SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.5 NO. 4 2026
DOI: 10.51984/F4S09Q48

وقائع مؤتمرات جامعة سبها
Sebha University Conference Proceedings
Conference Proceeding homepage: http://www.sebhau.edu.ly/journal/CAS

بروتوكول مصادقة متبادلة خفيف لأنظمة RFID الصحية باستخدام خوارزمية ASCON نموذج مقترح لتعزيز أمن بطاقات التأمين الصحي للمتقاعدين

فاطمة فؤاد الشريف[a]* ، فاطمة إمحمد مرعي امحمد[b] ,عبدالسلام بودربالة محمد أبو ذراع[b] ، عبدالقادر عبدالسلام سالم [b]

[a] قسم الحاسوب، كلية التربية الغريفة، جامعة سبها، ليبيا
[b] قسم الحاسوب، كلية التربية زويلة، جامعة سبها، ليبيا

الملخص

تعالج هذه الدراسة أوجه القصور في آليات التحقق التقليدية في بطاقات التأمين الصحي، ولا سيما الأنظمة القائمة على رمز الاستجابة السريعة (Code QR) العرضة للتزوير. فهذه الأنظمة معرّضة للتزوير، وإعادة الاستخدام، والتنصت، وقد تسمح بالوصول غير المصرح به إلى بيانات طبية حساسة. لذلك تقترح هذه الدراسة بروتوكول مصادقة متبادلة خفيف الوزن لأنظمة RFID في بيئة الرعاية الصحية، يعتمد على خوارزمية ASCON، وهي خوارزمية تشفير خفيف تدعم التشفير الموثق بالبيانات المرتبطة (AEAD) ودوال التجزئة. يتكون النموذج من ثلاثة أطراف هي بطاقة RFID منخفضة الموارد، وقارئ RFID يعمل وسيطاً للاتصال، وخادم خلفي موثوق يتولى إدارة المفاتيح وقاعدة البيانات. يستخدم البروتوكول أرقاماً عشوائية حديثة ومفاتيح مؤقتة مشتقة، ويتم تبادل رسائل مشفرة مزودة بوسوم تحقق، وينشئ في النهاية مفتاح جلسة فريداً لكل عملية مصادقة. خضع البروتوكول للتحقق الرسمي باستخدام منطق BAN وأداة ProVerif، إلى جانب تحليل أمني غير رسمي للهجمات وتقدير للتكلفة الحسابية والاتصالية. وأظهرت النتائج أن البروتوكول يحقق المصادقة المتبادلة، وسرية المفتاح، وحداثة الجلسة، ويقاوم هجمات إعادة الإرسال، والانتحال، والتنصت، والرجل في المنتصف، وفقدان التزامن. وبلغت تكلفته الحسابية نحو 21.7 ميكروثانية، في حين بلغت تكلفة رسالتي المصادقة الأساسيتين نحو 768 بت، وترتفع إلى 896 بت عند تضمين قيمة التحدي الاختيارية RN0، مما يجعله مناسباً لتطوير بطاقات تأمين صحي أكثر أماناً وقابلية للتوسع للمتقاعدين.

الكلمات المفتاحية:

RFID
ASCON
المصادقة المتبادلة
التشفير الخفيف
بطاقات التأمين الصحي
ProVerif

A Lightweight Mutual Authentication Protocol for Healthcare RFID Systems Using the ASCON Algorithm

Fatma Foad Alshrif [a]*, Fatima Imhamed Marei Imhamed [b], Abdulsalam Bouderbala Mohamed Abu Dhraa [b], Abdulqader Abdulsalam Salem

[a] Sebha University, Faculty of Education - Al-Ghurayfa, Al-Ghurayfa, Libya.
[b] Sebha University, Faculty of Education - Zuwayla, Libya

Keywords:

RFID
ASCON
Mutual Authentication
Lightweight Cryptography
Health Insurance Cards
ProVerif

ABSTRACT

This study addresses the shortcomings of traditional verification mechanisms used in health insurance cards, particularly systems based on Quick Response (QR) codes. These systems are vulnerable to forgery, replay, and eavesdropping, potentially allowing unauthorized access to sensitive medical data. To address these challenges, this study proposes a lightweight mutual authentication protocol for RFID-based healthcare systems using the ASCON lightweight cryptographic algorithm, which supports Authenticated Encryption with Associated Data (AEAD) and cryptographic hash functions. The proposed model consists of three entities: a resource-constrained RFID tag, an RFID reader that serves as a communication intermediary, and a trusted backend server responsible for key management and database administration. The protocol employs fresh random nonces and derived temporary keys, exchanges encrypted messages protected by authentication tags, and establishes a unique session key for each authentication session. The proposed protocol was formally verified using BAN logic and the ProVerif tool, in addition to an informal security analysis and an evaluation of its computational and communication costs. The

*Corresponding author:
E-mail addresses: fat.alshareef@sebhau.edu.ly ,(F. I. M. Imhamed) at.mare@sebhau.edu.ly
,(A. B. Abu Dhraa) abd.abthiraa@feduzew.sebhau.edu.ly ,(A. A. Salem) abda.mohammed6@feduzew.sebhau.edu.ly

Article History : Received 30 May 2026 - Received in revised form 30 September 2026 - Accepted 11 November 2026

theoretical results demonstrate that the protocol achieves mutual authentication, key secrecy, and session freshness while resisting replay, impersonation, eavesdropping, man-in-the-middle, and desynchronization attacks. The estimated computational cost is approximately 21.7 µs, whereas the communication cost of the two main authentication messages is approximately 768 bits, increasing to 896 bits when the optional RN0 challenge is included, making the proposed protocol a suitable solution for developing more secure and scalable RFID-based health insurance cards for retirees.

1. المقدمة

أصبحت أنظمة الرعاية الصحية الرقمية تعتمد بصورة متزايدة على البطاقات الذكية وتقنيات إنترنت الأشياء لتسريع التحقق من هوية المستفيدين منها، وتسهيل الوصول إلى الخدمات الطبية، وربط العيادات والمستشفيات وقواعد البيانات. وفي سياق بطاقات التأمين الصحي للمتقاعدين، لا تكون المشكلة تقنية فقط، بل ترتبط أيضًا بحماية فئة المتقاعدين، التي تحتاج إلى خدمة سريعة وموثوقة دون تعريض بياناتها الصحية أو الشخصية للخطر. لذلك ينبغي لأي نظام مقترح أن يحقق سرية البيانات، والتحقق المتبادل، وكفاءة التنفيذ على الأجهزة المقيدة [1]، [2]. كما تمثل قضايا أمن RFID وخصوصيتها أساسًا تصميميًا مهمًا عند ربط البطاقات الذكية بقواعد البيانات الطبية [3]. لذلك فإن أي نظام تحقق ينبغي أن يوازن بين سهولة الاستخدام، وانخفاض التكلفة، ومقاومة الهجمات، وقابلية العمل في بيئات محدودة الموارد.

تعتمد بعض الحلول الحالية على رموز QR لأنها سهلة الطباعة والقراءة، إلا أن هذه البساطة نفسها تجعلها عرضة للنسخ والتزوير وإعادة الاستخدام. وقد ناقشت الدراسات السابقة القيود الأمنية المرتبطة بالاعتماد على رموز QR الثابتة، بما في ذلك النسخ وإعادة الاستخدام والتوجيه إلى محتوى مزيف [4]. كما أن QR Code لا يوفر مصادقة متبادلة حقيقية بين البطاقة والقارئ والخادم؛ فالقارئ غالباً يقرأ قيمة ثابتة أو رابطاً مخزناً، دون أن تتمكن البطاقة من التحقق من شرعية الطرف المقابل. ونتيجة لذلك يمكن للمهاجم أن يستنسخ الرمز أو يعيد استخدامه أو يوجه المستخدم إلى خدمة مزيفة إذا لم تكن هناك طبقات تحقق إضافية.

تقدم تقنية RFID بديلاً عملياً لأنها تسمح بتبادل البيانات لاسلكياً عبر موجات الراديو دون الحاجة إلى رؤية بصرية مباشرة. غير أن استخدام RFIDوحده لا يكفي لضمان الأمن المطلوب. ولهذا تبرز الحاجة إلى بروتوكول مصادقة خفيف يناسب بطاقات RFID منخفضة القدرة، ولا يعتمد على خوارزميات ثقيلة مثل RSA أو ECC في طرف البطاقة؛ وهو اتجاه تدعمه الدراسات السابقة للتشفير الخفيف المخصص لأنظمة RFID المقيدة الموارد [5]. من هنا تأتي أهمية خوارزمية ASCON، التي توفر تشفيراً موثقاً خفيفاً وفعالاً للأجهزة المقيدة، مع دعم السرية وسلامة الرسائل في عملية واحدة، وقد اعتمدت خوارزمية ASCON من ضمن معيار NIST للتشفير الخفيف للأجهزة المقيدة [6]. تهدف هذه الدراسة إلى تصميم بروتوكول مصادقة متبادلة خفيف الوزن قائم على خوارزمية ASCON لتعزيز أمن بطاقات التأمين الصحي المعتمدة على تقنية RFID. ويركز البروتوكول على تحقيق المصادقة المتبادلة، وحماية سرية البيانات، ومقاومة الهجمات الأمنية الشائعة، مع المحافظة على انخفاض التكلفة الحسابية والاتصالية بما يلائم البيئات محدودة الموارد. وقد جرى تقييم البروتوكول من خلال التحقق الرسمي باستخدام منطق BAN وأداة ProVerif، إلى جانب تحليل أمني وتقدير للتكلفة الحسابية والاتصالية استناداً إلى قيم مرجعية واردة في الدراسات السابقة.

1.1 مشكلة البحث وأهدافه

تتمثل مشكلة البحث في كيفية توفير مصادقة متبادلة آمنة وخفيفة بين بطاقة RFID والقارئ والخادم في نظام بطاقات التأمين الصحي، مع الحفاظ على سرية البيانات وحماية هوية المتقاعد ومقاومة الهجمات الشائعة دون تحميل البطاقة عبئاً حسابياً مرتفعاً مع ضمان قابلية التوسع عند زيادة عدد البطاقات والمستخدمين ومرافق الرعاية الصحية. ويمكن تفصيل هذه المشكلة في خمسة جوانب:

- ضعف QR Code أمام النسخ وإعادة الاستخدام؛ غياب التحقق المتبادل بين الأطراف؛ حساسية البيانات الطبية؛ ومحدودية موارد بطاقات RFID.
- تصميم نموذج مصادقة متبادلة بين البطاقة والخادم عبر قارئ وسيط، بحيث لا يكشف البروتوكول الهوية الحقيقية للبطاقة في القناة العامة.
- استخدام ASCON بوصفها خوارزمية تشفير خفيف مناسبة للتطبيقات المقيدة، مع الاستفادة من نمط AEAD لتوفير السرية وسلامة الرسالة معاً.
- إثبات حداثة الجلسة ومقاومة إعادة الإرسال عبر أرقام عشوائية تتغير في كل جلسة، ثم اشتقاق مفتاح جلسة مستقل.
- تحليل البروتوكول رسمياً باستخدام منطق BAN وProVerif، وتحليله غير رسمياً ضد أبرز الهجمات، ثم تقدير كلفته الحسابية والاتصالية وتقييم قابلية توسعه من خلال تحليل تأثير زيادة عدد البطاقات والمستخدمين على متطلبات التخزين والكلفة الحسابية والاتصالية.

2.1 الخلفية العلمية والدراسات ذات الصلة

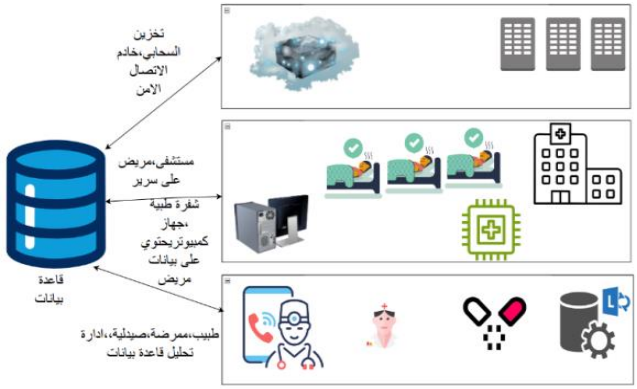
تطورت بروتوكولات المصادقة الخفيفة للأنظمة محدودة الموارد في اتجاهين رئيسيين. يعتمد الاتجاه الأول على عمليات حسابية بسيطة، مثل عملية XOR، والإزاحة، ودوال التجزئة، بهدف خفض التكلفة الحسابية والاتصالية، بينما يعتمد الاتجاه الثاني على خوارزميات التشفير الخفيف الموثق لتحقيق السرية وسلامة الرسائل في آن واحد. وفي هذا السياق، قدمت الدراسة المسحية التي أجراها Ashrif وآخرون [7] تحليلاً شاملاً لبروتوكولات المصادقة واتفاق المفاتيح في شبكات 6LoWPAN، وصنفت التقنيات المستخدمة، ونماذج التهديد، وأساليب التحقق الرسمي، وأشارت إلى استمرار التحديات المتعلقة بالخصوصية، والكفاءة، وقابلية التوسع.

وفي مجال أنظمةRFID ، يعتمد بروتوكول UDAP على عمليات حسابية خفيفة تشملXOR ، والإزاحة، والضرب النقطي لتقليل الحمل الحسابي [8]. كما يستخدم بروتوكول MedIoT-LAP التشفير الموثق الخفيف مع الدوال الفيزيائية غير القابلة للاستنساخ (PUFs) لتعزيز أمن تطبيقات إنترنت الأشياء الطبي [9]، بينما يستفيد بروتوكول MAP-PRINCE من خوارزمية PRINCE لتقليل تكلفة المصادقة في الوسوم محدودة الموارد [10]. وفي اتجاه آخر، اقترحت بعض الدراسات بروتوكولات للمصادقة الجماعية القائمة على آليات العتبة [11]، في حين قدمت دراسة Ghosh وآخرين بروتوكول مصادقة لبطاقات RFID الطبية يعتمد على أكواد

LCDلتحسين الكفاءة الأمنية وتقليل التكلفة الحسابية [12].

وفي بيئات الاتصال بين الآلات (M2M)، اقترح Ashrif وآخرون في دراسة أخرى لهم بروتوكول PSLAE للمصادقة والتشفير الموثق في تطبيقات Industry 4.0، والذي يجمع بين دوال التجزئة، وعملية XOR، والتشفير الموثق، والهويات المستعارة، والقيم العشوائية الحديثة، بهدف تقليل التكلفة الحسابية والاتصالية، مع توفير مقاومة لهجمات التتبع، وإعادة الإرسال، وتسرب الأسرار المؤقتة [13]. كما قدم Ashrif وآخرون بروتوكولاً آخر خفيفاً للمصادقة واتفاق المفاتيح في شبكات 6LoWPAN المخصصة لاتصالات M2M، يعتمد على عمليات تشفير متماثل منخفضة الكلفة وبنية عنقودية، مع التحقق الرسمي من خصائصه الأمنية [14]. وطور Ashrif وآخرون لاحقاً مخططاً آمناً وخفيفاً للمصادقة يدعم الحركة الجماعية في شبكات 6LoWPAN، مع التركيز على الحفاظ على كفاءة المصادقة أثناء انتقال العقد المتحركة بين المجموعات [15].

ورغم أهمية هذه الأعمال، فإنها تستهدف في الغالب سياقات 6LoWPAN أو M2M أو RFID العامة، بينما لا يعالج كثير منها بصورة متكاملة متطلبات بطاقة تأمين صحي فردية، مثل إخفاء الهوية، واسترداد التزامن، وربط المصادقة بسياق بيانات طبية حساسة. ويتميز النموذج المقترح بأنه يجمع بين أربعة عناصر في تصميم واحد: اعتماد ASCON كخوارزمية خفيفة معيارية، واستخدام أرقام عشوائية وقيم اشتقاق مفاتيح حديثة، وإدراج آلية لاسترداد التزامن عبر احتفاظ الخادم بالقيم الحالية والسابقة، وتقديم تحقق شكلي وتحليل أداء نظري. وبذلك لا يقتصر الإسهام على استبدال QR Code بتقنية RFID، بل يضيف طبقة بروتوكولية آمنة تجعل RFID أكثر ملاءمة لبيئة البيانات الطبية. ويلخص جدول 1 أبرز الفروق بين النموذج المقترح والأعمال ذات الصلة.



شكل 1. بيئة عمل النظام المقترح

جدول 1. مقارنة بين البروتوكول المقترح وبعض الأعمال ذات الصلة.

البروتوكول	السنة	التقنيات المستخدمة	التحقق	نقاط القوة	نقاط الضعف
UDAP	2024	XOR/إزاحة/ضرب نقطي	Scyther	خفيف جداً	لا يعالج إخفاء الهوية وفقدان التزامن بوضوح
MedIoT-LAP	2025	SPARKLE + PUFs	ProVerif + BAN	إخفاء هوية ومقاومة هجمات	لا يقدّم آلية استرداد تزامن واضحة
MAP-PRINCE	2025	PRINCE	تحليل نظري/محاكاة	زمن استجابة جيد	عدد عمليات تشفير أعلى
بروتوكول عتبة جماعي	2025	هاش + عتبة	Tamarin	مناسب للمصادقة الجماعية	ليس موجهاً للمصادقة الفردية
البروتوكول المقترح	هذه الدراسة	ASCON + KDF + Nonces	BAN + ProVerif	تزامن، إخفاء هوية، تكلفة منخفضة	لم ينفذ بعد على عتاد حقيقي

2. المواد وطرق العمل

1.2 بنية النظام المقترح

يتكون النظام من ثلاثة مكونات مترابطة. الأول بطاقة RFID أو الوسمTag ، وهي بطاقة التأمين الصحي التي يحملها المتقاعد، وتخزّن معرّفاً سرياً ومفتاحاً أولياً مشتركاً مع الخادم. والثاني القارئReader ، ويوجد في العيادة أو المستشفى، ويعمل كقناة تمرير بين البطاقة والخادم دون أن يمتلك المفاتيح السرية الأساسية. والثالث الخادم الخلفيBackend Server ، وهو الجهة المركزية المسؤولة عن قاعدة البيانات، وإدارة المفاتيح، والتحقق من صحة الرسائل، وإنتاج رسائل الاستجابة ومفاتيح الجلسة .بطاقة ⇄ (Tag) RFID قارئ ⇄ (Reader) RFID الخادم الخلفي وقاعدة البيانات. شكل(1). البنية العامة للنظام المقترح وتدفق الاتصال بين الأطراف الثلاثة.

تقلل هذه البنية العبء على البطاقة، لأن العمليات الأكثر حساسية، مثل البحث في قاعدة البيانات وإدارة القيم الحالية والسابقة، تتم في الخادم. كما يقل خطر اختراق القارئ، لأنه لا يحتاج إلى معرفة هوية البطاقة الحقيقية ولا إلى امتلاك المفتاح السريK، بل يمرر الرسائل المشفرة فقط. ويناسب هذا التصميم بيئة المستشفيات، حيث قد تتعدد نقاط القراءة ويبقى الخادم نقطة الثقة المركزية.

كما يراعي التصميم قابلية التوسع من خلال إبقاء القارئ كوسيط بسيط دون الحاجة إلى تخزين مفاتيح لكل بطاقة، بينما تتم إدارة السجلات والمفاتيح مركزياً في الخادم، مما يسمح بإضافة بطاقات ومرافق صحية جديدة دون تعديل بنية الاتصال الأساسية.

جدول 2. الرموز الأساسية في البروتوكول المقترح.

الرمز	الدلالة
TID	هوية سرية أو معرف مستعار للبطاقة
RID	هوية القارئ عند الحاجة في مرحلة التسجيل أو السياسات
K	مفتاح سري مشترك بين البطاقة والخادم
RN0	قيمة تحدي عامة يولدها القارئ لبدء الجلسة
RN1	رقم عشوائي تولده البطاقة في بداية المصادقة
RN2, RN3	قيمتان عشوائيتان يولدهما الخادم أثناء الاستجابة
K1, K2	مفاتيح مؤقتة مشتقة من K والقيم العشوائية
SK	مفتاح جلسة جديد وفريد لكل عملية مصادقة
CT1, CT2	نصان مشفران باستخدام ASCON
TAG1, TAG2	وسما تحقق لضمان سلامة الرسائل

جدول 3. تسلسل رسائل المصادقة في البروتوكول المقترح.

المرحلة	الاتجاه	الرسالة / العملية	الهدف الأمني
0	Reader ⟶ Tag	RN0	بدء جلسة جديدة بقيمة تحدي عامة
1	⟶ Tag ⟶ Reader Server	M1 = (CT1, TAG1, RN1)	إرسال هوية البطاقة مشفرة ومحمية بوسم تحقق
2	Server	Dec/Verify M1	التحقق من شرعية البطاقة داخل قاعدة البيانات
3	Server ⟶ Reader Tag ⟶	M2 = (CT2, TAG2, RN2)	إثبات شرعية الخادم وإرسال RN3 بشكل مشفر
4	Tag and Server	= SK KDF(K,RN1,RN2,RN3)	اشتقاق مفتاح جلسة فريد وحديث

2.2 تصميم البروتوكول المقترح

يعتمد البروتوكول على مرحلتين رئيسيتين: مرحلة التسجيل ومرحلة المصادقة. ففي التسجيل، ينشئ الخادم معرّفاً سرياً للبطاقة TID ومفتاحاً مشتركاًK ، ثم يخزّن القيم في قاعدة البيانات ويحمّل البطاقة بالقيم اللازمة. وفي

المصادقة، تتبادل الأطراف رسائل قصيرة تعتمد على أرقام عشوائية وقيم مشفرة. ويعرض جدول (2) الرموز والاختصارات الأساسية المستخدمة في وصف البروتوكول.

1.2.2مرحلة التسجيل

ينشئ الخادم في البداية سجلاً للبطاقة يحتوي على TID وK، و RID أو معلومات الصلاحيات المرتبطة بالمؤسسة الصحية. وتحفظ البطاقة القيم الدنيا اللازمة للتفاعل، بينما يحتفظ الخادم بنسخة حالية وأخرى سابقة من بعض القيم الحساسة، لتسهيل استرداد التزامن عند فشل أي تحديث. وتتم هذه المرحلة في قناة إدارية آمنة قبل تسليم البطاقة للمتقاعد.

2.2.2 مرحلة المصادقة

تبدأ الجلسة عندما يرسل القارئ قيمة RN0 إلى البطاقة، إعلاناً ببداية تفاعل جديد. ولا يُشترط أن تكون RN0 سرية؛ فهي تعمل كقيمة تحدٍّ عامة تربط الجلسة بزمنها الحالي. بعد ذلك تولّد البطاقةRN1 ، وتشتق مفتاحاً مؤقتاً K1 من المفتاح المشترك K والقيمةRN1 ، وفق العلاقة = K1 : KDF(K, RN1). ثم تشفّر الهوية السرية TID باستخدامASCON ، فتنتج CT1وTAG1، وتصبح الرسالة الأولى .M1 = (CT1, TAG1, RN1): ويمرر القارئ هذه الرسالة إلى الخادم دون تعديل.

عند وصولM1 ، يعيد الخادم اشتقاقK1 ، ويفك تشفيرCT1 ، ويتحقق من TAG1، ثم يبحث عن TID في قاعدة البيانات. فإذا نجح التحقق، يولّد الخادم RN2 وRN3، ويشتقK2 = KDF(K, RN2) ، ثم يشفّر RN3 لإنتاج CT2و .TAG2وتصبح الرسالة الثانيةM2 = (CT2, TAG2, RN2) :، وتُرسل إلى البطاقة عبر القارئ. وبعد نجاح التحقق منM2 ، يُشتق مفتاح الجلسة وفق .SK = KDF(K, RN1, RN2, RN3): وبذلك يمتلك الطرفان الشرعيان وحدهما مفتاح جلسة حديثاً لا يُعاد استخدامه. ويلخص جدول (3) اتجاه كل رسالة أو عملية والهدف الأمني المقابل لها.

3.2 التحقق الرسمي والتحليل الأمني

استخدمت الدراسة مسارين للتحقق من أمن البروتوكول المقترح: منطق BAN لتحليل الاعتقادات الأمنية بين البطاقة والخادم، وأداة [16] ProVerif لتحليل السرية ضمن نموذج مهاجم نشط من نوع Dolev-Yao. كما استُخدم منطق [17] BAN لتحليل خصائص المصادقة وحداثة المفاتيح. جُرّد القارئ من التحليل لأنه لا يملك المفاتيح السرية ولا يقرر قبول الهوية، وتم التركيز على الرسالتين الجوهريتين بين البطاقة والخادم. والصياغة المثالية للرسالة الأولى هي: <M1: Tag ⟶ Server: <RN1, {TID}K1>، والصياغة المثالية للرسالة الثانية: <M2: Server ⟶ Tag: <RN2, {RN3}K2>. وبافتراض أن المفتاح المشترك (K) معروف حصراً للبطاقة والخادم، وأن الأرقام العشوائية (RN1, RN2, RN3) هي قيم حديثة، يستنتج الخادم أن البطاقة قد أرسلت الهوية (TID) وتؤمن بها حالياً، بينما تستنتج البطاقة أن الخادم قد أرسل القيمة (RN3) ويؤمن بها حالياً. وكنتيجة نهائية، يستنتج الطرفان الشرعيان حداثة مفتاح الجلسة (SK) وكونه مفتاحاً مشتركاً آمناً."

أما فيProVerif ، فقد نُمذجت القناة العامة بحيث يستطيع المهاجم الاعتراض والتعديل وإعادة الإرسال. وأثبت النموذج سرية المفتاح المشتركK ، وسرية القيمة العشوائية الخاصة بالبطاقة، بينما أظهر أن RN0 قيمة عامة، لأنها تُرسل صراحة من القارئ. وهذه نتيجة منطقية، لأن RN0 لا تُستخدم سراً مشتركاً، بل قيمة تحدٍّ لبداية الجلسة. كما جرى تحليل المصادقة جزئياً عبر الأحداث، مع الحاجة إلى تطوير نموذج لاحق لإثبات المصادقة المحقونة Injective Authentication، وهي نقطة مهمة لبحث موسّع مستقبلاً.

1.3.2 مقاومة الهجمات

- إعادة الإرسال: تتغير RN1 و RN2وRN3في كل جلسة، فلا تنجح الرسائل القديمة، لأنها مرتبطة بمفاتيح مؤقتة مختلفة.
- انتحال الهوية: لا يستطيع المهاجم إنشاء CT1/TAG1 أو CT2/TAG2 صحيحين دون معرفةK ، وهو مفتاح غير معروف للمهاجم في النموذج الرسمي.
- التنصت: تمر الهوية السرية والقيمة RN3 داخل نصوص مشفرة، فلا يستفيد المهاجم من مراقبة القناة.
- الرجل في المنتصف: يؤدي أي تعديل في الرسائل إلى فشل وسمَي التحقق TAG1 أوTAG2 ، ما يمنع قبول الرسائل المعدَّلة.
- فقدان التزامن: يحتفظ الخادم بالقيم الحالية والسابقة، ليستعيد البطاقة تزامنها إذا انقطع الاتصال أثناء التحديث، وهي خاصية مهمة في البيئات الطبية.
- الخصوصية وعدم التتبع: يقلل استخدام معرّفات مشفرة وقيم عشوائية متغيرة قدرة المهاجم على ربط جلسات متعددة بالبطاقة نفسها، لكن إثبات عدم التتبع رسمياً يحتاج إلى نماذج خصوصية إضافية.

4.2 نموذج التهديد و افتراضات الثقة

يُفترض أن قناة الاتصال اللاسلكية بين البطاقة والقارئ، وكذلك القناة بين القارئ والخادم عند غياب طبقة نقل آمنة، قناة عامة يستطيع المهاجم مراقبتها، وحذف بعض رسائلها، وتعديلها، وإعادة إرسال رسائل قديمة، وإدخال رسائل جديدة. كما يُفترض أن المهاجم يستطيع حمل قارئ غير موثوق ومحاولة دفع البطاقة إلى الاستجابة، أو محاولة تقليد بطاقة شرعية أمام قارئ حقيقي. وتتوافق هذه الفرضية مع نموذج Dolev-Yao المستخدم عادة في أدوات التحقق الشكلية، حيث يُعامل التشفير صندوقاً مثالياً لا يمكن كسره إلا بامتلاك المفتاح الصحيح.

في المقابل، يفترض البروتوكول أن مرحلة التسجيل تتم في بيئة إدارية آمنة، وأن المفتاح السري K لا يخرج من البطاقة والخادم بعد التحميل الأولي. ويُفترض أيضاً أن الخادم الخلفي هو الطرف الأكثر موثوقية، لأنه يملك القدرة على حماية قاعدة البيانات، وتحديث السجلات، ومراقبة محاولات الدخول غير الناجحة. أما القارئ فيُعامل وسيطاً محدود الثقة: يمرر الرسائل، لكنه لا يملك القدرة على فك تشفير الهوية أو إنشاء رسائل صالحة دون تعاون الخادم. ويقلل هذا الفصل بين الأدوار أثر اختراق قارئ واحد داخل مؤسسة صحية، لأن سرية البطاقة لا تعتمد على سر مخزَّن في القارئ.

وتجدر الإشارة أيضاً إلى أن النموذج لا يغطي كل أنواع الهجمات الفيزيائية. فإذا استطاع مهاجم فتح البطاقة واستخراج المفتاح من الذاكرة، يصبح أي بروتوكول متماثل يعتمد على مفتاح مشترك معرَّضاً للخطر. لذلك يجب أن يصاحب التطبيق العملي اختيار شرائح مقاومة للعبث، وآلية لإبطال البطاقات المفقودة، وسياسات تحديث دورية للمفاتيح، وربط أحداث المصادقة بسجلات تدقيق داخل الخادم. وبهذا يصبح البروتوكول جزءاً من منظومة أمنية متكاملة، لا بديلاً عن إدارة الهوية والحوكمة الأمنية.

5.2 خوارزمية شبه برمجية مختصرة

لتوضيح خطوات تنفيذ البروتوكول المقترح، يمكن تمثيل آلية المصادقة

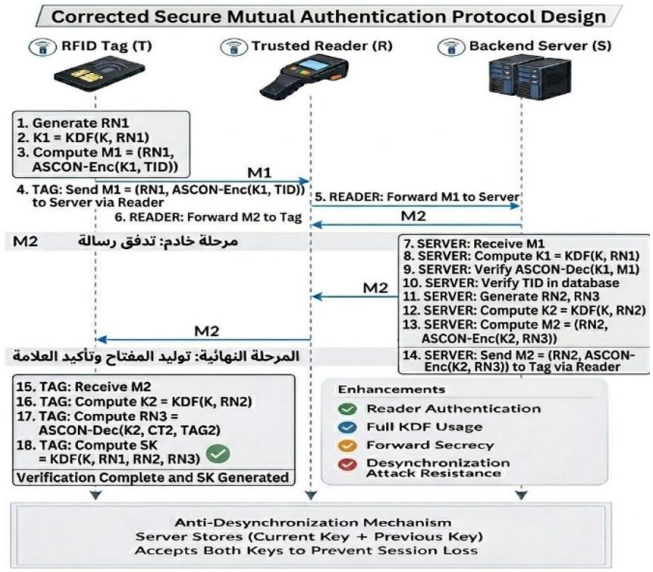
بخوارزمية شبه برمجية مختصرة. في جانب البطاقة، تستقبل البطاقة قيمة RN0، ثم تولّد RN1 وتشتق المفتاح المؤقت *K1* باستخدام المفتاح المشترك *K*. بعد ذلك تُشفّر المعرّف السري TID باستخدام ASCON وتنتج CT1 وTAG1، ثم ترسل الرسالة M1 إلى الخادم عبر القارئ. في جانب الخادم، يستقبل الخادم الرسالةM1، ويعيد اشتقاقK1 ، ويتحقق منTAG1، ثم بعد نجاح التحقق يولّد القيم العشوائية RN2 وRN3، ويشتقK2، ويشفّر RN3 لإنتاج CT2 وTAG2، ثم يرسل الرسالة M2 إلى البطاقة عبر القارئ.

عند استلام M2، تتحقق البطاقة من TAG2 وتستخرج RN3، ثم يشترك كل من البطاقة والخادم في اشتقاق مفتاح الجلسة SK باستخدام K وRN1 وRN2 وRN3. يوضح الشكل (2) التسلسل العام لخطوات الخوارزمية ومراحل إنشاء مفتاح الجلسة.

3. النتائج والمناقشة

1.3 تحليل الأداء والمقارنة

يعتمد تقييم الأداء على تقديرات نظرية. وتفترض الحسابات زمناً مرجعياً لدالة التجزئة الواحدة مقداره 3.25 ميكروثانية، وزمناً لتشفير أو فك تشفير ASCON مقداره 3.8 ميكروثانية، وزمناً لعملية XOR مقداره 0.5



شكل 2. تسلسل رسائل المصادقة في البروتوكول المقترح.

ميكروثانية. ووفق هذا التقدير، يحتاج البروتوكول المقترح إلى عمليتي تجزئة وأربع عمليات ASCON تقريباً، أي: 2 × 3.25 + 4 × 3.8 = 21.7 ميكروثانية. وهذه القيمة أقل من القيم المحسوبة لبروتوكولات مرجعية مثل UDAPوMedIoT-LAPضمن شروط المقارنة نفسها.

أما من حيث التكلفة الاتصالية، فتتكون M1 من CT1 و TAG1وRN1، وحجم كل حقل 128 بت، فيكون حجمها الإجمالي 384 بت. وتتكون M2 من CT2 و TAG2وRN2بالحجم نفسه، فيكون حجمها أيضاً 384 بت. وعليه، تبلغ تكلفة رسالتي المصادقة الأساسيتين M1 وM2 ما مجموعه 768 بت. وعند تضمين قيمة التحدي الاختيارية RN0، ترتفع التكلفة الكلية إلى 896 بت. وتشير هذه الأرقام إلى أن البروتوكول يحافظ على عدد قليل من الرسائل، وحجم بيانات مناسب لبيئات RFID ذات القيود الاتصالية.

جدول 4. ملخص مقارن للأداء والخصائص الأمنية.

البروتوكول	التكلفة الحسابية	التكلفة الاتصالية	ملاحظات أمنية
البروتوكول المقترح	≈ 21.7 µs	768 أو 896 بت	سرية K، مصادقة متبادلة، مقاومة فقدان التزامن
UDAP 2024	≈ 30 µs	≈ 1800 بت	خفيف جداً لكنه أضعف في الخصوصية والتزامن
MedIoT-LAP 2025	≈ 25.9 µs	≈ 2000 بت	قوي أمنياً لكنه لا يوضح استرداد التزامن

2.3 مقارنة تطبيقية بين QR Code وRFID-ASCON

يوضح الجدول التالي الدوافع التطبيقية لاعتماد تقنية RFID في أنظمة بطاقات التأمين الصحي، من خلال مقارنة المتطلبات الأمنية والتشغيلية مع آليات التعريف التقليدية مثل QR Code. ولا تهدف المقارنة إلى اعتبار QR Code غير مناسب لجميع التطبيقات، وإنما إلى توضيح أن بيئة التأمين الصحي، التي تتعامل مع بيانات شخصية وطبية حساسة وتتطلب التحقق من هوية المستخدمين عبر أطراف متعددة، تحتاج إلى خصائص أمنية إضافية تتجاوز القراءة البصرية للرمز. لذلك يوفر استخدام RFID مع بروتوكول مصادقة خفيف إطاراً أكثر ملاءمة لتحقيق المصادقة المتبادلة، وحماية الخصوصية، ودعم متطلبات الأنظمة الصحية محدودة الموارد.

جدول 5. مقارنة تطبيقية مختصرة بين آلية QR Code والنموذج المقترح.

البعد	QR Code التقليدي	RFID + ASCON المقترح
آلية القراءة	تتطلب رؤية مباشرة وتركيز كاميرا	قراءة لاسلكية قصيرة المدى دون رؤية مباشرة
إمكانية النسخ	عالية نسبياً إذا كان الرمز ثابتاً أو مصوَّراً	أقل بكثير بسبب المفاتيح والقيم العشوائية
المصادقة المتبادلة	غالباً غير متوفرة افتراضياً	متوفرة بين البطاقة والخادم عبر القارئ
حماية البيانات	قد تظهر البيانات أو الرابط بصورة مباشرة	تمر الهوية والقيم الحساسة داخل رسائل مشفرة
الخصوصية	يمكن ربط الرمز بصاحب البطاقة بسهولة	تتحسن عبر المعرّفات المشفرة والقيم المتغيرة
الاعتمادية التشغيلية	تتأثر بالخدوش والإضاءة وجودة الطباعة	أقل تأثراً بالعوامل البصرية، مع الحاجة لقارئ مناسب
القابلية للتوسع	مناسبة للتحقق البسيط	مناسبة للتكامل مع قواعد بيانات وسياسات صلاحيات

3.3 المناقشة

توضح النتائج أن قيمة البروتوكول لا تكمن في اختصار عدد الرسائل فقط، إذ تستخدم بعض البروتوكولات المرجعية عدداً مشابهاً من الرسائل. بل تكمن قيمته في الجمع بين معيار تشفير خفيف، واشتقاق مفاتيح مؤقتة، وتحقق شكلي، واسترداد للتزامن. وهذا الجمع مهم في تطبيقات التأمين الصحي، لأن فقدان التزامن قد يعطل بطاقة المتقاعد أو يستلزم إعادة إصدارها. لذلك يمثل نقل عبء الاسترداد إلى الخادم، بدلاً من البطاقة، قراراً تصميمياً مناسباً.

ومع ذلك، يجب التعامل مع النتائج بحذر، لأنها لا تمثل تجربة مختبرية على عتاد RFID فعلي. فالزمن الحقيقي قد يتأثر بنوع الشريحة، وسرعة القارئ، وطول الحزمة، ومعيار الاتصال، وطريقة تنفيذASCON ، واستهلاك الطاقة. كما أن نتائج التحقق باستخدام ProVerif تعكس الخصائص الأمنية ضمن

نموذج رمزي مجرد، ولا يغطي بالضرورة هجمات القناة الجانبية، أو أعطال العتاد، أو هجمات تتبع الخصوصية المعقدة.

4.3 حدود الدراسة

- الدراسة نظرية، ولم تُنفَّذ على بطاقات RFID أو قارئات حقيقية، لذلك تبقى أرقام الأداء تقديرية وليست قياسات ميدانية.
- لم تُجرَ أي تجربة برمجية باستخدام تطبيق مرجعي لخوارزمية ASCON، سواء على حاسوب أو متحكم دقيق، ولذلك تستند تقديرات الزمن والتكلفة بالكامل إلى قيم مرجعية من الأدبيات، لا إلى قياس أولي فعلي.
- ركّز التحقق الرسمي على السرية والمصادقة الأساسية، ولم يقدم إثباتاً كاملاً للمصادقة المحقونة أو عدم قابلية التتبع.
- لم تتناول الدراسة أمن قاعدة البيانات أو سياسات إدارة الصلاحيات داخل المستشفى، لأن التركيز كان على بروتوكول المصادقة.
- لم تُحلَّل هجمات القناة الجانبية، مثل تحليل الطاقة أو التوقيت، وهي مهمة عند الانتقال إلى التطبيق العتادي.

5.3 اعتبارات التطبيق الميداني

عند تحويل النموذج إلى نظام عملي في مؤسسة صحية، لا يكفي تنفيذ الرسائل فقط، بل يجب وضع سياسة تشغيل واضحة. وتبدأ هذه السياسة من مرحلة إصدار البطاقة، حيث تُربط هوية المتقاعد بملف صحي في الخادم، دون تخزين بيانات طبية حساسة داخل البطاقة نفسها. ويُفضَّل أن تحمل البطاقة معرّفاً مستعاراً لا يكشف الاسم أو الرقم الوطني. بعد ذلك، يُخصَّص لكل قارئ معرّف إداري وسجل تدقيق، بحيث يعرف الخادم أي قارئ طلب المصادقة ومتى حدثت العملية. وهذا لا يغيّر جوهر البروتوكول، لكنه يجعل النظام قابلاً للمساءلة عند وجود استخدام غير معتاد.

وعلى مستوى البنية التحتية، يجب حماية القناة بين القارئ والخادم ببروتوكول نقل آمن مثلTLS ، حتى لو كان البروتوكول المقترح يحمي الهوية داخل الرسائل. فالتشفير على مستوى التطبيق وحده لا يمنع هجمات حجب الخدمة، أو التلاعب بسجلات الاتصال، أو انتحال الخادم على مستوى الشبكة. كما يجب أن يخزّن الخادم المفاتيح داخل وحدة آمنة أو قاعدة بيانات مشفرة، وأن يفصل صلاحيات المسؤولين، حتى لا يستطيع موظف واحد استخراج مفاتيح البطاقات أو تعديل سجلات التأمين دون تدقيق.

ومن الناحية التشغيلية، يمكن البدء بتجربة محدودة على عدد صغير من البطاقات والقارئات في عيادة واحدة. وتُقاس خلال التجربة أربعة مؤشرات: زمن المصادقة من لحظة تقريب البطاقة حتى قبولها؛ ومعدل فشل المصادقة الطبيعي؛ واستهلاك الطاقة أو عمر البطاقة إذا كانت نشطة؛ وعدد محاولات الرفض بسبب رسائل قديمة أو غير صحيحة. فإذا أظهرت التجربة أن الزمن مقبول وأن معدل الفشل منخفض، يمكن توسيع النظام تدريجياً، مع تدريب الموظفين والمتقاعدين على طريقة الاستخدام وحماية البطاقة من الفقدان.

6.3 تقييم قابلية التوسع

تعتمد قابلية توسع البروتوكول المقترح على فصل وظائف المصادقة بين بطاقة RFID والقارئ والخادم الخلفي. فلا يحتاج القارئ إلى تخزين مفاتيح خاصة بالبطاقات، مما يقلل متطلبات الإدارة عند إضافة عدد كبير من القارئات أو البطاقات الجديدة. كما تقتصر عملية تسجيل بطاقة جديدة على إنشاء سجل مرتبط بها داخل قاعدة بيانات الخادم وتحميل القيم الأساسية اللازمة إلى البطاقة خلال مرحلة التسجيل الآمن. ومع زيادة عدد البطاقات والمستخدمين ومرافق الرعاية الصحية، يبقى حجم العمليات المطلوبة على البطاقة ثابتاً، لأن البطاقة تنفذ عمليات التشفير الخفيف واشتقاق المفاتيح فقط. في المقابل، يزداد العبء على الخادم نتيجة عمليات البحث وإدارة السجلات، لذلك تعتمد كفاءة النظام على تصميم قاعدة البيانات وآلية الفهرسة المستخدمة. ولتقليل زمن البحث عند توسع النظام، يمكن استخدام معرفات مستعارة مفهرسة (Indexed Pseudonyms) تسمح للخادم بتحديد سجل البطاقة دون الحاجة إلى البحث الشامل في قاعدة البيانات. ويحقق هذا التصميم توازناً بين متطلبات الأمن وقابلية التوسع، حيث يحافظ على خصوصية هوية المستخدم مع دعم زيادة عدد البطاقات ومستخدمي النظام دون تغيير بنية البروتوكول الأساسية.

7.3 الجوانب الأخلاقية وحوكمة البيانات الصحية

ترتبط بطاقات التأمين الصحي ببيانات شديدة الحساسية، لذلك لا ينبغي النظر إلى البروتوكول المقترح بوصفه آلية تقنية مستقلة فقط، بل جزءاً من إطار أخلاقي وإداري يحمي حق المتقاعد في الخصوصية. ويعني ذلك أن تحتوي البطاقة على أقل قدر ممكن من البيانات، ويُفضَّل أن تخزّن معرّفاً مستعاراً فقط، بينما تُحفظ البيانات الطبية والتأمينية في الخادم ضمن ضوابط وصول واضحة. كما ينبغي أن يكون كل طلب مصادقة قابلاً للتدقيق، بحيث يسجل النظام القارئ المستخدم، ووقت العملية، ونتيجة التحقق، دون كشف محتوى طبي غير لازم للموظف الذي أجرى العملية.

وتتطلب الحوكمة أيضاً تحديد سياسات للاحتفاظ بالسجلات وحذفها، ومنح الصلاحيات وفق مبدأ الحاجة إلى المعرفة. فالطبيب قد يحتاج إلى تفاصيل سريرية، بينما يحتاج الصيدلي إلى التحقق من الاستحقاق الدوائي فقط، ويحتاج موظف الاستقبال إلى تأكيد صلاحية البطاقة لا أكثر. ويمكن مستقبلاً ربط البروتوكول بنظام تحكم في الصلاحياتRole-Based Access Control ، بحيث لا تمنح المصادقة حق الوصول المطلق، بل تفتح قناة آمنة تُحدَّد بعدها صلاحيات كل دور داخل المؤسسة الصحية.

ومن المهم أيضاً إعداد آلية استجابة للحوادث. فإذا فقد المتقاعد بطاقته، أو ظهرت محاولات مصادقة متكررة وفاشلة، يجب أن يستطيع الخادم تعليق البطاقة مؤقتاً وإصدار بطاقة بديلة دون تعطيل خدمة المستفيد. كما ينبغي توعية المستخدمين والموظفين بأن الأمان لا يعتمد على الخوارزمية وحدها، بل على إدارة المفاتيح، وحماية القارئات، وتحديث البرمجيات، ومراقبة السجلات. وتجعل هذه الاعتبارات التحول إلى RFID-ASCON مشروعاً مؤسسياً متكاملاً، لا مجرد استبدال رمز QR ببطاقة لاسلكية.

4.الخاتمة والتوصيات

تقدم هذه الدراسة نموذجاً لمصادقة متبادلة خفيفة لأنظمة RFID الصحية باستخدام ASCON، وتعالج مشكلة الاعتماد على QR Code في بطاقات التأمين الصحي للمتقاعدين، وتقترح بروتوكولاً ثلاثي الأطراف يحقق مصادقة متبادلة بين البطاقة والخادم عبر قارئ وسيط، باستخدام أرقام عشوائية، ومفاتيح مؤقتة، ورسائل مشفرة، ومفتاح جلسة فريد لكل عملية مصادقة. وأظهر التحقق الرسمي باستخدام منطق BAN إمكانية إثبات خصائص المصادقة وحداثة مفتاح الجلسة، كما أظهر نموذج ProVerif حماية المفتاح المشترك ضمن نموذج المهاجم الرمزي. وأوضح التحليل الأمني غير الرسمي مقاومة البروتوكول لعدد من الهجمات الشائعة، مع الحفاظ على تكلفة حسابية واتصالية منخفضة تناسب بيئات الأجهزة المقيدة.

وتوصي الدراسة بتنفيذ البروتوكول عملياً على منصة RFID متوافقة مع

ISO 14443، أو منصة مدمجة مثل ARM Cortex-M0/M3، وقياس زمن المصادقة، واستهلاك الطاقة، والمسافة الفعالة. كما توصي بتوسيع نموذج ProVerif لإثبات المصادقة المتبادلة، واستخدام نماذج خصوصية متخصصة لإثبات عدم قابلية التتبع، ودراسة دمج سياسات التحكم في الصلاحيات داخل المؤسسة الصحية. وعلى مستوى التطبيق المحلي، يمكن اعتماد هذه الدراسة كنقطة انطلاق لخارطة طريق تنقل خدمات التأمين الصحي من QR Code إلى RFID مشفر، شرط أن يسبق التعميم اختبار ميداني محدود ومراجعة أمنية مستقلة.

5. قائمة المراجع

[1] Farooq, U., Khan, M. K., & Kumari, S. (2015). A secure RFID authentication protocol for healthcare environments using ECC. Journal of Medical Systems, 39(9), 1-12.

[2] He, D., Zeadally, S., Kumar, N., & Wu, W. (2017). A lightweight mutual authentication scheme for RFID in e-Healthcare. Journal of Ambient Intelligence and Humanized Computing, 8(6), 915-926.

[3] Juels, A. (2006). RFID security and privacy. IEEE Security & Privacy, 4(3), 42-49.

[4] Kumar, S., & Sharma, R. (2020). Security limitations of QR Code systems. International Journal of Information Security, 19(4), 401-410.

[5] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2011). Lightweight cryptography for RFID. Sensors, 11(12), 11471-11502.

[6] Turan, M. S., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2025). Ascon-Based Lightweight Cryptography Standards for Constrained Devices. NIST Special Publication 800-232. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-232.

[7] Ashrif, F. F., Sundararajan, E. A., Ahmad, R., Hasan, M. K., & Yadegaridehkordi, E. (2024). Survey on the authentication and key agreement of 6LoWPAN: Open issues and future directions. Journal of Network and Computer Applications, 221, 103759. https://doi.org/10.1016/j.jnca.2023.103759.

[8] Akiirne, Z., Sghir, A., & Bouzidi, D. (2024). UDAP: Ultra-lightweight dot product-based authentication protocol for RFID systems. Cybersecurity, 7(1), 68. https://doi.org/10.1186/s42400-024-00252-6.

[9] Tanveer, M., & Aldossari, S. A. (2025). MedIoT-LAP: Secure and efficient lightweight AEAD-based authentication protocol for medical IoT. Ain Shams Engineering Journal, 16(10), 103605. https://doi.org/10.1016/j.asej.2025.103605 .

[10] Naik, M. S., Sreekantha, D. K., Sairam, K. V. S. S. S. S., & Nataraju, C. S. (2025). Lightweight mutual authentication protocol for resource-constrained RFID tags with PRINCE cipher. IAES International Journal of Artificial Intelligence, 14(4), 3435–3443. https://doi.org/10.11591/ijai.v14.i4.pp3435-3443.

[11] Merabet, F., Challal, Y., Conchon, E., & Sauveron, D. (2025). Hash-based threshold group RFID authentication protocol for medical IoT applications. 2025 IEEE/ACS 22nd International Conference on Computer Systems and Applications (AICCSA), 1–8. https://doi.org/10.1109/AICCSA66935.2025.11315224.

[12] Ghosh, H., Maurya, P. K., & Bagchi, S. (2025). Authentication protocol for RFID-enabled TMIS: An LCD code-based approach. Peer-to-Peer Networking and Applications, 18(6), 317. https://doi.org/10.1007/s12083-025-02128-z.

[13] Ashrif, F. F., Sundararajan, E. A., Hasan, M. K., Ahmad, R., Hashim, A.-H. A., & Abu Talib, A. (2024). Provably secured and lightweight authenticated encryption protocol in machine-to-machine communication in Industry 4.0. Computer Communications, 218, 263–275. https://doi.org/10.1016/j.comcom.2024.02.008.

[14] Ashrif, F. F., Sundararajan, E. A., Hasan, M. K., Ahmad, R., Abdullah, S., & Wazirali, R. (2024). Secured lightweight authentication for 6LoWPANs in machine-to-machine communications. Computers & Security, 145, 104002. https://doi.org/10.1016/j.cose.2024.104002 .

[15] Ashrif, F. F., Sundararajan, E. A., Hasan, M. K., & Ahmad, R. (2025). A secure and lightweight group mobility authentication scheme for 6LoWPAN networks. Sensors, 25(5), 1458. https://doi.org/10.3390/s25051458.

[16] Blanchet, B. (2016). Modeling and verifying security protocols with the applied pi calculus and ProVerif. Foundations and Trends in Privacy and Security, 1(1–2), 1–135. https://doi.org/10.1561/3300000004.

[17] Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. ACM Transactions on Computer Systems, 8(1), 18–36. https://doi.org/10.1145/77648.77649.