزبون فيولّد تطبيق المستخدم ويستخدم مفتاح الجلسة KEK (Key Encrypting Key) ليشّفر محتوى الرّسائل المتبادلة خلال زمن حياة الطّلب.

علماً بأنَّ التطبيق يستخدم المفتاح KKM (Master Key Encrypting Key) أيضاً ليشّفر المفتاح KEK والختم الزّمني (time stamp). يُرسل التطبيق القيمة المشّفرة بالإضافةِ إلى معرّف الجهاز، وعنوان خدمة الزّبون إلى البوابة والتي تُترجم الرّسالة من جانب IoT إلى جانب الإنترنت (التّرجمة مطلوبة نظراً لاستخدامِ بروتوكولين مختلفين على كلِّ جانب)، ثمّ تمرّرها إلى خدمةِ الزّبون. تسترد خدمة الزبون المفتاح KKM من الرّقم التسلسلي، وتفك تشفير البيانات، ثمَّ تتحقّق من المفتاح KEK، بواسطة استخدام الختم الزمني (تجنباً للهجمات). من بعد ذلك تخزّن الخدمة مفتاح الجلسة لتستخدمهُ في تشفير وفك تشفير الرّسائل المستقبلية، التّي سوف يتم تبادلها مع التطبيق (خلال هذه الجلسة فقط). تعيد بعدئذٍ خدمة الزّبون إلى التطبيق دليلَ مفتاحِ الجلسة مع الختم الزّمني مضافاً إليه واحد، فتستقبل البوابة الرّد وتربط دليل مفتاح الجلسة KEK مع عنوان التطبيق.

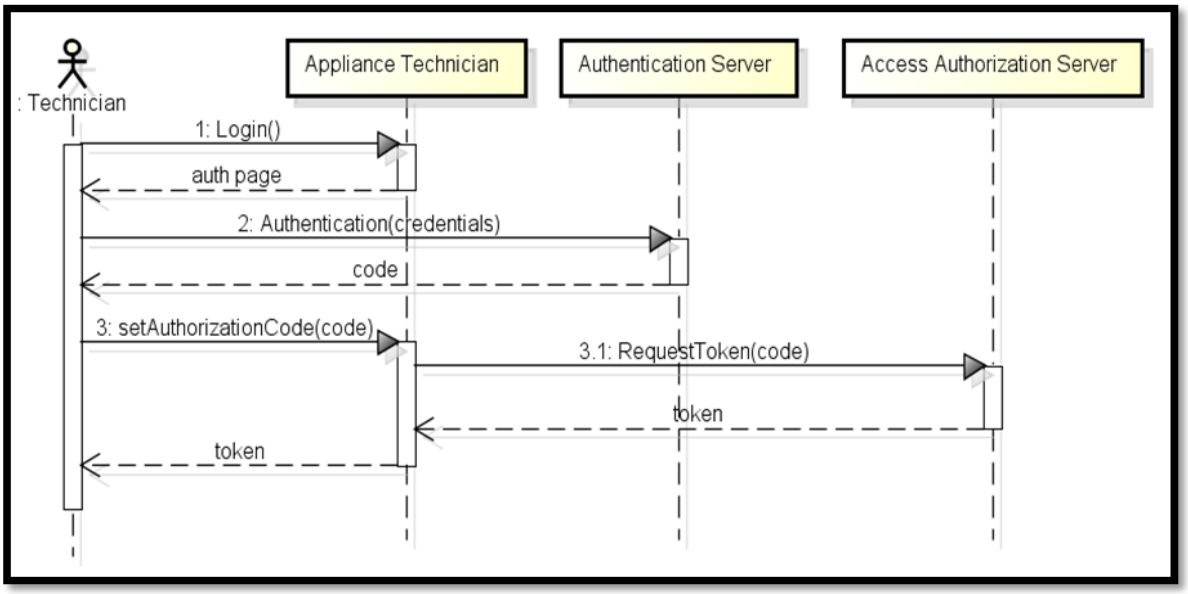
وتحوّل البوابة الرّسالة من سياق الإنترنت إلى سياق إنترنت الأشياء وتمرّرها إلى التطبيق والذي يستقبل بدوره الرّسالة المشّفرة بواسطة KEK، حيثُ يفك تشفيرها، ويتأكد من الختم الزّمني، ويقوم بعده بتشفير الطّلب مع ختمٍ زمني جديد ويرسلهُ إلى البوابة، بالإضافةِ إلى دليل مفتاح الجلسة المستخدم للتواصل مع خدمة الزّبون، والتي تسترد بدورها مفتاح الجلسة من خلال دليله المُرسل، ثمّ تفك تشفير الطّلب وتخزّنه حتّى يُصار إلى الرّد عليه من قبل التّقني وتعيد دليل

مفتاح الجلسة مجدّداً مع الختم الزمني إلى التطبيق الذي يستقبل الاستجابة، ويتأكد من الختم الزمني، ثمّ يقوم بتبليغ المستخدم بحالةِ الطّلبِ المُرسل.



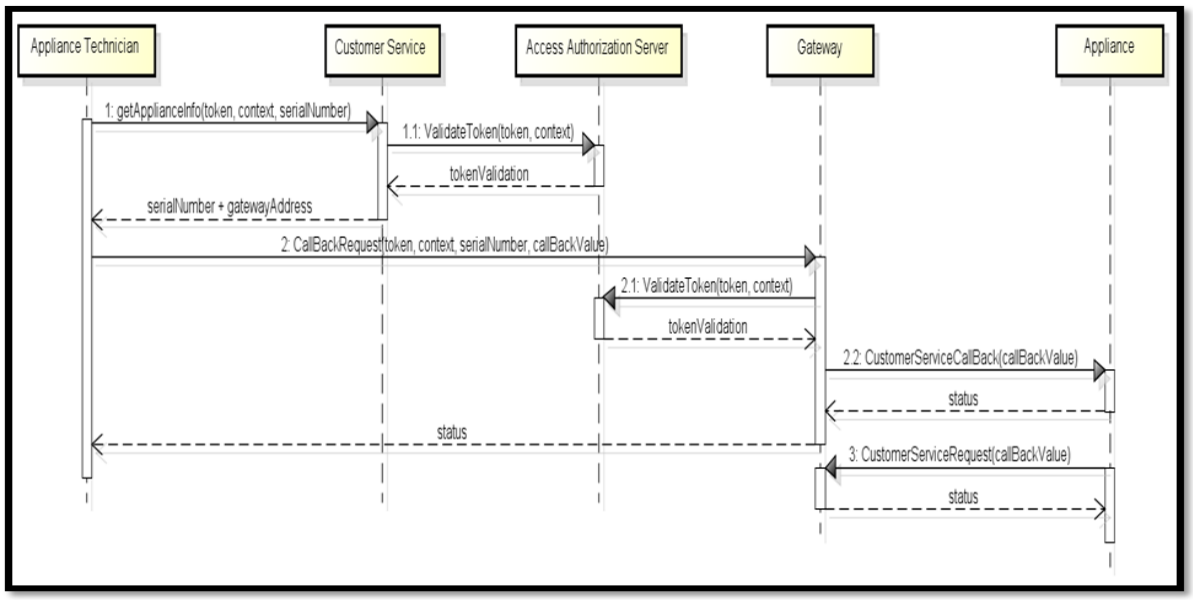
الشكل (3): تدّفق الرّسائل للطّلب المُنشأ من قبل التطبيق

المرحلة الثانية ويتم فيها المصادقة وتفويض النفاذ للتقني كما في الشكل (4) الذي يبين تدّفق الرّسائل المطلوبة للقيام بالمصادقة وتفويض النفاذ من أجل التقني. تبدأ المرحلة هذه بطلب التقني النفاذ إلى تطبيق المستخدم لتلبية طلبات المستخدمين، حيث يُعاد توجيهه إلى مخدّم التوثيق مع أوراق الاعتماد المطلوبة (الشّهادة)، والذي يتأكد بدوره من أوراق اعتماد التقني ويرد بكود (رمز) والذي يُستخدم من قبل التقني لطلبِ علاّمِ نفاذٍ من مخدّم التفويض، فيُعيد المخدّم علاماً يُستخدم من قبل التقني للاستجابةِ لطلبِ الزّبون. بعد إتمام عملية التوثيق والتفويض للتقني، سيصبح بإمكانهِ النفاذ إلى طلب البيانات باستخدام تطبيق التقني، حيثُ يسترد تطبيق التقني مفتاح الجلسة KEK ودليله، ثمّ يفك تشفير الطّلب، ويعالجه، ليمرّره من بعد تشفيره إلى البوابة التي تستقبل بدورها الاستجابة المشّفرة مع علاّم النفاذ (يتم التحقّق منه بواسطة التراسل مع مخدم التفويض)، لتمرر هذه الاستجابة المشفرة من بعد ذلك إلى تطبيق المستخدم الذي يفك تشفير الاستجابة بواسطة المفتاح KEK الذّي حصل عليه بالاعتماد على الدّليل، وأخيراً يجري العمل على معالجة الرّسالة الواردة.



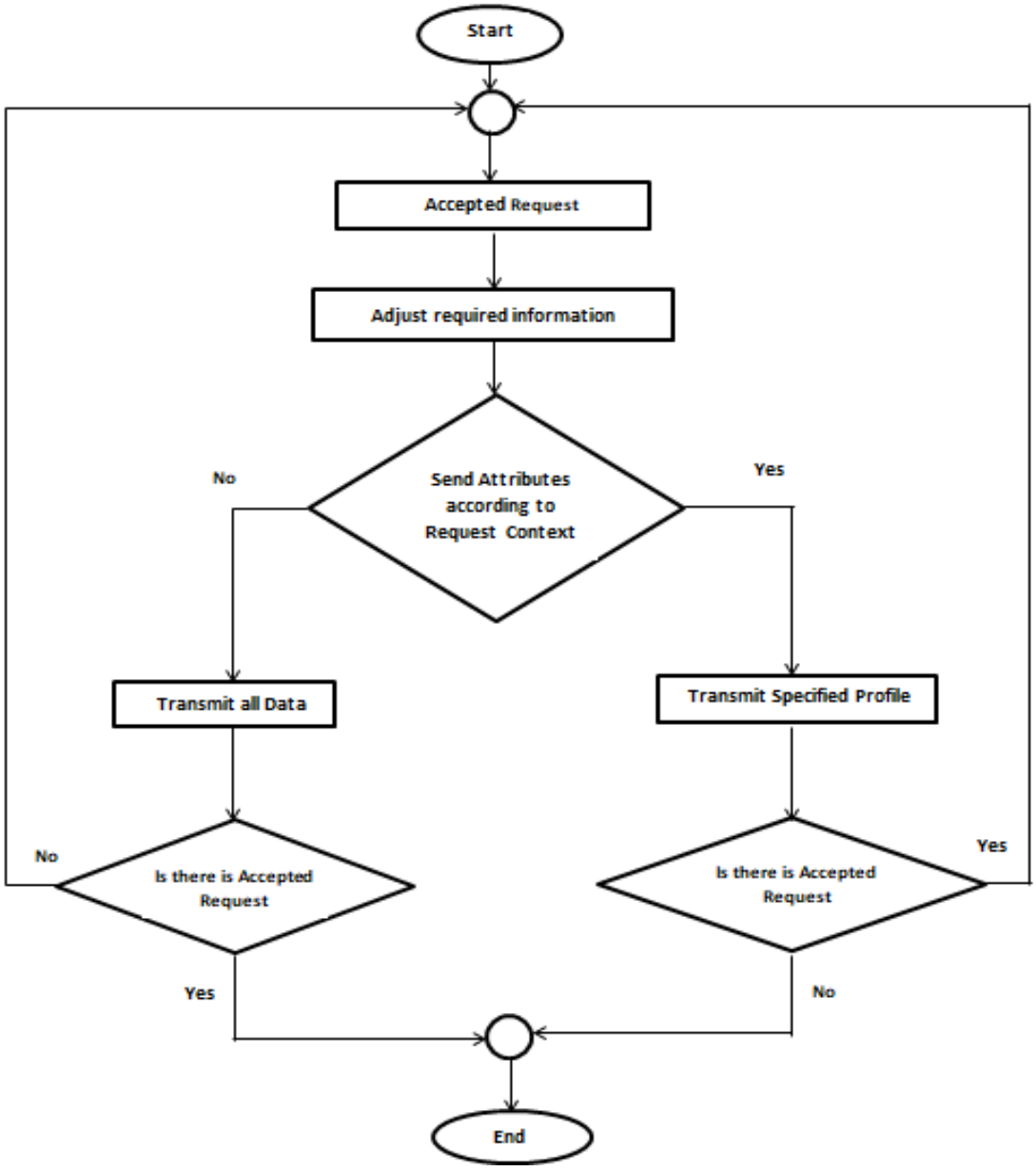
الشكل (4): المصادقة وتفويض النفاذ لأجل التقني

المرحلة الثالثة تبين تدفق بيانات الاتصال من جانب التقني، حيث يحدث هذا النّوع من الاتصال عندما يريد التّقني أن يجمعَ معلوماتٍ أو يحدّثَ تطبيق المستخدم على سبيل المثال، وهذا التدّفق يُوضّحه الشكل (4). فعلى افتراض أنَّ التّقني قد وثّق وفوّض، فإنّهُ يستخدم تطبيقه ليطلب من خدمةِ الزّبون CS بعض البيانات عن تطبيقِ المُستخدم، مُزوداً بالعلاّم والرّقم التسلسلي. تتحقّق خدمة الزّبون من العلاّم، وتجيب على طلب التقني فيما يخص بيانات التطبيق، حيث تتضمن هذه الإجابة عنوان البوابة، التّي تتصل مع التطبيق الهدف. بعدها يطلب تطبيق التقني من بوابة تطبيق الجهاز إقامة اتصال فيما بينهما، فتتحقق البوابة من علاّم التقني، ثُمَّ تُعلم التطبيق بطلب التقني.



الشكل(5): تدّفق الرّسائل من التقني إلى الجهاز الهدف

أما المرحلة الرابعة التي تلي مراحل التشفير، فهي مرحلة توفير عرض الحزمة المُتاح ويتم فيها تطبيق الخوارزمية المعدَّلة المُقترحة لتوفير عرض الحزمة والموضحة في الشكل (6). ولقد تمَّ تعديل عمل خوارزمية توفير عرض الحزمة بحيث يُصبح على النّحو الآتي:



الشكل (6): مخطط الخوارزمية المعدّلة لتوفير عرض الحزمة

إنَّ خوارزمية توفير عرض الحزمة المُعدَّلة تُستَدعى عند تلقِّي طلب بيانات خارجي Accepted request، علماً أنَّ طلبَ البيانات مقبول من ناحية الموثوقية والتفويض، وذلكَ من أجلِ تقليل كمية البيانات المراد إرسالها وفقاً لسياق الطّلب. وتسمح Adjust required information للمستخدمين بالتقليل من كمية البيانات المُرسلة إلى العقدة

(الجهاز) الهدف، حيث يتم فيها مقارنة واصفات طلب البيانات مع واصفات ملف المستخدم، لكن ذلك لن يكون إلاّ بموافقةِ المستخدم، حيثُ يترك لهُ الخيار فيما إذا كان يرغب بذلك أم لا.

ولابدَّ من الإشارةِ إلى أنَّ عدمَ موافقةِ المستخدم على خيارِ التّوفير سيؤدِّي لإرسال كامل البيانات دون القيام بعملية التوفير الانتقائي، وهذا يُظهر مرونة النموذج المقترح، وقدرته على تأمين التّوافقية مع أنظمة تدمج IdM مع إنترنت الأشياء في ظل مراعاة الاتصال الآمن فقط، دون الانتباه إلى كلٍّ من موارد الجهاز والشبكة. أمّا تفعيل خيار التّوفير فإنَّه يقود الخوارزمية إلى العمل على فلترةِ الواصفاتِ المرسلة إلى حدودها الدنيا (كل مجموعة واصفات attributes تشكّل ملفاً تعريفياً (profile))، أي انتقاء الملّف التعريفي المناسب لسياق الطلب، وإرساله. وتُكرّر هذهِ الخوارزمية مع استلامِ كلِّ طلب بيانات موثّق.

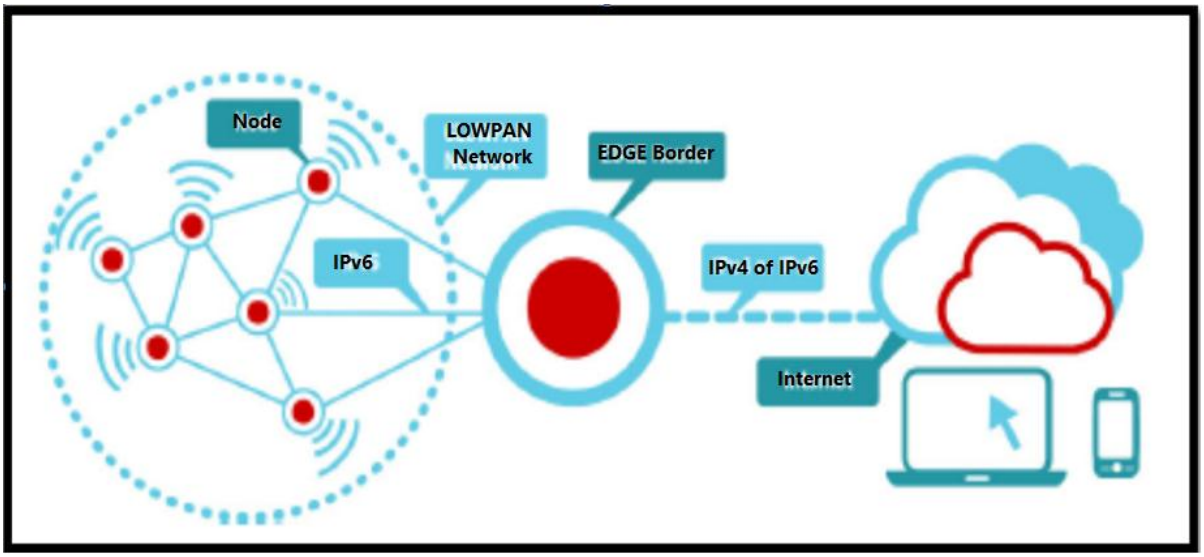
يُلاحَظ عند تطبيق خوارزمية توفير عرض الحزمة المعدَّلَة المُقتَرحة والمُعتمَدة في تصميم الإطار الجديد، أنَّ الجهاز لن يستلم إلاَّ ما هو مُصادق عليه أي خضع لتوثيق وتفويض خارجي ضمن شبكة الإنترنت، ممَّا يؤدي إلى إزاحة عبء تطبيق سياسات الخصوصيَّة من على عاتق جهاز إنترنت الأشياء وما يتبعه من تخفيض التعقيد الناتج عن تحميل المعالج قدرة حسابية كبيرة.

النتائج والمناقشة:

تم تقييم إطار الهوية المقترح باستخدام المُحاكي Cooja، وهو محاكي شبكات يعتمد نظام التشغيل Contiki [15]، والذي يسمح للمطّورين بتشغيلِ تطبيقاتِهم واختبارها. تم إجراء سيناريوهات كان الهدف منها تقييم إطار إدارة الهوية المقترح وفقاً لمعيارِ زمنِ الاستجابة، وذلكَ كتابعٍ لبارامترينِ، هما حجم الطّلبات المُرسلة وعدد الأجهزة. ويمكن تبرير اختيار هذا المعيار، بالنظر إلى كونهِ عاملاً مؤثراً في مفهوم جودة الخدمة المُقدّمة بواسطة الإطار المُقترح. حيثُ لا بُدَّ من قياس ما تفرضهُ عملية تأمين قناة الاتصال بين سياقي الإنترنت وإنترنت الأشياء من عبءٍ زمنيٍّ، ينعكس على هيئةِ تأخيرٍ في الاستجابة للطلبات المُرسلة من قبل الأجهزة.

ولقد تمَّ اعتماد بيئة المنزل الذّكي لدراسة السّيناريوهات المقترحة وفق المخطط المبيَّن في الشكل (7). حيث يُلاحَظ فيه أنَّ الشبكة المستخدمة في سياق إنترنت الأشياء، هي شبكة لاسلكية من النّوع (ZigBee) IEEE802.15.4. وتم تفعيل بروتوكول CoAP (بروتوكول التطبيقات المقيّدة) في سياق IoT، وهو عبارة عن بروتوكول طبقة تطبيقات، يُستخدم مع العقد والشبكات ذاتِ الموارد المحدودة، وهو ضروري على اعتبار أنَّ البروتوكولات التقليدية ثقيلة على الأجهزة ذات الذّاكرة المحدودة، أي هو بديل عن البروتوكول HTTP بالنسبةِ لتلكَ الأجهزة. كما تمَّ تفعيل البروتوكول HTTP في سياق الإنترنت.

ويبيِّن الجدول(1) البارامترات المعتمدة لنظام إطار إدارة الهويَّة المقترح من أجل إجراء السيناريوهات لاختبار النظام المقترح.



الشكل(7): مخطط نظام إطار تحديد الهويّة المقترح

الجدول (1): بارامترات المحاكاة

البارامتر	القيمة
الحزمة الترددية	2.4GHz (ISM)
معدل الإرسال	250 kbps
الرّقاقة الرّاديوية (البطاقة اللاسلكية)	CC2420 RF
استهلاك الطّاقة في حالة الإرسال	17.4 mA
استهلاك الطّاقة في حالة الاستقبال	18.8 mA
استهلاك الطّاقة في حالة الخمول (الاستماع)	426 µA
استهلاك الطّاقة في حالة النّوم	20 µA
ميزات طبقة التحكم في الوصول إلى الوسط (MAC)	Encryption with AES-128 bit CSMA/CA Retransmission
نوع العقدة	TmoteSky
نظام التشغيل	Contiki 3.0

سيناريوهات دراسة تأثير زيادة حجم الطلب على زمن الاستجابة في ظل تغيير عدد الأجهزة

اقتضت دراسةُ تأثيرِ زيادةِ حجم الطّلب على زمن الاستجابة في ظلِّ تغيير عدد الأجهزة القيام بِـ 24 سيناريو. إنَّ زمنَ الاستجابة كمعيارٍ شبكي يُعرّف بأنّهُ الزّمن المطلوب لتلبية الطّلب أي الحصول على استجابة، وذلك بدءاً من زمنِ إرسالِ الطّلب من قبلِ العقدةِ اللاسلكية إلى الجهة المعنية بتقديم الخدمة.

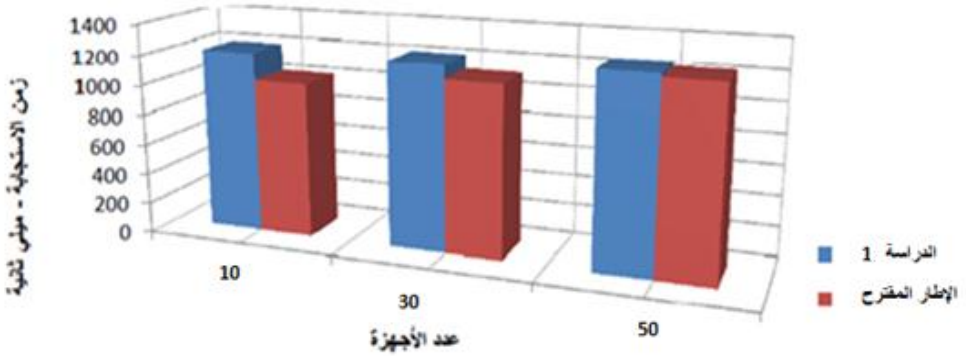
تمَّ تقييم أداء إطار تحديد الهويَّة المُقترَح وفقاً لبارامترين هما:

- ✓ إرسالِ المستخدم رسائلَ طلبٍ متغيرة الحجم تأخذ القيم التالّية: 32، 512، 1024، 4096 بايت (وهو حجم الحمولة الصافية الأعظمي الذّي تقبله الشبكة).
- ✓ تفعيل عدد متغير من الأجهزة في نطاق إنترنت الأشياء (خلف البوابة GW). وهذا العدد يأخذ القيم التّالية: 10، 30، 50 تطبيق (وهو عدد التّطبيقات/الأجهزة المنطقي المُمكن تواجده في بيئة المنزل الذّكي والعدد 50 يمثل العدد الأعظمي لها).

وقد تمَّ إجراء السِّيناريوهات أيضاً على النَّموذج المُقترَح في الدِّراسة [1] التي لم تعتمد خوارزميَّة توفير عرض الحزمة من أجل إجراء المقارنة مع النموذج المقترح.

تبيِّن الأشكال (8) و(9) و(10) و(11) مخططات زمن الاستجابة كتابع لزيادة عدد الأجهزة من أجل حجم طلبات 32، 512، 1024، 4096 بايت، على التَّوالي، وذلك لإطار تحديد الهويَّة المُقترَح بالمُقارنة مع النَّموذج في الدِّراسة [1]. نلاحظ تمكّن نموذج إطار تحديد الهوية المقترح من تحقيق زمن استجابة أقل من النموذج المُقارَن به، وهذا يُمكن تفسيرهُ من خلال قيام النموذج المقترح بتخفيض كمية البيانات المُرسلة عبر الشبكة، ممّا يقلّل من زمن النفاذ للشبكة، وبالتّالي ينعكس إيجاباً على زمنِ الاستجابة.

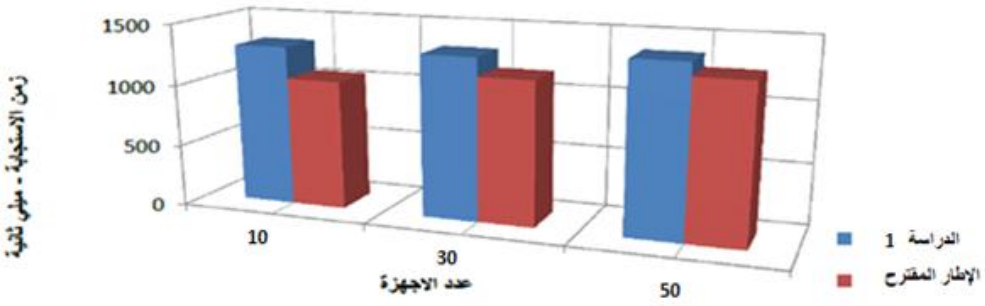
بيَّنت الجداول (1) و(2) و(3) و(4) أنَّ زمن استجابةِ النّموذج المقترح، يزداد مع زيادة عدد الأجهزة في شبكة إنترنت الأشياء، وتثبيت حجم الطّلب المُرسل من قبل المستخدم، لكنّهُ يبقى أقل من النموذج المُقَارَن به في الدراسة [1]، فضلاً على أنَّ زمنَ الاستجابة لكلا النموذجين يزداد مع زيادةِ حجمِ الطّلباتِ المُرسلة.



الشكل(8): زمن الاستجابة كتابع لزيادة عدد الأجهزة عند حجم طلب يبلغ 32بايت

الجدول(2): زمن الاستجابة لإطار إدارة الهوية المقترح مقارنة مع الإطار المقترح في الدراسة [1]عند حجم طلب 32 بايت

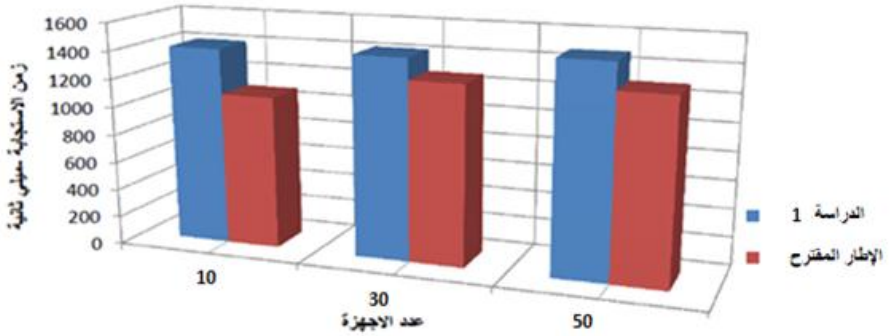
عدد الأجهزة	10	30	50
الدراسة [1]	1207 m.s	1219 m.s	1261 m.s
الإطار المقترح	1025 m.s	1126 m.s	1236 m.s



الشكل(9): زمن الاستجابة كتابع لزيادة عدد الأجهزة عند حجم طلب يبلغ 512بايت

الجدول(3). زمن الاستجابة للإطار المقترح مقارنة مع الإطار المقترح في الدراسة [1]عند حجم طلب 512 بايت.

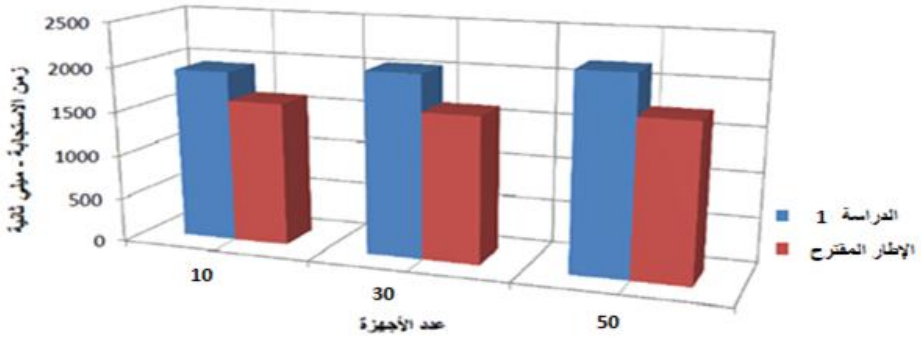
عدد الأجهزة	10	30	50
الدراسة [1]	1305 m.s	1315 m.s	1371 m.s
الإطار المقترح	1051 m.s	1165 m.s	1265 m.s



الشكل(10): زمن الاستجابة كتابع لزيادة عدد الأجهزة عند حجم طلب يبلغ 1024بايت

الجدول(4). زمن الاستجابة للإطار المقترح مقارنة مع الإطار المقترح في الدراسة [1]عند حجم طلب1024 بايت.

عدد الأجهزة	10	30	50
الدراسة [1]	1409 m.s	1425 m.s	1483 m.s
الإطار المقترح	1088 m.s	1275 m.s	1294 m.s



الشكل(11): زمن الاستجابة كتابع لزيادة عدد الأجهزة عند حجم طلب يبلغ 4096بايت

الجدول(5). زمن الاستجابة للإطار المقترح مقارنة مع الإطار المقترح في الدراسة [1]عند حجم طلب4096 بايت.

عدد الأجهزة	10	30	50
الدراسة [1]	1936 m.s	2045 m.s	2187 m.s
الإطار المقترح	1621 m.s	1638 m.s	1741 m.s

الاستنتاجات والتوصيات:

أظهرت النتائج بأنَّ إطار إدارة الهويَّة المُقترح ذو أداء جيد وذلكَ عند تقييمه من ناحيةِ المعيار الشّبكي وهو زمن الاستجابة وذلك في ظلِّ تغيير كلٍّ من عدد الأجهزة وحجمِ الطّلبات المُرسلة. وتمَّ التَّوصل إلى الآتي:

- ✓ يقل زمن استجابة جهاز إنترنت الأشياء عند زيادة عدد الأجهزة وبتثبيت حجم الطلب.
- ✓ إنَّ تطبيق خوارزميَّة تخفيض عرض الحزمة المعدَّلة وفقاً لسياق الطلب أدى إلى تقليل كمية البيانات المرسلة مما انعكس إيجاباً على زمن الاستجابة.
- ✓ حقق إطار تحديد الهوية المقترح أمناً للبيانات المتبادلة بين طرفي الاتصال (الإنترنت وإنترنت الأشياء) باستخدام التشفير المتناظر.
- ✓ إنَّ تطبيق خدمة تسجيل الدخول الموحد SSO أدَّى لإزاحة عبء تطبيق سياسات الخصوصيَّة من على عاتق الجهاز إلى مخدمات خارجية خاصة.
- ✓ تفوق النموذج مع استخدام إطار تحديد الهوية المقترح على النموذج في الدراسة [1] التي لم تعتمد خوارزميَّة توفير عرض الحزمة.
- ✓ عليهِ يُوصى باستخدامِ الإطارِ المُقترح كآليةٍ للمصادقة وتفويض النفاذ من أجل أجهزة إنترنت الأشياء ذات الموارد المحدودة، إذ استطاع المُحافظة على جودة الخدمة مع قدرته على توفير قناة اتصال آمنة وتسجيل دخول موحّد.

الأعمال المُستقبلية:

دراسة تأثير إطار تحديد الهويَّة المُقترح على استهلاك طاقة المعالج في الأجهزة محدودة الموارد (أجهزة إنترنت الأشياء).

References:

[1] WITKOVSKI, A.; SANTIN, A.; ABREU, V.; MARYNOWSKI, J. *An IdM and Key-based Authentication Method for providing Single Sign-On in IoT*. IEEE Global Communications Conference (GLOBECOM). December 2015.

[2] ATZORI, L.; IERA, A.; MORABITO, G. *The Internet of Things: A survey*. Computer Networks, vol. 54, no. 15, 2010, pp. 2787–2805

[3] CHIBELUSHI, C.; EARDLEY, A.; ARABO, A. *Identity Management in the Internet of Things: the Role of MANETs for Healthcare Applications*. Computer Science and Information Technology Vol. 1(2), 2013, pp. 73 – 81.

[4] ZHU, X.; BADR.Y. *Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions. Sensors.* 1 Dec. 2018.

[5] BELAPURKAR,A.; CHAKRABARTI,A.; PONNAPALLI,H.; VARADARAJAN, N.; PADMANABHUNI, S.; SUNDARRAJAN, S. *Distributed Systems Security: Issues, Processes and Solutions*, John Wiley & Sons, 2009.15.

[6] Liu, J.; Xiao,Y.; Chen, C. L. P. *Authentication and Access Control in the Internet of*

Things. Proc. of the ICDCSW - 32nd International Conference on Distributed Computing Systems Workshops, 2012, pp. 588–592.
[7] FREMANTLE, P.; AZIZ, B.; KOPECKY, J.; SCOTT, P. *Federated Identity and Access Management for the Internet of Things*. in Proc. of the International Workshop on Secure Internet of Things, 2014, pp. 10–17.
[8] LEO, M.; BATTISTI, F.; CARLI, M.; NERI, A. *A federated architecture approach for Internet of Things security*. in Proc. of the EMTC- Euro Med Telco, 2014, pp. 1–5.
[9] CIRANI, S.; PICONE, M.; GONIZZI, P.; VELTRI, L.; FERRARI, G. *IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios.* In IEEE Sens. J., vol. 15, no. 2, pp. 1224– 1234, 2015.
[10] HUMMEN, R.; ZIEGELDORF, J. H.; SHAFAGH, H.; RAZA, S.; WEHRLE,K. *Towards Viable Certificate-Based Authentication for The Internet of Things.* In Proc. of the Hot WiSec- Hot topics of the Hot WiSec- Hot topics on Wireless Network Security and Privacy, 2013, p. 37.
[11] LI, N.; WANG, Q.; DENG, Z. *Authentication framework of IIEDNS Based on LDAP & Kerberos.* In Proc. of the IC-BNMT- 32nd International Conference on Broadband Network and Multimedia Technology, 2010, pp. 695–699.
[12] SANTOS, MARIA L. B. A.; CARNEIRO, JÉSSICA C.; FRANCO, ANTÔNIO M. R.; TEIXEIRA, FERNANDO A.; HENRIQUES, MARCO A.; OLIVEIR LEONARDO B. *A Federated Lightweight Authentication Protocol for the Internet of Things.* In Science Direct. Volume 107, 1 October 2020.
[13] Farid, F.; Elkhodr, M.;Sabrina, F.; Ahamed, F.; Gide, E. A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. Sensors 2021, 21, 552. https://doi.org/10.3390/s21020552.
[14] CIRANI, S.; DAVOLI, L.; FERRARI, G.; LEONE, R.; MEDAGLIANI, P.; PICONE, M.; VELTRI, L. *A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things.* IEEE Internet of Things Journal, October 2014.
[15] The Contiki Operating System. [Online]. Available: http://www.contikios.org, accessed Sep. 15, 2019.
[16] A. DUNKELS, J.; ERIKSSON, N. F.; Tsiftes, N. *Powertrace: Network level Power Profiling for Low-power Wireless Networks*. Swedish Institute. Comput. Sci., Kista, Sweden, Tech. Rep. T2011:05, Mar. 2011.
[Online]. Available: http://soda.swedish-ict.se/4112/1/T2011_05.pdf
[17] Sadique, M,K.; Rahmani,R.; Johannesson,P.; Identity Management in Internet of Things: A Software Defined Networking Approach. Proceedings of the 2nd International Conference on Communication, Devices and Computing pp 495504. 17 December 2019.