مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (١٠) العدد (٨) ٢٠٢٦

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (8) 2026

تحقيق الاتصال الآمن بين الخدمات باستخدام قواعد تحكم ذكية

د. أليدا اسبر

(تاريخ الإيداع ٢٠٢٦/٢/١٥ . قُبِل للنشر في ٢٠٢٦/٥/٤)

□ ملخّص □

إن تحقيق الاتصال الآمن بين الخدمات يُعد عاملاً مهماً لتمكين التشغيل البيني بشكل فعال وموثوق. من الضروري جداً الحد من المخاطر التي قد تنشأ عند تحقيق التعاون بين الخدمات لأن الاتصال الموثوق هو الأساس الذي تبنى عليه الأنظمة في ظل التطور التكنولوجي، خاصة في المجالات الحيوية مثل التجارة الإلكترونية، والتعليم، والنقل، والرعاية الصحية، والترفيه، وإنترنت الأشياء IoT والأجهزة المنزلية الذكية، والمراقبة الأمنية، وغيرها.

لضمان نجاح هذا التعاون نحتاج إلى بيئة مثالية لتبادل البيانات وحمايتها من أي وصول غير مصرح به. حيث تتمثل المشكلة الأساسية التي يعالجها هذا البحث في محدودية الأنظمة الحالية للتعامل مع الطبيعة الديناميكية للخدمات المترابطة، حيث تفتقر معظم الأنظمة التقليدية إلى التكيف السياقي متعدد الأبعاد(زمني، بيئي،تشغيلي)، والإستباقية في إدارة التعارضات قبل حدوثها، والنمذجة الرياضية الموحدة التي تدمج المتطلبات الوظيفية والأمنية والسياقية.

قدم هذا البحث منهجية مطورة قائمة على قواعد منطقية ذكية لإدارة الوصول وتحديد الصلاحيات بدقة لتنفيذ المهام المطلوبة، والتحقق من التناقضات بين السياسات الأمنية للخدمات المترابطة مما يسهم في بناء بيئة خدمات متكاملة موثوقة وأمنة، يثبت النموذج فعاليته من خلال توفير إطار عمل رياضي يضمن السلامة والموثوقية قابل للتطبيق في الأنظمة الذكية، كما يتجلى ذلك في التطبيق العملي على نظام البيت الذكي.

حيث تم دمج الأبعاد السياقية المتعددة بنموذج واحد لتوحيد الرؤية بين الأمن والتشغيل والكفاءة حيث تم التركيز على المرونة والاستباقية في التعامل مع التحديات المتعددة، بالإضافة إلى التحويل من معالجة المشاكل إلى منع المشاكل وتوفير في التكاليف والوقت.

الكلمات المفتاحية: الخدمة، الاتصال الآمن، قواعد التحكم، إدارة الوصول السياقي.

*أستاذ مساعد في كلية الهندسة المعلوماتية جامعة حمص، قسم هندسة البرمجيات ونظم المعلومات

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (١٠) العدد (٨) ٢٠٢٦

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (8) 2026

Achieving Secure Inter-Service Communication Using Intelligent Control Rules

Dr.Alida ESBER*

(Received 15/2/2026. Accepted 4/5/2026)

□ ABSTRACT □

Achieving secure communication between services is an important factor for enabling effective and reliable interoperability. It is very necessary to reduce the risks that may arise when achieving cooperation between services, because reliable communication is the foundation upon which systems are built, especially in light of technological development, particularly in vital fields such as e-commerce, education, transportation, healthcare, entertainment, the Internet of Things (IoT), smart home appliances, security monitoring, and others.

To ensure the success of this cooperation, we need an ideal environment for data exchange and protecting it from any unauthorized access. The main problem addressed by this research is the limitation of current systems in dealing with the dynamic nature of interconnected services, as most traditional systems lack multi-dimensional contextual adaptation, proactivity in managing conflicts before they occur, and a unified mathematical model that integrates functional, security, and contextual requirements.

This research presents a developed methodology based on intelligent logical rules for managing access and accurately determining permissions to perform required tasks, and verifying inconsistencies between security policies of interconnected services, which contributes to building an integrated, reliable, and secure service environment. The model proves its effectiveness by providing a mathematical framework that ensures safety and reliability, applicable to smart systems, as demonstrated in the practical application on a smart home system.

Multiple contextual dimensions were integrated into a single model to unify the vision between security, operation, and efficiency, with a focus on flexibility and proactivity in dealing with multiple challenges, in addition to shifting from problem handling to problem prevention, saving costs and time.

Keywords: Service, Secure Communication, Control Rules,Contextual Access Management.

* Assistant Professor of Software Engineering, Homs University

مقدمة

إن تطور التكنولوجيا شهد تحولاً جذرياً في أنظمة التشغيل البيني، حيث أصبحت أنظمة الخدمات المترابطة حجر الأساس في البنى التحتية لبناء الأنظمة الحديثة. أدى هذا التحول إلى ظهور تحديات أمنية معقدة تتعلق بإدارة السياسات المتباينة والتحكم في الوصول الديناميكي. تكمن الإشكالية الأساسية في محدودية الأنظمة الحالية في التعامل مع الطبيعة الديناميكية للخدمات المترابطة، حيث تفتقد معظم الأنظمة التقليدية للقدرة على التكيف السياقي والاستباقية في إدارة التعارضات.

حيث تكمن المشكلة في أن لكل خدمة سياسات أمنية (**Security & privacy**) وخصوصية خاصة بها. عند محاولة دمج هذه الخدمات تتولد تناقضات أمنية تعيق عملية التشغيل (الاتصال بين الخدمات). على سبيل المثال قد تسمح سياسة إحدى الخدمات بالوصول إلى بيانات معينة بينما تمنعها سياسة خدمة أخرى مرتبطة بها. لذلك يهدف هذا البحث لتقديم نموذج يعتمد على قواعد منطقية ذكية لإدارة التفاعلات بين الخدمات بشكل آمن. يعتمد هذا النموذج على مجموعة قواعد يتم من خلالها التحقق من سياق التشغيل قبل تنفيذ أي إجراء، مما يضمن منع التعارضات المحتملة.

هدف وأهمية البحث

هدف البحث لتقديم نموذج رياضي متكامل يربط بين المتطلبات الوظيفية والأمنية والسياقية قابل للتحقق والبرهنة وقابل للتطبيق في أنظمة ذكية وقابل للتوسع نحو الأنظمة الذكية الآمنة (مدن أو مصانع ذكية) والقابلة للتشغيل البيني.

بالإضافة لدمج الأبعاد السياقية المتعددة (زمنية، بيئية، تشغيلية) بنموذج واحد لتوحيد الرؤية بين الأمن والتشغيل والكفاءة حيث تم التركيز على المرونة والاستباقية في التعامل مع التحديات المتعددة. بالإضافة إلى التحويل من معالجة المشاكل إلى منع المشاكل وتوفير في التكاليف والوقت.

اعتمد هذا البحث على منهجية نظرية رياضية في بناء النموذج المقترح والتحقق من صحته ،حيث تم استخدام أدوات المنطق الرمزي لصياغة قواعد التحكم في الوصول وتحديد الصلاحيات بدقة لتنفيذ المهام المطلوبة.

الدراسات المرجعية

تشكل أنظمة التشغيل البيني بين الخدمات تحدياً كبيراً، تعتبر البنية خدمية التوجه SOA (Service Oriented Architectural) من البنى الأكثر استخدامًا لحل مشكلة التعاون بين الخدمات، حيث وجدت البنية خدمية التوجهSOA (LOMOW.2005)لتقدم حلاً يتكيف مع مشكلة قابلية التشغيل البيني للخدمات لكنه ظل محدوداً ، وهذا لا يتوافق مع التطور الكبير للتكنولوجيا ولأنترنت الأشياء لأنها لا تزال هذه الأنظمة تعاني من قيود جوهرية كالتكيف السياقي وإدارة التعارضات السياقية.

في الواقع، يشتمل النظام البيني للخدمات على بيئة متعددة السياقات لتحقيق التعاون وتنفيذ العملية المطلوبة، إن كل خدمة ترتبط بسياق معين وتحقيق التشغيل البيني يتطلب التعاون بينها و القدرة على دمج الوظائف بشكل صحيح وفقًا للاحتياجات الخاصة بكل سياق لكن هذا يزيد من تعقيد النظام ومخاطر عدم الاتساق(MARKOVIC–STEVEAN.2020) .

اعتمدت أنظمة المعلومات على مجموعة واسعة من أنظمة الدعم القائمة على التكنولوجيا مثل نظم إدارة قواعد البيانات ولغات البرمجة(BURMEISTER.al.2019) ، وما إلى ذلك لكنها تُظهر مستوى عالٍ من التعقيد

التكنولوجي وتفتقر إلى قابلية التشغيل البيني للنظام. إنها تنطوي على تكرار المعلومات التي تسبب التناقضات وتقليل المرونة وقابلية التوسع في بنياتها، مما يعقد عملية التشغيل البيني رغم استخدام أنظمة إدارة سير العمليات إلا أنها قد تزيد بشكل سلبي من تعقيد وعدم اتساق التشغيل بين الخدمات الهادفة لتحقيق العملية المطلوبة (JAVANBAKHT-CHIAE. 2023).

إن الأمان والخصوصية وسهولة الاستخدام هي سمات الجودة لأنظمة وخدمات تكنولوجيا المعلومات (KHANPARA, .al.2023)في نفس الوقت يجب ألا تؤدي التقنيات المتعلقة بالوقت والأمان والخصوصية إلى تعقيد سير العمليات لذلك يتوجب وجود مشاركة ضرورية سواء في التطوير أو في وقت التشغيل.

لا تزال هذ الأنظمة تعاني من قيود أساسية في التكيف السياقي، وإدارة التعارضات السياقية ودمج الأمان في بنية النظام، عدة أعمال قدمت لمعالجة هذه القيود لكن كانت الحلول جزئية وتفتقر للنمذجة الديناميكية للسياق(الزمني والبيئي) مما يجعلها غير قادرة على التكيف مع الظروف المتغيرة(KRICHEN.2019).

أعمال أخرى ركزت على أنظمة البيئة الذكية والسياقية لكنها لم تأخذ بعين الاعتبار مشكلة التعارضات الأمنية(KALARIA-KAYES.2024) .

أعمال أخرى استخدمت التعلم الألي لاكتشاف التعارضات لكن بعد حدوثها دون إيجاد حلول لاتخاذ القرار المناسب لتنفيذ العملية المطلوبة بنجاح (AMBAT-SAHOO.2024) (HUANG.al.2021) نبين في الجدول التالي[1] مقارنة بين الدراسات المذكورة.

جدول[1]: مقارنة بين الدراسات المرجعية

الدراسة	ايجابيات	سلبيات	النموذج المقترح
SOA(NEWCOMER -LOMOW.2005)	اختيار الخدمة المثلى لتحقيق التعاون	زيادة عدد الخدمات المقدمة لتحقيق التعاون يزيد تعقيد النظام.	يقدم النموذج المقترح آلية إدارة التفاعلات بطريقة منظمة مما يقلل التعقيد حيث يتم تخزين جميع القواعد في مستودع واحد(مستودع سياسات الخدمة) وتم الاعتماد على قواعد منطقية باستخدام الأدوار والصلاحيات. يعالج النموذج المقترح ثلاثة أبعاد سياقية(زمني، بيئي، تشغيلي)في قاعدة واحدة مما يزيد من دقة القرارات الأمنية. النموذج المقترح يعتمد على كشف استباقي للتعارضات قبل التنفيذ حيث يتم التحقق من شرط الشمولية كشرط أساسي للسماح بالتنفيذ ، مما يمنع وقوع المخاطر الأمنية.
Improving Formal Verification and Testing Techniques for Internet of Things and Smart Cities (KRICHEN.2019).	تقديم أساس منطقي للاستدلال	تفتقر إلى النمذجة الديناميكية للسياق(الزمني و البيئي) مما يجعلها غير قادرة على التكيف مع الظروف المتغيرة.	
Adaptive context-aware access control for iot environments leveraging fog computing(KALARIA-KAYES.2024)	التحكم في الوصول السياقي وديناميكية اتخاذ القرار	اقتصار السياق على البعد الزمني دون معالجة التعارضات.	
Anomaly detection and energy consumption prediction in smart homes using machine learning(AMBAT-SAHOO.2024)	استخدام التعلم الألي لأتمتة الكشف عن التعارضات.	اكتشاف التعارضات بعد وقوعها أي بعد التنفيذ ولا يعمل على منعها مما يزيد المخاطر.	
A Context-Aware Internet of Things-Driven Security Scheme for Smart Homes(KHANPARA, .al.2023)	مخطط أمني للبيوت الذكية باستخدام انترنت الأشياء	يركز على الجانب الأمني دون إدارة التعارضات	
Conflict detection in iot-based smart homes (HUANG.al.2021)	كشف التعارضات في المنازل الذكية باستخدام الرسم البياني وخوارزميات معرفية.	يستخدم خوارزميات تعلم ألي بسيط محدودة التعامل مع الأبعاد السياقية، يكشف التعارضات بعد التنفيذ دون منعها.	

إن جميع الأعمال السابقة لم تقدم منهجية لدمج الأبعاد السياقية المتعددة(زمنية، بيئية، تشغيلية) في قاعدة منطقية واحدة تجمع بين القوة النظرية(كالنمذجة الرياضية) والبساطة التطبيقية حيث عمل البحث لمواجهة التحديات السابقة بدمج البعدين الزمني والبيئي في قاعدة منطقية واحدة وتم استخدام قواعد استباقية لكشف التعارضات ومنعها قبل التنفيذ مما يقلل التكاليف والمخاطر.

يستعرض هذا البحث نموذج رياضي متكامل يربط بين المتطلبات الوظيفية والأمنية والسياقية قابل للتحقق والبرهنة وقابل للتطبيق في أنظمة ذكية وقابل للتوسع نحوالأنظمة الذكية(مدن أو مصانع ذكية) الآمنة والقابلة للتشغيل البيني.

بالتالي هدف البحث إلى دمج الحالات المتفرقة المذكورة في الأعمال السابقة بنموذج واحد لتوحيد الرؤية بين الأمن والتشغيل والكفاءة مع التركيز على المرونة والاستباقية في التعامل مع التحديات المتعددة.

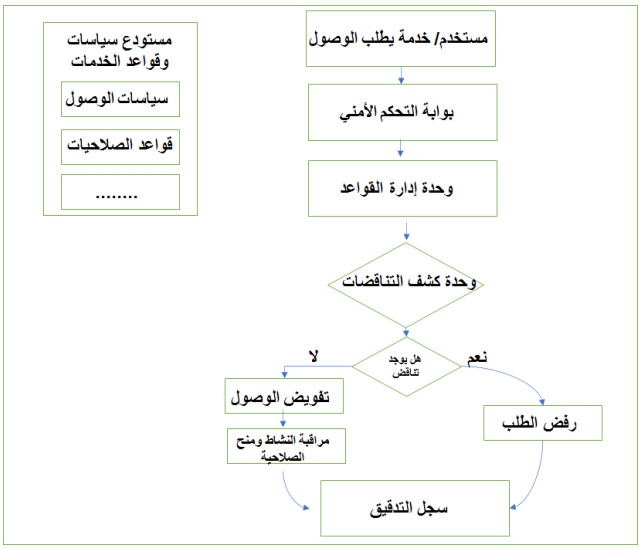
أيضا هدف إلى التحويل من معالجة المشاكل إلى منع المشاكل وتوفير في التكاليف والوقت، بالإضافة إلى تقديم أدلة رياضية على الصحة والسلامة لضمان الجودة علمياً وحلول قابلة للتطوير والتوسع مما يساعد على معالجة المشاكل الهيكلية للتشغيل البيني الآمن.

المنهجية المقترحة بهدف إدارة الوصول والتحكم في التفاعلات بين الخدمات

لإدارة الوصول والتحكم في التفاعلات بين الخدمات اعتمد في هذا البحث على قواعد محددة وهي عبارة عن مجموعة من القواعد المنطقية لاكتشاف التناقضات بين سياسات الخدمات بشكل آلي (Automatic conflict Detection).

يرتكز النموذج على المكونات الرئيسية الموضحة في الشكل [1] والذي يمثل البنية العامة للنظام المقترح المكون من المكونات التالية والتي تعمل بتسلسل محدد:

- مستودع سياسات الخدمات: قاعدة بيانات مركزية تحتوي على جميع القيود والصلاحيات (القواعد الخاصة بكل خدمة).
- بوابة التحكم الأمني: نقطة الدخول الموحدة لجميع طلبات الوصول.
- وحدة إدارة القواعد: المسؤولة عن استقبال طلبات الوصول من الخدمات وتجميع القواعد من مختلف السياسات.
- وحدة كشف التناقضات: المحرك الأساسي الذي يحلل القواعد المتعلقة بطلب معين لاكتشاف أي تعارضات عندما تسمح إحدى القواعد بالوصول بينما تمنعه آخرى، مثلا عندما تعتمد صلاحية خدمة على بيانات لا يسمح لها بالوصول إليها، أي أنه يقوم بالتحقق من مطابقة الطلبات للسياسات الأمنية.
- مراقبة النشاط بهدف تتبع الأنشطة والعمليات الخاصة بكل خدمة لاكتشاف السلوك غير المطلوب.



الشكل[1]: إدارة الوصول والتحكم في التفاعلات بين الخدمات.

إن طلب الوصول هو الرسالة التي ترسلها خدمة ما أو (جهاز ما) إلى النظام لطلب الإذن بتنفيذ عملية معينة أو خدمة، حيث تقوم بوابة التحكم الأمني والتي تعتبر نقطة الدخول الوحيدة لجميع طلبات الوصول وتوجيها إلى وحدة إدارة القواعد والتي تقوم بتجميع هذه القواعد من مختلف السياسات وفق الأولوية وحسب السياق ثم ترسلها إلى وحدة كشف التناقضات والتي تقوم بتحليل القواعد المتعلقة بطلب معين لاكتشاف أي تعارض بينهما(مثلاً إجراء تشغيل المكيف وجهاز آخر يسبب حمل زائد) ليتم اتخاذ القرار إما بتفويض الوصول أو الرفض حيث سجل التدقيق يتضمن جميع الأحداث والإجراءات والقرارات التي تحدث داخل النظام وهو جزء لا يتجزأ من وحدة مراقبة النشاط حيث يسجل كل المعلومات بهدف التحليل والمراجعة والتحقق قبل تنفيذ الخدمة.

وإن جميع الخدمات يجب أن تحقق (السرية، سلامة البيانات، التوافرية القدرة على الاستجابة) لضمان إنشاء نظام ذكي يدير التفاعلات بين الخدمات المختلفة تلقائياً، مع ضمان الأمان والكفاءة.

- السرية (Confidentiality): حماية البيانات من الإفشاء غير المصرح به من خلال آليات تشفير متقدمة ونماذج تحكم في الوصول(TOJIMAMATOVICH.2023).
- سلامة البيانات (Data Integrity): ضمان دقة واتساق البيانات خلال دورة حياتها الكاملة باستخدام تقنيات التوقيع الرقمي والتحقق من السلامة(MEGOUACHE.al.2020) .
- موثوقية النظام (System Reliability): استمرارية أداء الخدمة وفقاً للمواصفات المحددة من خلال آليات التحقق من الصحة ومعالجة الأخطاء.
- التوافرية (Availability): الحفاظ على استمرارية عمل الخدمة من خلال أنظمة التحميل .
- كفاءة الأداء (Performance Efficiency): قدرة النظام على معالجة الطلبات المتزامنة ضمن الفترات الزمنية المحددة(GOOCKS.2019) .
- القدرة على الاستجابة (Responsiveness): قدرة النظام على معالجة الطلبات المتزامنة ضمن المهلات الزمنية المحددة(FETH–MAIER& POLST.2017) .

بالتالي لضمان تقديم خدمات موثوقة يجب تحقيق الحماية أثناء التنفيذ بتطبيق آلية تحكم فورية لحماية البيانات لضمان عدم تسرب المعلومات الحساسة خارج النطاق المصرح به (PRAMANIK–2022)، وضمان تنفيذ العمليات ضمن المسارات المحددة مسبقاً دون عراقيل تحت ظروف التشغيل المختلفة، ومراعاة القيود الزمنية عن طريق تقديم قواعد تتكيف مع الظروف (القواعد الزمنية والسياقية) لتجنب التناقضات الزمنية والسياقية وتتكيف مع الظروف المتغيرة وتتمكن من الكشف الاستباقي للمشاكل قبل حدوثها.

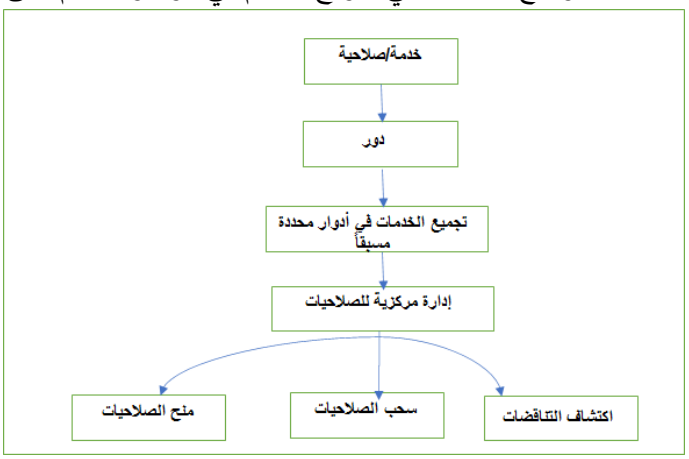
قدمت عدة أعمال لكن الإشكالية الأساسية تكمن في محدودية الأنظمة الحالية في التعامل مع الطبيعة الديناميكية للخدمات المترابطة، حيث تفتقد معظم الأنظمة التقليدية للقدرة على التكيف السياقي والاستباقية في إدارة التعارضات.

الإطار العام لإدارة الوصول

يمثل الشكل نموذج التحكم في الوصول ويستخدم في أنظمة إدارة الوصول لتسهيل إدارة الصلاحيات وتقليل التعقيد.

حيث النموذج المقترح لا يعتمد فقط على صلاحيات الأدوار بل يتضمن شروط إضافية من خلال دمج الأبعاد السياقية المتعددة (السياق الزمني والياق البيئي) مع آلية الكشف الاستباقي عن التعارضات.

يعتمد نموذج التحكم في الوصول على تجميع الخدمات في أدوار ذات صلاحيات محددة مسبقا مما يسهل إدارة الصلاحيات ويقلل من التعقيد يوضح الشكل التالي نموذج التحكم في الوصول القائم على الأدوار.



الشكل[2]: التحكم في الوصول حسب الصلاحيات

الهدف من نموذج إدارة الوصول بدلا من ربط الصلاحيات مباشرة بالمستخدمين يتم ربطها بأدوار ثم يتم تعيين المستخدمين لهذه الأدوار حيث يمكن أن يكون المستخدم أي كيان يطلب الوصول لخدمة معينة، بينما الأدوار هي مجموعات منطقية من الصلاحيات تتوافق مع وظائف محددة والصلاحية هي إذن بتنفيذ عملية محددة وتعطى للدور وليس للمستخدم مباشرة وهذا النموذج يتكامل مع الشكل [1] حيث يقدم الصلاحيات والذي بدوره يعالج مسألة كشف التعارض الاستباقي قبل التنفيذ.

لمنح الأذونات تم تعريف علاقة النشر

autoDirect(x, y, TimeContext, EnvContext) → auto(x, y, TimeContext, EnvContext)

autoDirect(Entity1, Entity2, TimeContext, EnvContext) → auto(Entity1, Entity2, TimeContext, EnvContext)−:

valid_time_context(TimeContext)،

valid_environment_context(EnvContext)،

not conflicting_context(Entity1, Entity2, TimeContext, EnvContext).

autoDirect :الإذن المباشر للوصول

x :الكيان الذي يطلب الوصول (مثل: المستخدم، الجهاز)

Y :الكيان المطلوب الوصول إليه .

TimeContext :السياق الزمني (متى)

EnvContext :السياق البيئي (أين، تحت أي ظروف)

للتحقق الرياضي من القاعدة تم تعريف المتغيرات المنطقية

P=valid_time_context(TimeContext)،

Q=valid_environment_context(EnvContext)،

R=not conflicting_context(Entity1, Entity2, TimeContext, EnvContext).

S= autoDirect(Entity1, Entity2, TimeContext, EnvContext)

T=auto(Entity1, Entity2, TimeContext, EnvContext)

autoDirect(Entity1, Entity2, TimeContext, EnvContext) → auto(Entity1, Entity2, TimeContext, EnvContext)−: P,Q,R

إذا:

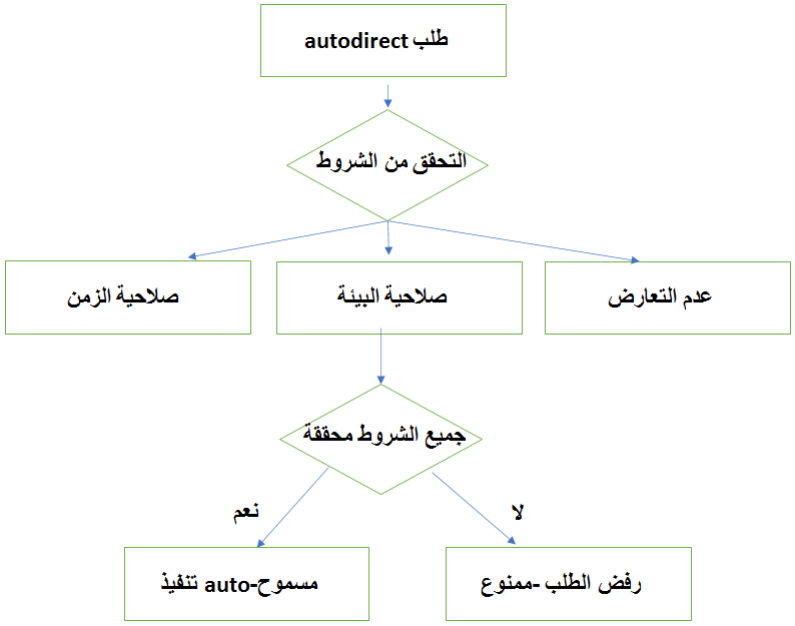
$$S \rightarrow T \Leftrightarrow (\text{if and only if})(P \wedge Q \wedge R)$$

تضمن هذه الصيغة السلامة المطلقة للتنفيذ حيث يستحيل تنفيذ أي إجراءT دون تحقق جميع الشروط مسبقا (P,Q,R) كما موضح في الشكل[3] والذي يوضح مسار تنفيذ القاعدة واتخاذ القرار بناء على القواعد المنطقية المقترحة حيث لايتم التنفيذ إلا اذا تحققت الشروط الثلاثة جميعهاP∧Q∧R(التحقق الزمني ، التحقق من السياق، التحقق من عدم وجود تعارض).

حيث يتم التحقق الزمني أولا بمقارنة الوقت مع النطاقات الزمنية المسجلة في سياسات الخدمة المستهدفة، إذا تبين أن لوقت غير مناسب يتم رفض الطلب فورا دون الانتقال إلى الخطوات التالية مما يوفر وقت المعالجة، أما إذا كان الوقت مناسبا ينتقل الطلب إلى مرحلة التحقق من الظروف البيئية ومدى تطابقها مع الشروط المحددة في سياسات الخدمة، في حال المطابقة ينتقل الطلب إلى مرحلة كشف التعارضات حيث يتم تحليل العلاقة بين الطلب الحالي وحالة النظام، حيث يتم فحص التعارضات التالية: تعارض الموارد(كتعارض استهلاك الطاقة بين جهازين)، والتعارض الأمني والتعارض الزمني(كتداخل الجداول الزمنية) وتعارض الأولويات(الطلبات أولويات مختلفة مثلا طلبان متزامنان على نفس الموارد المحددة للطاقة الكهربائية حيث تتجاوز القدرة المطلوبة الحد المسموح به مما يخلق تعارض يحتاج الحل بناء على الأولويات) حيث يتم الاعتماد على القواعد المخزنة في مستودع وسياسات الخدمات والحالة الراهنة للخدمات في النظام.

بعد التحقق من الشروط يتم اتخاذ القرار بتنفيذ الطلب، أما في حال تحقق شرط واحد أو أكثر يرفض مع ذكر السبب المحدد للرفض عدم ملائمة(الوقت، الظروف البيئية) أو وجود تعارض.

تكمن الأهمية لهذا الترتيب في تحقيق التوازن بين الدقة والكفاءة والاكتشاف الاستباقي للتعارضات قبل حدوثها مما يضمن عدم تنفيذ أي إجراء إلا بعد التحقق من جميع الشروط المطلوبة.



الشكل[3]: مخطط تدفق اتخاذ القرار

تم تعريف جدول الحقيقة بالشكل التالي:

P	Q	R	(P^Q^R)	S(auto direct)	T(auto)	S→T
T	T	T	T	T	T	T
T	T	F	F	F	T	T
T	F	T	F	F	T	T
T	F	F	F	F	T	T
F	T	T	F	F	T	T
F	T	F	F	F	T	T
F	F	T	F	F	T	T
F	F	F	F	F	T	T

لتحقيق الاتساق (consistency) يجب أن يتحقق الشرط:

$\neg\exists\ (S \wedge \neg(P \wedge Q \wedge R))$ // لا يوجد تناقض

أي أن تحقيق الاتساق يتطلب عدم وجود أي تعارض(يوجد تعارض في حال كان الوقت مثلا غير مناسب والظروف البيئية غير مناسبة في سيناريو البيت الذكي أو يوجد تعارض آخر).

وعرف الشرط بالشكل التالي:

$conflicting_context \equiv \neg P \vee \neg Q \vee \neg R$

$\therefore$ التناقض يحدث عندما: $P \wedge Q \wedge R \wedge conflicting_context = P \wedge Q \wedge R \wedge (\neg P \vee \neg Q \vee \neg R) = False$ // لا تعارض

يبين الجدول التالي الرموز والمفردات والمجالات والمسندات المستخدمة في القواعد:

الرموز الأساسية	المفردات	المجالات

$\forall x$: لكل x (Universal Quantifier)
$\exists x$: يوجد x (Existential Quantifier)
$\rightarrow$: يستلزم (Implication)
$\wedge$: و (AND)
$\vee$: أو (OR)
$\neg$: ليس (NOT)
$\Box$: دائماً (Always)
$\Diamond$: في النهاية (Eventually)
$\in$: ينتمي إلى
	E, E1, E2 : كيانات (Entities)
	T: سياق زمني (TimeContext)
	C: سياق بيئي (EnvContext)
	S: حالة النظام (System State)
		ENTITY = {$e_1, e_2, ..., en$} // مجموعة الكيانات
		TIME = {$t_1, t_2, ..., tm$} // الأوقات الممكنة
		ENV = {$c_1, c_2, ..., ck$} // السياقات البيئية
		المسندات
		AutoDirect(e_1, e_2, t, c) : طلب تشغيل تلقائي من e_1 إلى e_2
		Auto(e_1, e_2, t, c) : تنفيذ التشغيل التلقائي
		ValidTime(t) : السياق الزمني صالح
		ValidEnv(c) : السياق البيئي صالح
		Conflicting(e_1, e_2, t, c) : يوجد تعارض

ضمن وحدة كشف التناقضات عرفنا مجموعة من القواعد التي تمنع التنفيذ في حالات التعارض وتضمن أن لكل المدخلات مخرج وحيد بحيث يضمن التنفيذ عند توفر الشروط، حيث تم تعريف القواعد التالية:

القاعدة ١: لكل طلب تشغيل تلقائي يستلزم شروط صحة السياق وعدم التعارض وينتج عنه التنفيذ(أي يجب أن يتحقق شرط autoDirect لكل طلب أي يجب أن تتحقق الشروط(Valide Time,ValidEnv, not conflicting).

$$\forall e_1 \forall e_2 \forall t \forall c\ [\ AutoDirect(e_1, e_2, t, c) \rightarrow (ValidTime(t) \wedge ValidEnv(c) \wedge \neg Conflicting(e_1, e_2, t, c)) \wedge Auto(e_1, e_2, t, c)]$$

القاعدة ٢: الحتمية أي إذا تحققت الشروط فإن التنفيذ يؤدي إلى حالة فريدة للنظام.

$$\forall e_1 \forall e_2 \forall t \forall c \; [\; (ValidTime(t) \wedge ValidEnv(c) \wedge \neg Conflicting(e_1, e_2, t, c)) \rightarrow \; \exists! s \; [Auto(e_1, e_2, t, c) \rightarrow Reach(s)]]$$

قواعد سلامة التنفيذ:

$$\Box \forall e_1 \forall e_2 \forall t \forall c \; [\; (ValidTime(t) \wedge ValidEnv(c) \wedge \neg Conflicting(e_1, e_2, t, c)) \rightarrow \; \Diamond AutoDirect(e_1, e_2, t, c)]$$

$$\Box \forall e_1 \forall e_2 \forall t \forall c \; [\; AutoDirect(e_1, e_2, t, c) \; \rightarrow \; \neg Conflicting(e_1, e_2, t, c)]$$

تم تعريف التعارض بالشكل التالي:

$$Conflicting(e_1, e_2, t, c) \equiv \exists e_3 \; [e_3 \neq e_1 \wedge e_3 \neq e_2 \wedge Priority(e_3) > Priority(e_1)] \; \vee \; ResourceConflict(e_1, e_2) \; \vee \; TemporalConflict(t)$$

وعرفت قاعدة عدم التعارض بحيث لايمكن تنفيذ طلبين متعارضين في نفس الوقت لنفس الكيانات.

$$\forall e_1 \forall e_2 \forall t \forall c \; [\; AutoDirect(e_1, e_2, t, c) \wedge AutoDirect(e_3, e_4, t, c) \rightarrow \; e_1 = e_3 \vee e_2 = e_4 \vee \neg Simultaneous(t)]$$

وعرفنا خاصتي الاستجابة والاستقرار لضمان أن كل طلب يؤدي في النهاية إلى تنفيذ ، وفي حال كانت الشروط غير صالحة يبقى الطلب غير ممكن.

$$\Box [AutoDirect(e_1, e_2, t, c) \rightarrow \Diamond Auto(e_1, e_2, t, c)]$$

$$\Box [\neg ValidTime(t) \vee \neg ValidEnv(c) \rightarrow \Box \neg AutoDirect(e_1, e_2, t, c)]$$

تم التأكد من صحة هذه القواعد من خلال تطبيقها على سيناريو للبيت الذكي.

عرفت الكيانات E وهي: مكيف صالة، مكيف غرفة نوم، إضاءة صالة، إضاءة مطبخ، أجهزة أمن، نظام ري، سخان ماء.

السياقات: صباح، ظهيرة، مساء، مشغول، غير مشغول، حار، بارد،آمن، خطر.

السيناريو ١: تشغيل المكيف في الصالة

autoDirect(صالة_مكيف, تشغيل, مساء, [مشغول, حار]) :-
valid_time_context(مساء), الوقت بين 6-11 مساءً
valid_environment_context([مشغول, حار]), يوجد أشخاص ودرجة حرارة >25
not conflicting_context (صالة مكيف, تشغيل, مساء, [مشغول, حار]).

التحقق الرياضي:

P = valid_time_context(مساء) = true (الوقت 8 مساءً)
Q = valid_environment_context([مشغول, حار]) = true
R = ¬conflicting_context = true (لا تعارض) ∴ P ∧ Q ∧ R = true ⇒ autoDirect → auto

تحققت جميع الشروط ولا يوجد تعارض(مثل وجود حمل زائد على الطاقة) لذا يتم التنفيذ.

سيناريو ٢: محاولة تعطيل نظام كاميرا الأمان:

```
autoDirect(كاميرا أمان , إطفاء, ليل, [غيرمشغول]) :-
valid_time_context(ليل), true
valid_environment_context([غير مشغول]), true
not conflicting_context(كاميرا أمان, إطفاء ليل, [غيرمشغول]). false
```

النتيجة Autodirect ممنوع لأن conflicting context regress true حيث أن تعطيل كاميرات الأمان عندما يكون البيت غير مشغول يمثل ثغرة أمنية كبيرة وبالتالي تمنع القاعدة هذا الإجراء.

مناقشة النتائج والمقارنة

يقدم هذا البحث نموذجا رياضيا لإدارة الوصول والتحكم في التفاعلات بين الخدمات المترابطة، حيث يمثل هذا النموذج نقلة من الأنظمة التقليدية التي تفتقر للتكيف السياقي متعدد الأبعاد(زمني، بيئي، تشغيلي)وكشف التعارضات قبل التنفيذ، إلى نموذج رياضي متكامل قابل للتوسع نحو أنظمة أكبر(المدن، المصانع الذكية)، قدم النموذج المقترح تحسينات أساسية في مجالات(الأمان والاستباقية والشمولية)، حيث قدم البحث إطارا رياضيا متكاملا يحول الأنظمة الذكية إلى أنظمة استباقية ذكية بحيث لا يضمن التشغيل الأمن فحسب بل أثبت رياضيا القدرة على منع التعارضات تحت جميع الظروف وبالتالي حقق هذا البحث عملية التشغيل البيني الأمن للتحكم في الوصول السياقي ليس فقط من يصل بل (متى وأين وكيف) بالإضافة لاتخاذ قرارات أمنية ذكية وحماية ديناميكة متطورة وبالتالي ضمان التشغيل الأمن تحت جميع الظروف .

التوصيات المستقبلية

دمج تقنيات الذكاء الصنعي والتعلم الألي والمنطق الضبابي بهدف التوسع في تطبيقات انترنت الأشياء بحيث سيطبق النموذج في مجالات أوسع مثل المدن الذكية، أو تنظيم استهلاك الطاقة في المعامل الكبرى ومنع التعارضات بين الخطوط.

لتحقيق ذلك يتم العمل على بناء محاكي رياضي لنظام الأمن الذكي باستخدام النمذجة الرياضية وإثبات أنه آمن(يمنع جميع التعارضات)، فعال(يتخذ قرارات صحيحة)، سريع(زمن استجابة معقول).

الخاتمة

قدم هذا المقال نموذجاً متكاملاً قائماً على قواعد منطقية ذكية لتحقيق التشغيل البيني الآمن بين الخدمات. يثبت النموذج فعاليته من خلال توفير إطار عمل رياضي متين يضمن السلامة والموثوقية، كما يتجلى ذلك في التطبيق العملي على نظام البيت الذكي. من خلال الشروط الثلاثة الأساسية (السياق الزمني، السياق البيئي، وعدم التعارض)، يستطيع النظام اتخاذ قرارات آمنة وذكية تمنع الثغرات الأمنية وتحسن الكفاءة.

مع التوجه العالمي نحو رقمنة كل شيء، من المتوقع أن تزداد الحاجة لمثل هذه النماذج الأمنية الاستباقية. إن التوصيات المستقبلية التي تم طرحها، وخاصة تلك المتعلقة بالذكاء الاصطناعي والتطبيقات الصناعية الواسعة، تفتح آفاقاً جديدة للبحث والتطوير. يعتبر هذا العمل لبنة أساسية نحو بناء أنظمة رقمية متكاملة لا تكون فيها الكفاءة على حساب الأمان، ولا الأمان عائقاً أمام التقدم.

المراجع العلمية

1. AMBAT, A,SAHOO, J. 2024, *Anomaly detection and energy consumption prediction in smart homes using machine learning. ETRI Journal, 1-12.*

2. BURMEISTER,F, DREWS,P, SCHIRMER, I. 2019, *A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation. Proceedings of the Hawaii International Conference on System Sciences.*

3. FETH, D, MAIER, A, POLST, S, 2017. *A User-Centered Model for Usable Security and Privacy. Has.*

4. GOOCKS, M. O, 2019, *Recent developments in Computing of system reliability, IEEE transactionson reliability.*

5. HUANG, B, DONG, H, BOUGUETTAYA, A, 2021. *Conflict detection in iot-based smart homes. IEEE International Conference on Web Services (ICWS).*

6. JAVANBAKHT, N, CHIAE, S, 2023. *A Generic Business Architecture Reference Model Using Systems Theory Perspective in Enterprise Architecture. IEEE 25th Conference on Business Informatics (CBI).*

7. KALARIA, R, KAYES, A, RAHAYU, W, PARDEDE, E, SALEHI, A,2024. *Adaptive context-aware access control for iot environments leveraging fog computing. International Journal of Information Security, 23, 3089–3107.*

8. KHANPARA, P, LAVINGIA, K, Trivedi, R.; Tanwar, S.; Verma, A.; Sharma, R. (2023). A Context-Aware Internet of Things-Driven Security Scheme for Smart Homes. Security & Privacy.

9. KRICHEN, M, 2019, *Improving Formal Verification and Testing Techniques for Internet of Things and Smart Cities. Mobile Networks and Applications.*

*10.*MARKOVIC, M, STEVEAN, G, 2020, *A Knowledge-Based Document Assembly Method to Support Semantic Interoperability of Enterprise Information Systems. Enterprise Information Systems.*

*11.*MEGOUACHE, L, ABDELHAFID, Z, MAHIEDDINE, D, 2020, *Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and Information Sciences, 10(15).*

*12.*NEWCOMER, E, LOMOW, G,2005, *Understanding SOA with Web Services. Addison Wesley.*

*13.*PRAMANIK, S, 2022, *An Effective Secured Privacy-Protecting Data Aggregation Method in IoT. Achieving Full Realization and Mitigating the Challenges of the Internet of Things.*

*14.*TOJIMAMATOVICH, J. V,2023, *CONCEPT AND ESSENCE OF INFORMATION SECURITY. Web of Synergy: International Interdisciplinary Research Journal, 2(4), 643-6.*