مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (10) العدد (10) 2026

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

مراجعة شاملة ونموذج مصادقة متعددة العوامل قائم على السياق لتأمين تكامل IoT وOT

م. لين سلامه *

م. فراس غانم **

(تاريخ الإيداع 2026/4/16. قُبِل للنشر في 2026/5/18)

□ ملخّص □

تقدم هذه الدراسة مراجعة منهجية وتحليلًا نقديًا لآليات المصادقة في بيئات إنترنت الأشياء (IoT)، مع التركيز على التحديات الأمنية المعقدة الناتجة عن التكامل المتزايد مع أنظمة التكنولوجيا التشغيلية (OT). تستعرض الدراسة الأطر التقليدية والحديثة للمصادقة، بما في ذلك نماذج المصادقة متعددة العوامل (MFA) والنماذج المعتمدة على السياق (Context-Aware Authentication)، مع تقييم أدائها من حيث الأمان، التعقيد الحسابي، وقابلية التوسع.

وبناءً على تحليل الفجوات البحثية، تقترح الدراسة نموذج مصادقة متقدم متعدد العوامل قائم على السياق، يدمج بين عوامل الهوية الثابتة والديناميكية، ويعتمد على بيانات سياقية آنية مثل الموقع الجغرافي، سلوك المستخدم، ومعرفات الأجهزة. يتضمن النموذج بنية متعددة الطبقات مدعومة بآليات إعادة مصادقة تكيفية (Adaptive Re-authentication) لتعزيز القدرة على اكتشاف السلوكيات غير الطبيعية والتعامل معها في الزمن الحقيقي.

ولضمان ملاءمة النموذج لبيئات IoT محدودة الموارد، يتم توظيف تقنيات تشفير خفيفة مثل التشفير بالمنحنيات الإهليلجية (ECC) وعمليات XOR، بما يحقق توازنًا فعالًا بين متطلبات الأمان والكفاءة الحسابية. وتشير نتائج التحليل النظري والمقارن إلى أن النموذج المقترح يحقق تحسنًا ملحوظًا في متانة الأمان (Security Robustness) مع تقليل الحمل الحسابي، مقارنة بالحلول التقليدية.

الكلمات المفتاحية (Keywords): إنترنت الأشياء، IoT، أمن إنترنت الأشياء، المصادقة، أجهزة إنترنت الأشياء، التحديات الأمنية في إنترنت الأشياء

*مهندسة حاصلة على درجة الماجستير في تكنولوجيا المعلومات والاتصالات – كلية هندسة تكنولوجيا المعلومات والاتصالات – جامعة طرطوس– سوريا

** مهندس حاصل على درجة الماجستير في تكنولوجيا المعلومات والاتصالات – كلية هندسة تكنولوجيا المعلومات والاتصالات – جامعة طرطوس– سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (10) العدد (10) 2026

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

A Comprehensive Review and a Context-Aware Multi-Factor Authentication Model for Secure IoT–OT Integration

Eng. Leen Salameh *

Eng. Firas Ghanem **

(Received 16/4/2026. Accepted 18/5/2026)

□ ABSTRACT □

This study presents a systematic review and a critical analysis of authentication mechanisms in Internet of Things (IoT) environments, with a particular focus on the complex security challenges arising from the increasing integration with Operational Technology (OT) systems. The study examines both traditional and modern authentication frameworks, including Multi-Factor Authentication (MFA) and Context-Aware Authentication models, evaluating their performance in terms of security, computational complexity, and scalability. Based on the identified research gaps, this work proposes an advanced context-aware multi-factor authentication model that integrates both static and dynamic identity factors. The model leverages real-time contextual data such as geographical location, user behavior, and device identifiers. It adopts a multi-layered architecture supported by adaptive re-authentication mechanisms to enhance the detection and mitigation of anomalous activities in real time.

To ensure suitability for resource-constrained IoT environments, the model incorporates lightweight cryptographic techniques such as Elliptic Curve Cryptography (ECC) and XOR operations, achieving an effective balance between security requirements and computational efficiency. Theoretical and comparative analysis indicates that the proposed model significantly improves security robustness while reducing computational overhead compared to conventional approaches.

Keywords: Internet of Things, IoT, IoT Security, Authentication, IoT Devices, Security Challenges in IoT

* Master of Communication Technology Engineering Department, Information and communication TechnologyEngineering, Tartous University, Syria

** Master of Communication Technology Engineering Department, Information and communication TechnologyEngineering, Tartous University, Syria

1- مقدمــة:

يمكن اعتبار إنترنت الأشياء (IoT) ظاهرة حديثة أصبحت ضرورة اجتماعية متزايدة الأهمية. فمن الأجهزة المنزلية الذكية والأجهزة القابلة للارتداء إلى المستشعرات الصناعية، مهد إنترنت الأشياء الطريق نحو أنظمة تعتمد بشكل كبير على الأتمتة واتخاذ القرار الذكي. ويمتد هذا التحول ليشمل التكنولوجيا التشغيلية (OT)، والتي تمثل البنية التحتية التقنية الفيزيائية التي تتكون من أنظمة برمجية ومادية تُستخدم في العمليات الصناعية المرتبطة بالآلات والمرافق والبنى التحتية المختلفة.

أدى التكامل بين إنترنت الأشياء والتكنولوجيا التشغيلية إلى ظهور تطبيقات متقدمة مثل التصنيع الذكي، أنظمة التحكم الذكية في الطاقة، والبنية التحتية الذكية. وعلى الرغم من الإمكانات الكبيرة التي يوفرها هذا التكامل، خاصة من حيث الكفاءة والعمل في الزمن الحقيقي، إلا أنه يفرض تحديات إضافية، لا سيما في مجال المصادقة (Authentication). فقد كانت أنظمة OT تاريخيًا معزولة، ولكن عند ربطها بشبكات IoT أصبحت عرضة لنفس التهديدات التقليدية، مثل الوصول غير المصرح به، تسرب البيانات، وانتحال الهوية. وتبرز هذه التحديات أهمية تعزيز الأمان في بيئة IoT–OT (Almazroi et al., 2023).

1-1 الأمان والمصادقة في إنترنت الأشياء IoT

يُعد أمن الشبكات، الذي يشمل حماية الشبكة ووسائل الاتصال، إلى جانب الأمن السيبراني الذي يركز على حماية المواقع والخوادم وعمليات تبادل البيانات، من العناصر الأساسية لضمان بيئة آمنة. وتزداد هذه التحديات تعقيدًا في أنظمة IoT–OT نظرًا للعدد الكبير من الأجهزة التي تقوم بجمع البيانات ومشاركتها وتخزينها. (Sudha et al., 2024)

يرتكز الأمان على مفهومين أساسيين:

- السرية (Confidentiality): ضمان عدم وصول البيانات إلى جهات غير مصرح لها
- المصداقية (Authenticity): التأكد من أن البيانات ومصدرها حقيقيان

وكما هو الحال في أي شبكة، تتطلب شبكات إنترنت الأشياء عمليات مصادقة للتحقق من هوية المستخدمين والأجهزة. وتساهم أنظمة المصادقة القوية في تقليل مخاطر الوصول غير المصرح به والتهديدات الأمنية. إلا أن الاعتماد على الأساليب التقليدية مثل كلمات المرور والمصادقة أحادية العامل لم يعد كافيًا في بيئة IoT بسبب الطبيعة الديناميكية للأجهزة (Bansal, 2023).

1-2 التحديات والحلول الناشئة

مع التوسع المستمر في استخدام أجهزة إنترنت الأشياء في الحياة اليومية والعملية، أصبحت الحاجة إلى آليات مصادقة موثوقة أمرًا ضروريًا. ويُعد ظهور المصادقة متعددة العوامل (MFA) خطوة مهمة في هذا المجال، حيث تعزز مستوى الأمان من خلال استخدام أكثر من عامل للتحقق من هوية المستخدم قبل منحه الوصول إلى الأجهزة أو الشبكات، مما يقلل من مخاطر سرقة كلمات المرور أو الوصول غير المصرح به (Morais et al., 2023).

ومع ذلك، يواجه تطبيق حلول IoT العديد من التحديات الأمنية والتشغيلية، نتيجة لغياب معايير أمنية موحدة، وارتفاع تكاليف الأجهزة، بالإضافة إلى القيود التشغيلية مثل عمر البطارية المحدود. وعلى الرغم من

الإمكانات الكبيرة لهذه التقنيات، إلا أن اعتمادها لا يزال بطيئًا في العديد من المؤسسات، مما يستدعي المزيد من الدراسات لفهم العوائق التي تحد من انتشارها.

أهم التحديات المرتبطة بإنترنت الأشياء تشمل (Kumar et al., 2022):

- الخصوصية والأمان: تُعد الخصوصية والأمان من أهم التحديات في بيئات إنترنت الأشياء، حيث تكون أجهزة IoT عرضة لعدة أنواع من الهجمات مثل تسرب البيانات، وهجمات حجب الخدمة (DoS)، إضافة إلى الوصول غير المصرح به.
- تخزين ومعالجة البيانات: تقوم أجهزة إنترنت الأشياء بإنتاج كميات ضخمة من البيانات بشكل مستمر، الأمر الذي يتطلب آليات فعّالة للتخزين، وإدارة منظمة للبيانات، بالإضافة إلى تقنيات تحليل ذكية.
- جودة الخدمة (QoS): يتطلب تشغيل تطبيقات إنترنت الأشياء تحقيق مستوى مرتفع من جودة الخدمة، خصوصًا فيما يتعلق بتوفير عرض نطاق ترددي كافٍ (Bandwidth) وضمان معدل نقل بيانات مرتفع (Throughput). وترتبط هذه المتطلبات بشكل وثيق بالاعتماد المتزايد على الخدمات السحابية، مما يستدعي وجود بنية تحتية مستقرة وموثوقة.
- التوافقية والتوحيد القياسي: تُعد مشكلة عدم توافق الأجهزة والمنصات المختلفة من أبرز العوائق في بيئات IoT، حيث تعتمد هذه الأنظمة على بروتوكولات متعددة وغير موحدة، مما يؤدي إلى صعوبات في التكامل والتشغيل البيني.
- أمن وسلامة الأجهزة: نظرًا لانتشار أجهزة إنترنت الأشياء في بيئات متنوعة ومفتوحة، فإنها تصبح عرضة لمخاطر أمنية متعددة تشمل الاختراق أو حتى التدمير المادي للأجهزة.

ويهدف هذا البحث إلى تحليل وتقييم آليات المصادقة الحالية في بيئات إنترنت الأشياء (IoT)، مع التركيز على التحديات الأمنية الناشئة عن التكامل المتزايد مع أنظمة التكنولوجيا التشغيلية (OT). كما يسعى إلى دراسة أوجه القصور في أساليب المصادقة التقليدية، وخاصة الأنظمة أحادية العامل، من حيث الأمان وقابلية التوسع والكفاءة. وبناءً على ذلك، يقترح البحث نموذجًا متقدمًا للمصادقة متعددة العوامل (MFA) يعتمد على دمج العوامل الثابتة والديناميكية مع مراعاة السياق (Context-Aware Authentication)، بهدف تعزيز مستوى الحماية ضد الهجمات السيبرانية مثل انتحال الهوية والوصول غير المصرح به. كما يركز البحث على تحقيق توازن بين متطلبات الأمان العالية والقيود التشغيلية لأجهزة إنترنت الأشياء محدودة الموارد، بما يضمن تحسين الأداء العام وكفاءة النظام في البيئات الذكية.

2- مواد البحث و طرائقه:

يعتمد هذا البحث على منهجية تحليلية-مقارنة تهدف إلى دراسة وتقييم تقنيات المصادقة في بيئات إنترنت الأشياء (IoT) والتكنولوجيا التشغيلية (OT). حيث تم استخدام مراجعة أدبية منهجية (Systematic Literature Review) للأبحاث والدراسات الحديثة ذات الصلة بمجال المصادقة متعددة العوامل (MFA) والمصادقة المعتمدة على السياق (Context-Aware Authentication)، وذلك لتحديد الفجوات البحثية الحالية وفهم الاتجاهات الحديثة في هذا المجال.

كما تم اعتماد أسلوب التحليل المقارن بين النماذج والخوارزميات المختلفة من حيث مستوى الأمان، التعقيد الحسابي، استهلاك الموارد، وقابلية التوسع في بيئات IoT محدودة الإمكانيات. بالإضافة إلى ذلك، تم تحليل

الخصائص الأمنية للعوامل المستخدمة في أنظمة المصادقة مثل العوامل الثابتة (كلمات المرور والمفاتيح) والعوامل الديناميكية (الموقع، سلوك المستخدم، ومعرّفات الأجهزة).

وبناءً على هذا التحليل، تم تطوير تصور لنموذج مصادقة متعدد العوامل مدعوم بالسياق، مع التركيز على تصميم خوارزميات خفيفة الوزن مناسبة للأجهزة منخفضة القدرة، وذلك لتحقيق توازن بين الكفاءة الأمنية والأداء التشغيلي في البيئات الذكية.

الأعمال ذات الصلة (Related Work)

لا تزال عملية المصادقة في أنظمة إنترنت الأشياء (IoT) تمثل قضية بحثية مهمة بسبب الحاجة إلى تطوير حلول آمنة وموثوقة لربط الأجهزة الذكية. يستعرض هذا القسم مجموعة من الدراسات الحديثة التي نُشرت خلال العامين الأخيرين، والتي تناولت جوانب متعددة من آليات المصادقة في بيئات .IoT وقد قدمت هذه الدراسات استراتيجيات متنوعة لمعالجة التحديات الأمنية، مع التركيز على تقنيات خفيفة الوزن، عالية الكفاءة، وقابلة للتوسع.

يهدف هذا القسم إلى عرض أبرز نتائج هذه الدراسات، بالإضافة إلى تقديم تحليل مقارن لها بناءً على مجموعة من معايير التقييم مثل المنهجيات المستخدمة، التقنيات المعتمدة، والنتائج المحققة.

نظرة عامة على الأعمال ذات الصلة

تناولت الدراسة المعنونة **"EM-PUFs and Deep Learning Based IoT Device Authentication"** نهجًا جديدًا لمصادقة أجهزة IoT باستخدام دوال PUF المعتمدة على الانبعاثات الكهرومغناطيسية .(EM) تعتمد هذه الطريقة على التقاط الانبعاثات الفريدة للأجهزة أثناء تشغيلها، ويتم استخدام نماذج التعلم العميق مثل الشبكات العصبية والمشفرات التلقائية (Autoencoders) لتحقيق المصادقة بدقة عالية وصلت إلى F1-score بقيمة 0.99. يتميز هذا النهج بالخصوصية وانخفاض التكلفة وقابلية التوسع، كما يعالج مشكلات مثل RFI والهجمات الجانبية (Ibrahim et al., 2024) (SCA).

وبالاستناد إلى محور أمانIoT ، قدمت دراسة أخرى إطار عمل جديدًا للمصادقة في المنازل الذكية يعتمد على التعلم المُراقب (Supervised Learning) والمعلومات السياقية. يقدم هذا النموذج-SSL) (SHAFآليات مضادة لهجمات كشف المفاتيح، وانتحال الهوية، وسرقة الأجهزة، مع تحقيق مصادقة ثنائية الاتجاه .(Mutual Authentication) ويعتمد على سمات سياقية مثل سجلات نشاط المستخدم، التقويم، وبيانات Bluetooth أو .IP أظهرت النتائج تفوق النموذج من حيث زمن الاستجابة، تكلفة الحساب، ومستوى الخصوصية.

وفي مجال مختلف، قدم **Abdulwahab Ali Almazroi** مخططًا مبتكرًا لمصادقة الكراسي المتحركة الذكية، يركز على تحقيق توازن بين الأمان وانخفاض التعقيد الحسابي. يهدف نظام **SLMAS** إلى تعزيز أمان عملية التحقق باستخدام مصادقة متبادلة بين الجهاز والمستخدم. أظهرت النتائج أن النظام أسرع وأكثر أمانًا وأقل استهلاكًا للموارد مقارنة بالبروتوكولات التقليدية، خاصة في بيئات IoT الحساسة للوقت (Almazroi et al., 2023).

أما دراسة **Abhishek Bansal** فقد تناولت التحديات الأمنية في IoT مع التركيز على المصادقة والتفويض، حيث استعرضت تقنيات مثل الشهادات الرقمية و PKIوحماية البيانات. كما ناقشت محدودية هذه

الأساليب في بيئات IoT ذات الموارد المحدودة، واقترحت استخدام التعلم الآلي لتحسين المصادقة الثنائية. كما أبرزت أهمية تطوير بروتوكولات خفيفة الوزن ومقاومة للهجمات مع تحسين إدارة الثقة (Bansal, 2023).

وفي قطاع الرعاية الصحية، تناولت دراسة (Raja et al., 2024) مفهوم الاتصال الآمن في أجهزة IoT الطبية، مع التركيز على ضمان سلامة البيانات وسريتها. قدمت الدراسة منصة **Light IoT** المصممة لتكون منخفضة الاستهلاك للطاقة وعالية الأمان. تعتمد المنصة على بروتوكولات مثل TLS/SSL و PKIو RBAC، بالإضافة إلى تقنيات تشفير خفيفة مثل XOR والدوال التجزئية، مما يجعلها مناسبة للبيئات الطبية الحساسة والزمنية.

كما قدمت دراسة (Gong et al., 2023) نموذجًا خفيف الوزن وآمنًا للمصادقة عبر المجالات المختلفة في IoT، حيث ركزت على تقليل تكلفة الحساب والاتصال مع الحفاظ على مستوى عالٍ من الأمان. وقد أظهرت النتائج قدرة النظام على تقليل زمن الاستجابة وتحسين الأداء في الأنظمة متعددة الخوادم.

في المقابل، اقترحت دراسة (Wu et al., 2023) نظام مصادقة ذكي للمنازل يعتمد على تقنية Intel SGX مع بوابة مركزية لمنع الهجمات الداخلية. وقد تم التحقق من النموذج باستخدام نموذج(Real or Random (RoR ، وأظهرت النتائج كفاءة عالية في تقليل التكلفة الحسابية وتحسين مستوى الأمان.

وفي مجال إنترنت المركبات(IoV) ، قدمت دراسة (Tabany & Syed, 2024) بروتوكول مصادقة خفيف الوزن يعتمد على عمليات XOR والدوال التجزئية، مما يقلل التعقيد الحسابي بشكل كبير. أظهر النظام قدرة عالية على مقاومة الهجمات مع زمن تنفيذ منخفض جدًا يصل إلى 0.018 مللي ثانية.

أما دراسة (Kavianpour et al., 2023) فقد ركزت على مشكلة البيانات الضخمة فيIoT ، حيث قدمت طريقة مصادقة تعتمد على بيانات بيئية مستخرجة من الحساسات لتحديد الأجهزة ومنع الاتصالات غير الطبيعية. وقد أظهر النموذج كفاءة عالية في اكتشاف محاولات الانتحال مع استهلاك منخفض للطاقة.

وقدمت دراسة (Kumar et al., 2022) آلية مصادقة خفيفة للمنازل الذكية تعتمد على التشفير غير المتماثل، مع مقاومة لهجمات إعادة الإرسال وانتحال الخادم وهجمات .Man-in-the-Middle كما حافظت على أداء جيد من حيث السرعة واستهلاك الطاقة.

وفي دراسة (Bettahar et al., 2024) تم اقتراح مخطط مصادقة آمن وتبادل مفاتيح جلسة باستخدام الدوال التجزئية وعمليات XOR والمفاتيح الديناميكية. كما تم التحقق من صحة النظام باستخدام أدوات BAN logic وAVISPA، مما أكد مقاومته لأنواع متعددة من الهجمات.

أما دراسة (Zuo et al., 2023) فقد قدمت نموذجًا مجهول الهوية وخفيف الوزن للمصادقة في البيئات المنزلية الذكية، حيث يعتمد على دوال تجزئة أحادية الاتجاه وتقنيات تشفير مختلفة، مع تحقيق توازن جيد بين الأمان والكفاءة.

في حين اقترحت دراسة (Fayad et al., 2018) نظام مصادقة وتفويض يعتمد على تقنيةBlockchain ، مما يسمح بتكامل عمليات التحقق والتفويض ضمن إطار واحد قابل للتوسع. وقد أظهرت النتائج كفاءة عالية وتكلفة تنفيذ منخفضة.

وقدمت دراسة (Gonçalves et al., 2023) نموذجًا اتحاديًا (Federated) للمصادقة في الزراعة الذكية باستخدام OpenID Connect و Keycloakو MQTT، مما يسمح بإدارة آمنة للمستخدمين والأجهزة عبر مواقع متعددة.

وأخيرًا، قدمت دراسة (Thakur et al., 2023) آلية مصادقة خفيفة تعتمد على الثقة–(Trust Based Authentication)من مرحلتين، حيث تستخدم عمليات حسابية ثقيلة في المرحلة الأولى وخفيفة في المرحلة الثانية. وقد أظهرت النتائج مقاومة قوية لهجمات مثل MITM و DoSوفقًا لأدوات.AVISPA

المقارنة بين الأعمال ذات الصلة

يوضح هذا القسم مقارنة موجزة بين أحدث الدراسات المتعلقة بآليات المصادقة في .IoT وتعرض هذه المقارنة أهم الأساليب والمنهجيات والتقنيات المستخدمة، بالإضافة إلى تقييمها من حيث مستوى الأمان والأداء ونوع الأجهزة المستهدفة.

الجدول1 : مقارنة بين النماذج السابقة

المرجع	الفكرة الرئيسية	المنهج	التقنيات المستخدمة	مستوى الأمان	الأداء	الأجهزة المستهدفة	النتائج
(Ibrahim et al., 2024)	المصادقة على IoT باستخدام الانبعاثات الكهرومغناطيسية (EM) وPUFs	EM emissions ، التعلم العميق	الشبكات العصبية، المشفرات التلقائية	مرتفع	مرتفع	أجهزة IoT متنوعة	F1-Score = 0.99
(Sudha et al., 2024)	مصادقة المنازل الذكية باستخدام التعلم المُراقب	معلومات سياقية، تعلم مُراقب	بيانات سياقية، مصادقة متعددة العوامل	مرتفع	تقليل العبء الحسابي	أجهزة المنازل الذكية	تحسين زمن الاستجابة وكفاءة التكلفة
(Almazroi et al., 2023)	مصادقة متبادلة خفيفة الوزن للكراسي المتحركة الذكية	مصادقة، تصميم خفيف	مصادقة متبادلة، تقنيات تشفير	مرتفع	كفاءة عالية	كراسي متحركة ذكية	تفوق على البروتوكولات من حيث السرعة والتكلفة والأمان
(Bansal, 2023)	نهج حديث للمصادقة والتفويض في IoT	تقنيات تعلم آلي، PKI ، شهادات رقمية	تجزئة، XOR ، بيانات ECC حيوية	مرتفع	متوسط	شبكات IoT	التركيز على دمج التعلم الآلي والبروتوكولا ت الخفيفة
(Raja et al., 2024)	اتصال آمن باستخدام مصادقة Light متبادلة في IoT	مصادقة متبادلة، Light IoT	TLS/SSL ، RBAC، PKI ، دوال تجزئة خفيفة	مرتفع	مرتفع	في IoT الرعاية الصحية	نقل بيانات آمن وموفر للطاقة
(Gong et al., 2023)	مصادقة خفيفة وآمنة في IoT	مصادقة موزعة، متعددة الطبقات	تشفير متماثل، Challenge-Response	متوسط	مرتفع	أجهزة IoT	تقليل التأخير والحمل الحسابي
(Wu et al., 2023)	نظام وصول آمن للمنازل الذكية	SGX ، بوابة	SGX ، Gateway	مرتفع	متوازن	المنازل الذكية	أمان أعلى مع تكلفة منخفضة

(Tabany & Syed, 2024)	مصادقة خفيفة IoV لمركبات	XOR ، تجزئة	XOR ،Hash functions	مرتفع	منخفض جدًا (0.018 ms)	المركبات	مقاومة هجمات محدودة
(Kavianpour et al., 2023)	مصادقة خفيفة تعتمد على البيئة	متغيرات بيئية	بيانات حساسات، TCP/IP ، Hashing	مرتفع	منخفض التعقيد	أجهزة منخفضة الطاقة	مقاومة الانتحال باستخدام بيانات البيئة
(Kumar et al., 2022)	مصادقة خفيفة للمنازل الذكية	تشفير غير متماثل	Public-key cryptography	مرتفع	منخفض التأخير والطاقة	المنازل الذكية	مقاومة للهجمات مع كفاءة عالية
(Bettahar et al., 2024)	مصادقة آمنة وتبادل مفاتيح جلسة	مفاتيح ديناميكية، Hash	Hash ،XOR ، timestamps	مرتفع	انخفاض الحمل الحسابي	المنازل الذكية	تم التحقق باستخدام BAN وAVISPA
(Zuo et al., 2023)	مصادقة مجهولة خفيفة للمنازل الذكية	مصادقة مجهولة	Hash ،ECC ، PUF	مرتفع	تكلفة منخفضة	IoT أجهزة	أمان وكفاءة عالية
(Fayad et al., 2018)	مصادقة وتفويض باستخدام Blockchain	Blockchain	Java ، Blockchain	مرتفع مع قابلية توسع	خفيف وسريع	IoT بوابات	تكلفة منخفضة وأداء جيد
(Gonçalves et al., 2023)	مصادقة اتحادية للزراعة الذكية	Keycloak ،OpenID	MQTT ، Keycloak	مرتفع	كفاءة عالية	زراعي IoT	إدارة صلاحيات آمنة
(Thakur et al., 2023)	مصادقة قائمة على الثقة	مصادقة ثنائية المرحلة	XOR ، تشفير، قرارات خادم	مرتفع	كفاءة عالية	IoT أجهزة	مقاومة MITM وDoS والتجسس

المنهجية المقترحة Methodology

تهدف المنهجية المقترحة إلى معالجة التحديات الأساسية في أمن إنترنت الأشياء، وخاصة مشكلة المصادقة في بيئات تجمع بين IoT و .OTوعلى عكس أنظمة تكنولوجيا المعلومات التقليدية التي تركز على البيانات، تتعامل أنظمة OTمع العمليات الفيزيائية والتحكم الصناعي، مما يجعل متطلبات الأمان أكثر حساسية وتعقيدًا. لذلك، يجب أن تمر أجهزة IoT بعملية مصادقة قوية قبل دمجها في بيئات OT الهجينة.

يقدم هذا القسم نموذجًا جديدًا للمصادقة متعددة العوامل (MFA) مع إدراك السياق (Context-Aware MFA)، مصمم خصيصًا لتلبية متطلبات أنظمة .OT ويهدف النموذج إلى تعزيز مستوى الأمان مع تقليل التعقيد الحسابي، بما يتناسب مع القيود المفروضة على أجهزة IoT منخفضة الموارد، مع ضمان تشغيل موثوق ومستقر في بيئات.OT

مشكلة آليات المصادقة الحالية

كما تم توضيحه في الأقسام السابقة، تعاني آليات المصادقة الحالية في شبكات IoT من عدة تحديات رئيسية. من أبرز هذه التحديات مشكلة قابلية التوسع، حيث لا تستطيع الأنظمة الحالية التعامل بكفاءة مع الزيادة الكبيرة في عدد الأجهزة المتصلة.

كما أن الاعتماد على أنظمة كلمات المرور أو المصادقة أحادية العامل يؤدي إلى مخاطر أمنية عالية، مثل سهولة الاختراق أو انتحال الهوية (Bansal, 2023). وعلى الرغم من أن أنظمة المصادقة الثنائية توفر مستوى أمان أعلى، إلا أنها تتطلب موارد حسابية كبيرة، مما يجعلها غير مناسبة للأجهزة محدودة القدرة في بيئات IoT (Almazroi et al., 2023).

بالإضافة إلى ذلك، فإن عدم وجود توحيد قياسي في معماريات IoT يؤدي إلى مشاكل في التوافق بين الأجهزة، مما يزيد من صعوبة تحقيق نظام مصادقة آمن وفعال (Kumar et al., 2022) .

وبناءً على ذلك، يتضح وجود حاجة ملحة لتطوير نموذج مصادقة جديد يجمع بين الكفاءة الأمنية وانخفاض التعقيد الحسابي، مع الحفاظ على الأداء المناسب للأجهزة منخفضة الموارد. إن إيجاد حل يوازن بين هذه المتطلبات يعد أمرًا ضروريًا لتعزيز أمان وكفاءة شبكات إنترنت الأشياء.

الحل المقترح(Proposed Solution)

يهدف الحل المقترح إلى تحقيق البساطة وقابلية التوسع في نموذج المصادقة متعددة العوامل (MFA) لعدد كبير من أجهزة إنترنت الأشياء .(IoT) يعتمد هذا النموذج على دمج عدة عوامل مصادقة مع الاعتماد على المعايير السياقية إلى جانب تقنيات التشفير التقليدية، بهدف تعزيز مستوى الأمان مع تقليل التعقيد الحسابي إلى أدنى حد ممكن، خصوصًا في الأجهزة محدودة القدرة.

- نموذج المصادقة متعددة العوامل(MFA)

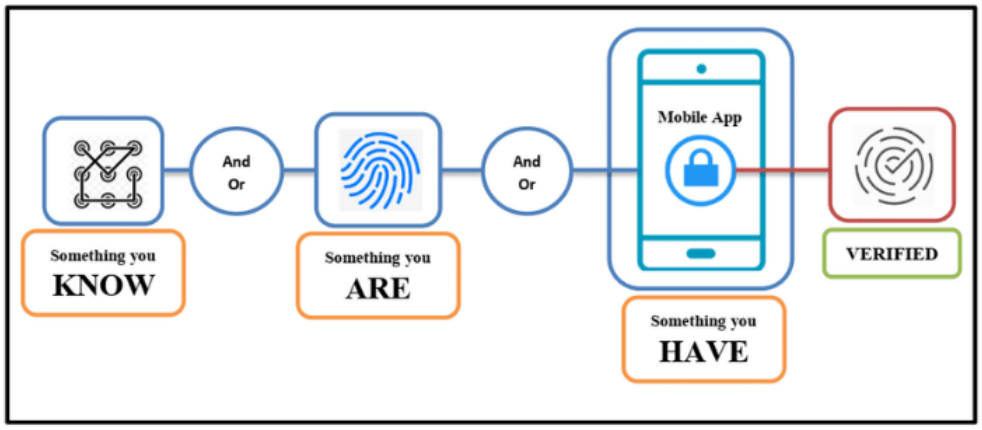
يقترح نموذج المصادقة متعددة العوامل لأجهزة إنترنت الأشياء مجموعة من ثلاث فئات رئيسية من عوامل التحقق:

ما تعرفه(Something You Know) : يعتمد هذا العامل على كلمات المرور التقليدية أو الأرقام السرية (PIN) أو مفاتيح الدخول، مع تطبيق آليات توليد كلمات مرور ديناميكية. يتم تحديث كلمات المرور بشكل دوري، مما يقلل من احتمالية التعرض لهجمات مثل تسريب بيانات الاعتماد أو هجمات التخمين القسري .(Brute Force)كما أن الطبيعة الديناميكية لكلمات المرور تجعلها غير قابلة لإعادة الاستخدام بعد اختراقها، مما يعزز مستوى الأمان.

ما تملكه(Something You Own) : يعتمد هذا العامل على رمز أمان خاص بالجهاز مثل بطاقة RFIDأو أي معرف فريد مرتبط بالجهاز. يهدف هذا العامل إلى ضمان أن الأجهزة المصرح لها فقط هي التي يمكنها الوصول إلى النظام، بينما يتم رفض أي جهاز غير موثوق. كما يمكن استخدام رموز وصول (Access Tokens)كآلية إضافية، بحيث لا يتم منح الوصول إلى الموارد الحساسة إلا للأجهزة التي تمتلك الرمز الصحيح.

ما تكونه(Something You Are) : يعتمد هذا العامل على البيانات البيومترية مثل بصمة الإصبع أو التعرف على الصوت. تم تصميم هذا النوع من المصادقة خصيصًا ليتناسب مع بيئات إنترنت

الأشياء التي تعتمد على الحوسبة الطرفية(Edge Computing) ، مما يقلل الحاجة إلى قدرات حسابية عالية. كما أن استخدام خوارزميات بيومترية خفيفة الوزن ومتوافقة مع بيئات IoT يضمن تحقيق التوازن بين الأمان وكفاءة الأداء دون التأثير على موارد الجهاز.



الشكل 1: مكونات نموذج المصادقة متعددة العوامل (MFA Components)

- المصادقة السياقية(Contextual Authentication)

بالإضافة إلى العوامل الثلاثة التقليدية للمصادقة، يقترح هذا النموذج استخدام المصادقة السياقية كطبقة أمان إضافية. تعزز هذه الآلية عملية التحقق من خلال الاستفادة من المعلومات البيئية والسياقية مثل موقع الجهاز، وقت الوصول، والبيانات الحسية أو التشغيلية.

تُعد المصادقة المعتمدة على السياق ذات أهمية خاصة في بيئات التكنولوجيا التشغيلية(OT) ، نظرًا للطبيعة المستقرة والمقيدة نسبيًا للمعايير السياقية. فعوامل مثل موقع الجهاز، والجداول الزمنية لتشغيل النظام، والظروف الصناعية المحيطة غالبًا ما تكون ثابتة أو ضمن أنماط محددة مسبقًا. على سبيل المثال، قد تسمح بعض أنظمة التحكم الصناعية بالوصول فقط خلال فترات الصيانة أو عند وجود الأجهزة ضمن نطاقات مادية محددة.

تعزز هذه الطبقة السياقية الإضافية مستوى الأمان بشكل كبير، حيث تضمن أن عملية المصادقة لا تعتمد فقط على بيانات اعتماد ثابتة، بل أيضًا على ظروف تشغيلية آنية. كما أنها تدعم متطلبات السلامة والموثوقية في أنظمة OTمن خلال تقليل مخاطر الوصول غير المصرح به أو السلوك غير الطبيعي أثناء العمليات الحرجة.

- التقنيات التشفيرية خفيفة الوزن

نظرًا للطبيعة المحدودة موارد أجهزة إنترنت الأشياء(IoT) ، يعتمد الإطار المقترح على آليات تشفير خفيفة لتحقيق توازن مثالي بين الأمان والكفاءة الحسابية. يتم استخدام التقنيات التالية:

تشفير المنحنيات الإهليلجية:(ECC)

يوفر ECC مستوى عالٍ من الأمان باستخدام أحجام مفاتيح أصغر بكثير مقارنة بخوارزميات التشفير ذات المفتاح العام التقليدية. وهذا يجعله مناسبًا جدًا لأجهزة IoT ذات القدرة المحدودة في المعالجة والذاكرة. كما أنه ملائم لبيئات OTالتي تتطلب اتصالات آمنة طويلة الأمد مع تقليل الحمل الحسابي. وتتيح كفاءته تنفيذ عمليات مصادقة سريعة، وهو أمر ضروري في التطبيقات الزمنية الحساسة. كما يُعد مقاومًا لعدة نماذج هجوم متقدمة، مما يعزز متانة النظام على المدى الطويل.

تشفير :XOR

يتم استخدام عمليات XOR خفيفة لتشفير بيانات المصادقة أثناء نقلها. توفر هذه الطريقة تشفيرًا سريعًا وفعالًا مع تقليل كبير في الاستهلاك الحسابي، مما يجعلها مناسبة لبيئات OT التي تتطلب زمن استجابة منخفضًا واستهلاكًا محدودًا للموارد.

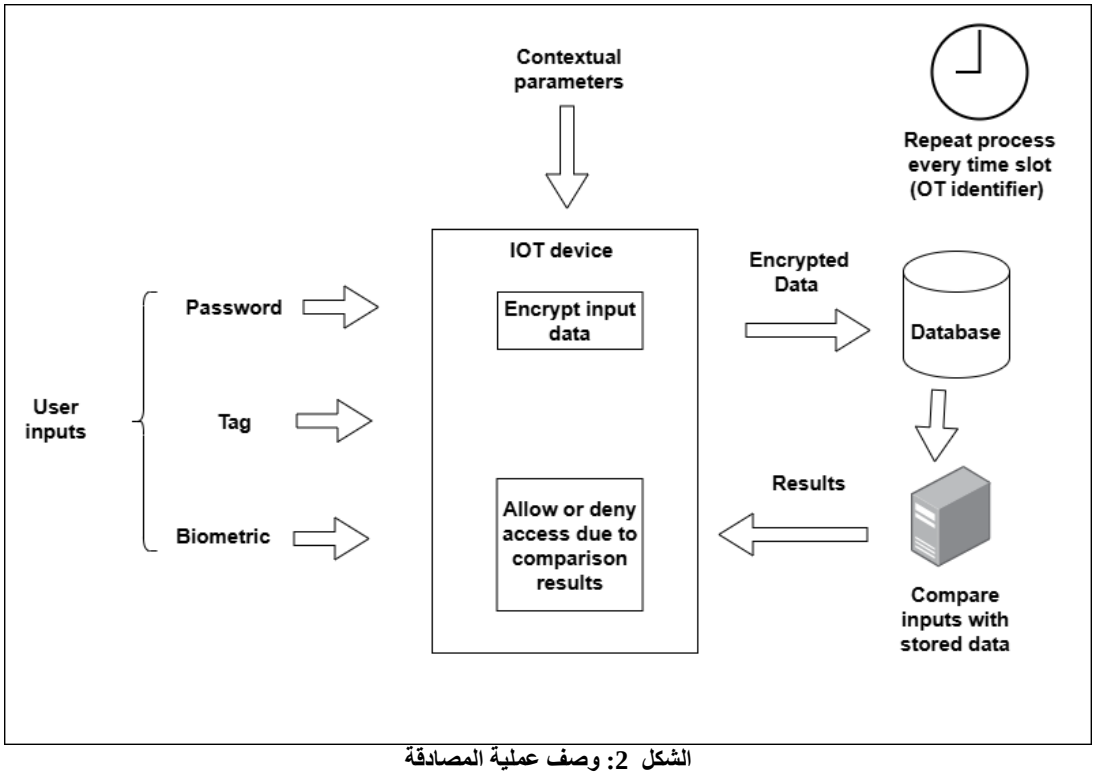
دوال التجزئة:(Hash Functions)

تُستخدم الدوال أحادية الاتجاه لضمان سلامة البيانات وتأمين تبادل المعلومات بين أجهزة IoT والأنظمة المركزية. توفر هذه الدوال مقاومة قوية لهجمات إعادة الإرسال وهجمات الوسيط(MITM) ، حيث تجعل البيانات غير قابلة للاسترجاع أو إعادة الاستخدام. كما تدعم الكشف عن التلاعب في قنوات الاتصال بين IoT و.OT

بشكل عام، يُعد ECC العمود الفقري التشفيري الأساسي في إطار المصادقة المقترح نظرًا لتوازنه بين الأمان العالي وكفاءة الأداء. ويضمن دمجه دعم بيئات IoT محدودة الموارد مع مقاومة قوية للتهديدات الحديثة.

3-نتائج البحث ومناقشتها:

تتكون عملية المصادقة المقترحة من عدة مراحل متسلسلة ومتوازية لضمان أمان شامل خلال جميع مراحل التفاعل مع نظام إنترنت الأشياء.



الشكل 2: وصف عملية المصادقة

مرحلة التسجيل: في مرحلة التسجيل، يقوم المستخدم أو الجهاز بتقديم بيانات المصادقة مثل كلمات المرور، الأرقام السرية(PIN) ، البيانات البيومترية، والمعايير السياقية مثل الموقع وسجل الوصول السابق. يتم

تخزين هذه البيانات بشكل آمن داخل النظام، ويتم إنشاء معرف فريد لمرة واحدة (OT Identifier) مرتبط بهذه البيانات. يُستخدم هذا المعرف كمرجع دائم للجلسات المستقبلية.

مرحلة المصادقة: في هذه المرحلة، يقوم المستخدم أو الجهاز بإدخال بيانات المصادقة مثل كلمة المرور، PIN، البيانات البيومترية، والمعلومات السياقية مثل الموقع وسجل الوصول. يقوم النظام بمقارنة هذه البيانات مع المعلومات المخزنة مسبقًا. عند نجاح التحقق، يتم إنشاء معرف OT جديد خاص بالجلسة الحالية لضمان أمان الاتصال ومنع إعادة استخدام بيانات الاعتماد.

إعادة المصادقة الديناميكية: تهدف إعادة المصادقة الديناميكية إلى تأمين الجلسات طويلة الأمد. بخلاف المصادقة الثابتة التي تتم مرة واحدة فقط عند تسجيل الدخول، تقوم هذه الآلية بإعادة التحقق بشكل دوري بناءً على التغيرات السياقية أو السلوك غير الطبيعي.

على سبيل المثال، إذا انتقل المستخدم من بيئة إلى أخرى (مثل الانتقال من المنزل إلى موقع خارجي)، يقوم النظام بتفعيل عملية إعادة المصادقة. قد تتضمن هذه العملية التحقق البيومتري أو إرسال كلمة مرور لمرة واحدة .(OTP)تضمن هذه الآلية استمرار أمان الجلسة ومنع أي اختراق أثناء التشغيل.

التحقق خفيف الوزن: يتم تطبيق تقنيات التشفير خفيفة الوزن مثل ECC و XORودوال التجزئة للتحقق من هوية الأجهزة وتأمين نقل البيانات. تساعد هذه التقنيات في الحفاظ على سرية وسلامة البيانات مع تقليل استهلاك الموارد الحسابية.

دمج معرفات الاستخدام لمرة واحدة(OT Identifiers)

- يتم إنشاء معرف OT جديد لكل جلسة مصادقة .
- يكون هذا المعرف فريدًا ومؤقتًا ومشفرًا لمنع إعادة الاستخدام .
- يتم تحديثه أثناء إعادة المصادقة الديناميكية لضمان استمرار أمان الجلسة .
- يساهم ذلك في تقليل مخاطر هجمات إعادة الإرسال .(Replay Attacks)

وصف عملية الاختبار(Pseudo Code)

يتكون تدفق النظام من أربع مراحل رئيسية: التسجيل، المصادقة، إعادة المصادقة الديناميكية، والتحقق باستخدام التشفير الخفيف. (يتم عرض الكود الزائف في الملحق)

مرحلة التسجيل :إنشاء هوية الجهاز/المستخدم ومعرف .OT.

مرحلة المصادقة :التحقق من البيانات وإنشاء معرف جلسة .

إعادة المصادقة الديناميكية :التحقق المستمر بناءً على السياق .

التحقق خفيف الوزن :ضمان أمان الاتصال باستخدام التشفير الخفيف .

تعمل هذه المراحل معًا لضمان نظام مصادقة آمن وقابل للتوسع وفعال في بيئات.IoT

4- الاستنتاجات والتوصيات

الاستنتاجات

يعالج إطار المصادقة المقترح التحديات الأساسية في بيئات إنترنت الأشياء، مثل الحاجة إلى المصادقة المستمرة، الحماية من اعتراض بيانات الاعتماد، وتحسين كفاءة استخدام الموارد. يضمن استخدام معرفات OT أن تكون كل جلسة فريدة وقابلة للتتبع، مما يقلل بشكل كبير من مخاطر إعادة الاستخدام وهجمات إعادة الإرسال.

تعزز إعادة المصادقة الديناميكية من مرونة النظام من خلال دمج الوعي السياقي. فعند حدوث تغييرات في موقع المستخدم أو البيئة التشغيلية، يتم تفعيل خطوات تحقق إضافية لضمان أمان الجلسة. وهذا مهم بشكل خاص في التفاعلات طويلة المدى.

تساعد تقنيات التشفير خفيفة الوزن مثل ECC و XORفي الحفاظ على مستوى عالٍ من الأمان دون زيادة العبء الحسابي أو استهلاك الطاقة، مما يجعل النموذج مناسبًا للأنظمة واسعة النطاق ذات الموارد المحدودة.

بشكل عام، من المتوقع أن يؤدي هذا النموذج إلى تحسين كبير في الأمان، القابلية للتوسع، والقدرة على التكيف في بيئات IoT المختلفة.

التوصيات

1. يمكن تطوير النموذج مستقبلًا عبر دمج تقنيات الذكاء الاصطناعي لتوقع السلوك غير الطبيعي وتحسين إعادة المصادقة. كما يمكن استكشاف استخدام معرفات OT متقدمة تعتمد على البلوك تشين أو التشفير المقاوم للحوسبة الكمومية.
2. كذلك، يجب تحسين تقنيات التشفير الخفيف بما يتناسب مع فئات أجهزة IoT المختلفة، مع إجراء اختبارات عملية في بيئات IoT و OTحقيقية لتقييم الأداء والقابلية للتوسع.

5- المراجع:

ALMAZROI, A. A., LIAQAT, M., ALI, R. L., & GANI, A. 2023. SLMAS: A Secure and Light Weight Mutual Authentication Scheme for the Smart Wheelchair. *Applied Sciences 2023, Vol. 13, Page 6564*, *13*(11), 6564.

BANSAl, A. 2023. Authentication and Authorization in an IoT Based System:

A Modern Approach. *ISSA Journal*, 15–18.

BETTAHAR, M. H., LOUAZANI, A., & SEKHRI, L. 2024. *Secure and efficient authentication framework for IoT-based smart home using dynamic key*.

FAYAD, A., HAMMI, B., & KHATOUN, R. 2018. An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach. *2018 3rd International Conference on Security of Smart Cities, Industrial Control System and Communications, SSIC 2018 - Proceedings*, 1–7.

GONÇALVES, C., SOUSA, B., VUKOVIC, M., & KUSEK, M. 2023. A federated authentication and authorization approach for IoT farming. *Internet of Things*, *22*, 100785.

GONG, B., ZHENG, G., WAQAS, M., Tu, S., CHEN, S., GONG, B., ZHENG, G., WAQAS, M., Tu, S., & CHEN, S. 2023. LCDMA: Lightweight cross-domain mutual identity authentication scheme for internet of things. *IEEE Internet of Things Journal*, *10*(14), 12590–12602.

IBRAHIM, O. A., SCIANCALEPORE, S., & DI PIETRO, R. 2024. MAG-PUFs: Authenticating IoT devices via electromagnetic physical unclonable functions and deep learning. *Computers & Security*, *143*, 103905.

KAVIANPOUR, S., RAZAQ, A., & HALES, G. 2023. *A secure lightweight authentication mechanism for IoT devices in generic domain*.

KUMAR, V., MALIK, N., SINGLA, J., JHANJHI, N. Z., AMSAAD, F., & RAZAQUE, A. 2022. Light Weight Authentication Scheme for Smart Home IoT Devices. *Cryptography 2022, Vol. 6, Page 37*, *6*(3), 37.

MORAIS, D., ZUQUETE, A., & MENDES, A. 2023. Adaptive, Multi-Factor Authentication as a Service for Web Applications. *2023 7th Cyber Security in Networking Conference, CSNet 2023*, 74–80.

RAJA, A., SAHANA, M. S., PRATHIBBHAVANI, P. M., & VENUGOPAL, K. R. 2024. Secure Communication using Mutual Authentication in Light IoT. *Proceedings of ICWITE 2024: IEEE International Conference for Women in Innovation, Technology and Entrepreneurship*, 471–476.

SUDHA, K. S., JEYANTHI, N., IWENDI, C., SUDHA1, K. S., JEYANTHI2, N., IWENDI3, and C., SUDHA, K. S., JEYANTHI, N., & IWENDI, C. 2024. Secure Supervised Learning-Based Smart Home Authentication Framework. *International Journal of Computer Networks & Communications (IJCNC), Vol.16, No.1*, *16*(16), 1. https://doi.org/10.5121/IJCNC.2024.16101

TABANY, M., & SYED, M. 2024. A lightweight mutual authentication protocol for internet of vehicles. *Journal of Advances in Information Technology*, *15*(2), 155–163.

THAKUR, A., KUMAR, P., & CHAURASIA, N. 2023. *A Lightweight Trust Based Secure Authentication Mechanism for IoT Devices*.

WU, T. Y., MENG, Q., CHEN, Y. C., KUMARI, S., & CHEN, C. M. 2023. Toward a Secure Smart-Home IoT Access Control Scheme Based on Home Registration Approach. *Mathematics 2023, Vol. 11, Page 2123*, *11*(9), 2123.

ZUO, X., WANG, Z., Li, A., HUO, Y., & NIU, S. 2023. A Lightweight Anonymous Authentication and Key Negotiation Scheme in Smart Home Environments. *Wuhan University Journal of Natural Sciences*, *28*(6), 523–530.

6-الملحق (الكود):

```
>> Registration Phase
Function Reg (userInput):
   Input password, PIN, biometricData, contextualData
   OT_Identifier = GenerateOTIdentifier(userInput, timestamp)
   Store(userInput, OT_Identifier)
   Return "Registration process Success"

>> Authentication Phase
Function Auth(userInput):
   Input password, PIN, biometricData, contextualData
   storedData = RetrieveFromDatabase(userInput.identifier)
   If Verify(userInput, storedData):
      New_OT_ID = GenerateOTIdentifier(userInput, timestamp)
      UpdateOTIdentifierInDatabase(userInput.identifier, New_OT_ID)
      Return "Authentication Process Success", New_OT_Identifier
   Else:
      Return "Authentication Process Failed"

>>Dynamic Reauthentication
Function DynamicReauthentication(userInput, currentContext):
   If ContextChanged(currentContext) OR SuspiciousActivityDetected():
      Collect additionalBiometric OR GenerateOneTimePassword(OTP)
     If VerifyAdditionalCredentials(userInput, currentContext):
        New_OT_Identifier = GenerateOTIdentifier(userInput, timestamp)
        UpdateOTIdentifierInDatabase(userInput.identifier,
New_OT_Identifier)
        Return "Reauthentication Successful", New_OT_Identifier
      Else:
        Return "Reauthentication Failed"
   Else:
      Return "No Reauthentication Needed"

>> Lightweight Verification
Function LightweightVerification(data):
   EncryptedData = ApplyLightweightEncryption(data)
   verificationResult = CentralSystem.VerifyEncryptedData(EncryptedData)
   Return verificationResult

// Generate OT Identifier
Function GenerateOTIdentifier(userInput, timestamp):
   OT_Identifier = HashFunction(userInput + timestamp)
   Return OT_Identifier

>>Integration of One-Time Identifiers
Function HandleOTIdentifiers(userInput, sessionData):
   OT_Identifier = GenerateOTIdentifier(userInput, timestamp)
```

```
        If ReplayAttackDetected(OT_Identifier):
        Return "Access Denied: Replay Attack Detected"
    Else:
        StoreOTIdentifierInSession(sessionData, OT_Identifier)
        Return "OT Identifier Valid"

>> Test process
Function IoTAuthenticationProcess():
    Reg (userInput)
    Auth(userInput)
    While SessionActive:
        DynamicReauthentication(userInput, currentContext)
    verificationResult = LightweightVerification(data)
    If verificationResult == "Verified":
        ProceedWithSession()
    Else:
        TerminateSession()
```