المجلة العلمية لجامعة الملك فيصل
The Scientific Journal of King Faisal University
العلوم الأساسية والتطبيقية
Basic and Applied Sciences

اقتراح نموذج آمن متكامل لنظام الحوسبة السحابية من خلال دراسة نماذج مرجعية

نيروز الزين و زكريا مهروسة و محمود رحال
قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، حلب، سوريا

Proposal for a Secure Integrated Scheme for Cloud Computing Systems

Nairouz Alzin, Zakria Mahrousa and Mahmoud Rahhal
Department of Computer Engineering, Faculty of Electrical & Electronic Engineering, University of Aleppo, Aleppo, Syria

KEYWORDS
الكلمات المفتاحية
AES, Digital Signature, RSA, Security Issue, MD5, Privacy and Security
التوقيع الرقمي، الأمن والخصوصية ، خوارزمية AES، خوارزمية RSA، خوارزمية الاختزال MD5، متطلبات الأمن

RECEIVED الاستقبال	ACCEPTED القبول	PUBLISHED النشر
16/09/2020	18/10/2020	01/12/2020

https://doi.org/10.37575/b/cmp/0030

الملخص

تُعد نماذج التَّوقيع الرقمي من ابرز واهم المتطلبات اللازمة للتعاملات الإلكترونية الموثوقة، وتتسابق الأبحاث فيما بينها للحصول على نموذج يحقق أكبر قدر ممكن من متطلبات الوثوقية والأمان. يقترح هذا البحث نموذجاً آمناً متكاملاً؛ بغية تحقيق متطلبات ومعايير: الوثوقية، والتحقق، والحماية، وخاصيتي التحقق وعدم الإنكار لكل من المرسل والمستقبل في نظام الحوسبة السحابية، كما يتميز النموذج المقترح بخاصية التنفيذ الزمني السريع نسبياً، فضلًا عن أنه يحقق متطلبات أمنية عديدة تتطلب أزمنة إضافية في النماذج المرجعية المبينة في الدراسة المرجعية التي أجريناها لعدة نماذج للتوقيع الرقمي. حيث أثبتت النتائج أنَّ زمن التنفيذ اللازم لإجراء النموذج لا يتجاوز الـ Sec1 في طرف الإرسال وSec4 في طرف الاستقبال، وذلك لأحجام ملفات متغايرة تصل إلى 200 KB وهو حجم كبير نسبياً في الرسائل الموثقة التي قلما تصل إلى هذه الأحجام.

ABSTRACT

Digital signature schemes are thought to be essential requirements for authenticated electronic transactions, and researchers have been working hard to provide a suitable scheme to satisfy the large number of reliability and security requirements. This research proposes a secure integrated scheme that meets authentication, verification, non-repudiation and protection requirements for both the transmitter and the receiver in a cloud computing system. The proposed scheme provides a faster execution time, while satisfying several of the requirements, than in referenced models. The results demonstrate that the execution time of the proposed scheme does not exceed one second on the transmission side and four seconds at the receiving end for various file sizes up to a maximum of 200 kilobytes, a relatively large size for authenticated messages that rarely reach these huge sizes.

1. المقدمة

مازالت الحوسبة السحابية غير معتمدة في بعض المؤسسات والشركات بالرغم من انتشارها الواسع واعتمادها من مؤسسات وشركات أخرى، وغالباً ما يكون السبب الذي تحتج به الشركات والمؤسسات التي لا تعتمد نظام الحوسبة السحابية هو عدم وجود نظام آمن ومتكامل وسريع زمنياً يلبي المتطلبات الأمنية التي تحتاجها الحوسبة السحابية، وقد أُجريت عدة دراسات حول التحديات الأمنية للحوسبة السحابية وتحديد المتطلبات الأمنية لنقل وتخزين البيانات في الحوسبة السحابية؛ لضمان سرية البيانات وسلامتها ووثوقيتها كما في Tabrizchi and Yahya *et al.*, 2019) (Rafsanjani, 2020;.

كما درس الباحثان Khan and Sharma (2019) متطلبات الأمن في الحوسبة السحابية، واقترحا استخدام خوارزميات التشفير المتناظرة وغير المتناظرة لتأمين البيانات، كما أكَّدا أهمية استخدام خوارزمية AES (Advance Encryption Standard) المتناظرة في تشفير البيانات لسرعتها ومرونتها، وقد درس باحثان آخران Kumar and Badal (2019) متطلبات الأمن الأساسية في الحوسبة السحابية، وأكَّدا أهمية تطبيق التشفير الهجين والدمج بين الخوارزميات المتناظرة وغير المتناظرة؛ لتأمين البيانات في الحوسبة السحابية بالآليات المختلفة بالتشفير الهجين والتوقيع الرقمي معاً لتحقيق سرية البيانات وسلامتها ووثوقيتها، واستطاع الباحثون في Miao *et al.* (2019) تقديم حل لتأمين البيانات في نظام الطباعة السحابية من خلال التشفير الهجين، فقد حللوا أوجه القصور في منصة الطباعة السحابية الحالية، وقاموا بتصميم منصة طباعة سحابية آمنة من خلال الدمج بين التشفير الهجين الذي يدمج بين خوارزمية RSA (Rivest Shamir Adleman) وخوارزمية AES والتوقيع الرقمي باستخدام خوارزمية الاختزال SHA1، حيث تتم عملية التوقيع الرقمي والتشفير للملف المطلوب في طرف الإرسال، وفي طرف الاستقبال تتم عملية فك التشفير والمطابقة للتحقق من وثوقية الملف المرسل، وبالتالي، استطاع النموذج المُقدَّم تزويد المستخدمين بخدمات طباعة موثوقة، إلا أنه لم يحقق جميع المتطلبات الأمنية للحوسبة السحابية.

واتجه باحثون آخرون في Iwasokun *et al.* (2019) إلى اقتراح حل يضمن سلامة البيانات المالية، كـ: سلامة بطاقات الائتمان الحساسة، وسلامة البيانات المالية الأخرى عند نقلها عبر الحوسبة السحابية، واستخدموا خوارزمية الاختزال MD5 (Message Digest 5) مع خوارزمية RSA بمفتاحيها العام والخاص، حيث يقوم المرسل بتوقيع الرسالة بالمفتاح الخاص للمرسل في طرف الإرسال، بينما يقوم المستقبل في طرف الاستقبال بفك تشفير التوقيع الرقمي بالمفتاح العام للمرسل، وحققت الطريقة المقترحة مستوى عالياً لخصوصية البيانات وسلامتها عند نقلها عبر الحوسبة السحابية مقارنة مع طرق مقترحة في أبحاث أخرى، إلا أنها لم تحقق المتطلبات الأمنية كافة للحوسبة السحابية، ودمج باحثان آخران Sadikin and Wardhani (2016) بين التشفير والتوقيع الرقمي لتحقيق وثوقية البيانات وسلامتها والتحقق وعدم الإنكار في نظام إلكتروني لتسجيل البيانات الصحية، وذلك لمنع حدوث مشاكل: السرقة، أو التعديل، أو العمليات غير الموثوقة الأخرى، وقد اقترحا مخططين:

أحدهما للحماية لمنع العبث الخارجي أو الاطلاع على البيانات، وذلك بتشفير بيانات المرضى بخوارزمية AES المتناظرة.

والمخطط الآخر للتحقق من الوثوقية من خلال التوقيع الرقمي بتشفير خلاصة الرسالة بالمفتاح الخاص لخوارزمية RSA غير المتناظرة، وللحصول على خلاصة الرسالة استخدموا خوارزمية SHA256، وقد حقق تطبيق كل من التشفير والتوقيع الرقمي حماية سرية لبيانات المرضى من السرقة أو العبث، كما حقق وثوقية البيانات وسلامتها، بينما اقترح باحثون آخرون Harini *et al.* (2017) نموذجاً يجمع بين التوقيع الرقمي لتوثيق الرسالة والتشفير لتأمين سرية البيانات، واستخدموا خوارزمية الاختزال MD5 للحصول على خلاصة الرسالة، وخوارزمية AES المتناظرة لتأمين سرية البيانات، وخوارزمية RSA غير المتناظرة للتوقيع الرقمي بمفتاحيها العام والخاص، ووجدوا أنَّ نموذجهم المقترح يحقق وثوقية وسرية البيانات وسلامتها، وقد قمنا باستعراض نموذجهم المقترح ودراسة المتطلبات الأمنية التي يحققها في بحثنا.

أما في Fauzan and Paulus (2018)، فقد اقترح الباحثان نموذجاً آمناً متكاملاً يحقق السرية والوثوقية للبيانات من خلال تطبيق التشفير باستخدام خوارزمية AES لتأمين سرية البيانات، والتوقيع الرقمي للتحقق من الوثوقية، حيث يتم تشفير الملف باستخدام خوارزمية AES، أما التوقيع الرقمي، فيتم باستخدام المفتاح العام للمرسل، وذلك بعد تطبيق خوارزمية الاختزال SHA256 على الملف المرسل، وفي طرف الاستقبال يتم فك التشفير للرسالة باستخدام خوارزمية AES مع التحقق من الوثوقية بالمفتاح

Corresponding Author: Nairouz Alzin nairouzalzin@gmail.com, 00963944926555 المؤلف المراسل: نيروز الزين

الخاص للمرسل، واستنتجوا أنَّ الحل المقترح يمثل نموذجاً آمناً متكاملاً لتأمين البيانات، ولكن لا يحقق متطلبات الأمن كافة في الحوسبة السحابية.

كما استطاع باحثان آخران K and Vinod (2018) تحقيق خاصية عدم الإنكار من المرسل باقتراحهما نموذجاً هجيناً يجمع بين التشفير الهجين لتأمين سرية البيانات بخوارزمية AES مع التوقيع الرقمي الذي يؤمن الوثوقية والتحقق من هوية والمرسل بخوارزمية RSA، وذلك من خلال التوقيع بالمفتاح الخاص للمرسل في جهة الإرسال، أما في جهة الاستقبال، فيتم فك التوقيع بالمفتاح العام للمرسل، مما يحقق عدم الإنكار من جهة المرسل، وقد حقق النموذج المقترح سرية البيانات، فضلاً عن: وثوقيتها، وسلامتها، وعدم الإنكار من جهة المرسل، واتجه الباحث في Adeshina (2020) إلى اقتراح نموذج للتوقيع الرقمي يجمع بين خوارزميتين من أشهر خوارزميات التوقيع الرقمي، وهما: خوارزميتي RSA وElliptic Curve El-Gamal، وقد قام الباحث بالمقارنة بين الخوارزميتين، ووجد أنَّ خوارزمية Elliptic Curve El-Gamal تستغرق زمناً أقل فقط في توليد المفاتيح بالمقارنة مع خوارزمية RSA التي تعد أبطء نسبياً في توليد المفاتيح، ولكن أكَّد أنَّ استخدام خوارزمية RSA أفضل؛ لكونها أكثر أماناً وأسرع من خوارزمية Elliptic Curve El-Gamal في عمليتي التوقيع والتحقق؛ لأنَّ التوقيع للملفات الموثقة يتم مرة واحدة فقط في الغالب، بينما التحقق يتكرر مرات عدة، وقد قمنا بمقارنة زمن التنفيذ مع نموذجنا المقترح في بحثنا، ويمكن أن نلخص جهود الباحثين السابقة في سعيهم إلى إيجاد نموذج يحقق أغلب أو جميع متطلبات الأمن في الحوسبة السحابية، سواء أكان باستخدام الخوارزميات المتناظرة أم غير المتناظرة أم باستخدام التوقيع الرقمي أم الدمج فيما بينها، ذلك يتم من خلال اقتراح نماذج لدمجهم؛ بغية تحقيق متطلبات الحوسبة السحابية بأقل زمن تنفيذ ممكن.

يهدف هذا البحث إلى اقتراح نموذج آمن ومتكامل يلبي المتطلبات الأمنية لمستخدمي الحوسبة السحابية، فيضمن هذا النموذج عدم الاطلاع الداخلي (مستخدمي الحوسبة السحابية غير المتراسلين)، كما يضمن عدم الاطلاع الخارجي (مستخدم من خارج الحوسبة السحابية)، ويؤمّن هذا النموذج توثيق الرسالة بتوقيع رقمي من المرسل، كما يؤمّن حماية الرسالة من العبث الداخلي أو الخارجي، ويؤمّن للمرسل التحقق من وصول الرسالة للمُستقبِل، وخاصية عدم الإنكار من قِبل المُستقبِل، كما يؤمن للمُستقبِل وصول الرسالة موثقة من قبل المُرسِل مع إمكانية التَّحقق من هويته وعدم إنكار المرسل أنه قام بإرسالها، ويؤمّن هذا النموذج إجراء المتطلبات السابقة كافة بزمن قياسي نسبياً، وبالتالي، هدف البحث الأساسي الوصول إلى هذا النموذج بأقل زمن تنفيذ ممكن، وذلك من خلال دراسة عدة نماذج موجودة سابقاً أو مقترحة في هذا البحث.

2. المواد وطرق العمل

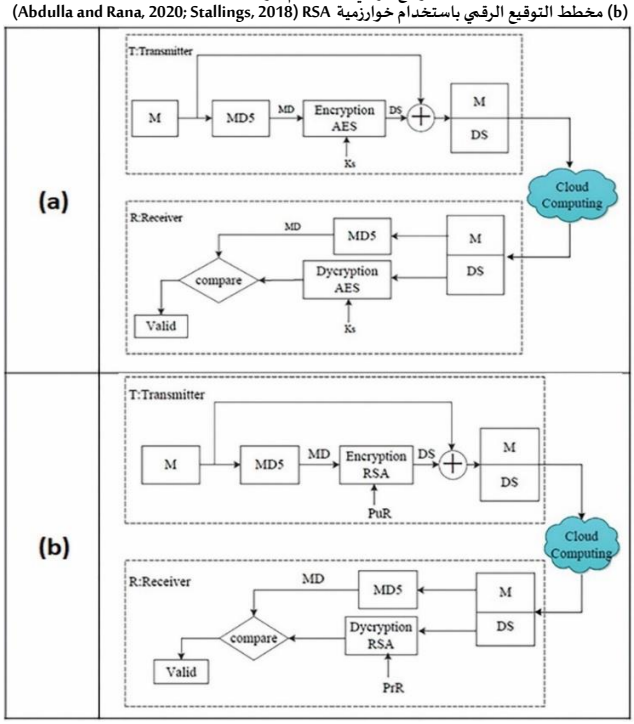
قمنا بدراسة عدة نماذج مرجعية ومقترحة للتوقيع الرقمي، ومناقشة هذه النماذج وفق المواصفات والمزايا التي تؤمنها بغية اقتراح نموذج آمن ومتكامل للتوقيع الرقمي في نظام الحوسبة السحابية، حيث تمَّت مناقشة عدم الاطلاع على الرسالة سواء أكان الاطلاع داخلياً أم خارجياً، وحماية الرسالة من العبث الداخلي والخارجي، ويقصد بالداخلي: عندما يقوم أحد مستخدمي الحوسبة السحابية بالاطلاع أو العبث برسالة لمستخدمَيْنِ آخريْن يقومان بالتراسل، كما تمَّت مناقشة توثيق الرسالة بحدِّ ذاتها هل هي موثقة أم لا؟ وذلك بصرف النظر عمن يقوم بتوثيقها، كما تمَّت مناقشة إمكانية معرفة الموثق (المرسل)، ومناقشة خاصيتي التحقق وعدم الإنكار لكل من: المُرسِل، والمُستقبِل.

بِعَدِّ المدخلات الآتية:

- T: Transmitter المرسل.
- R: Receiver المستقبل.
- M: Message الرسالة المطلوب حمايتها (النص الصريح).
- Ks: المفتاح السري لخوارزمية AES (Panjwani *et al.*, 2020; Mohan *et al.*, 2020).
- Pu = (e, n) : المفتاح العام لخوارزمية RSA (Al-Kaabi and Belhaouari, 2019; Parthasarathy *et al.*, 2019).
- Pr = (d, n): المفتاح الخاص لخوارزمية RSA (Al-Kaabi and Belhaouari, 2019; Parthasarathy *et al.*, 2019).
- PuT، PrT المفتاحان العام والخاص للمرسل بخوارزمية RSA.
- PuR، PrR المفتاحان العام والخاص للمستقبل بخوارزمية RSA.
- MD: Message Digest خلاصة الرسالة (Khatri and Agarwal, 2020; Kareem and Rahma, 2019).
- DS: Digital Signature التوقيع الرقمي.
- C: Cipher text النص المشفر.
- CC: Complex Cipher text النص المشفر المعقد.

يبين الشكل 1(a) مخططاً مرجعياً لإجراء التوقيع الرقمي باستخدام الخوارزمية المتناظرة AES مع خوارزمية الاختزال MD5، حيث يتم اختزال الرسالة بوساطة هذه الخوارزمية؛ للحصول على خلاصتها (MD) بعد تشفير الخلاصة نحصل على (DS) التوقيع الرقمي، فتتم إضافته إلى الرسالة (M)؛ لنحصل على رسالة موثقة تُرسَل عبر الحوسبة السحابية، ثم في طرف المستقبل يتم: فصل الرسالة عن التوقيع، وإيجاد خلاصة الرسالة (MD)، وفك تشفير التوقيع الرقمي، ومقارنة خلاصة الرسالة الناتجة عن خوارزمية الاختزال MD5 مع خلاصة الرسالة الناتجة عن فك تشفير التوقيع الرقمي، ويتم التحقق عن طريق المطابقة.

الشكل (1): (a) مخطط التوقيع الرقمي باستخدام خوارزمية AES (Khakim *et al.*, 2020)
(b) مخطط التوقيع الرقمي باستخدام خوارزمية RSA (Abdulla and Rana, 2020; Stallings, 2018)



يؤمّن المخطط السابق المبين بالشكل 1(a) إمكانية توثيق الرسالة وحمايتها من العبث الخارجي لعدم امتلاك المفتاح السري (Ks) إلا لمستخدمي الحوسبة السحابية، لكن يمكن الاطلاع على الرسالة داخلياً وخارجياً، ويمكن العبث بها من أحد مستخدمي الحوسبة السحابية، ولا يمكن التحقق من هوية المرسل أو التحقق من وصولها إلى المستقبل، ويمكن لكليهما الإنكار، كما لا يمكن معرفة موثق الرسالة (T) المرسل، لذلك تتم عادة إجراء التوقيع الرقمي باستخدام خوارزمية غير متناظرة، كما هو مبين بالشكل 1(b) الذي يوضح إجراء التوقيع الرقمي بالآلية ذاتها التي يقوم بها النموذج الموضح بالشكل 1(a)، لكن يتم تشفير (MD) باستخدام المفتاح العام للمستقبل PuR، وبالتالي، يكون فك تشفير (DS) بالمفتاح الخاص للمستقبل PrR.

حيث يؤمّن المخطط المبين بالشكل 1(b) فضلاً عن خاصية توثيق الرسالة والحماية من العبث الخارجي التي يؤمّنها المخطط المبين بالشكل 1(a)، خاصية عدم العبث الداخلي والتحقق من وصول الرسالة إلى المستقبل الذي لا يمكن له إنكار ذلك؛ لعدم وجود المفتاح الخاص إلا لديه، لكن تبقى

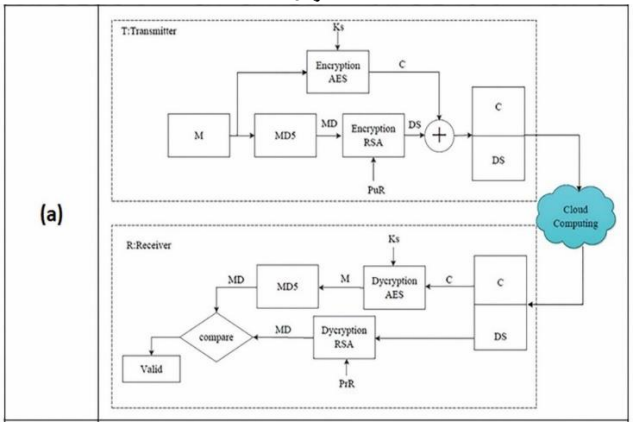
الرسالة عرضة للاطلاع من قِبل مستخدمي الحوسبة السحابية، ولا يمكن التحقق من هوية المرسل، ويمكن للمرسل إنكار أنه قام بإرسال الرسالة لعدم معرفة مُوثِّق الرسالة.

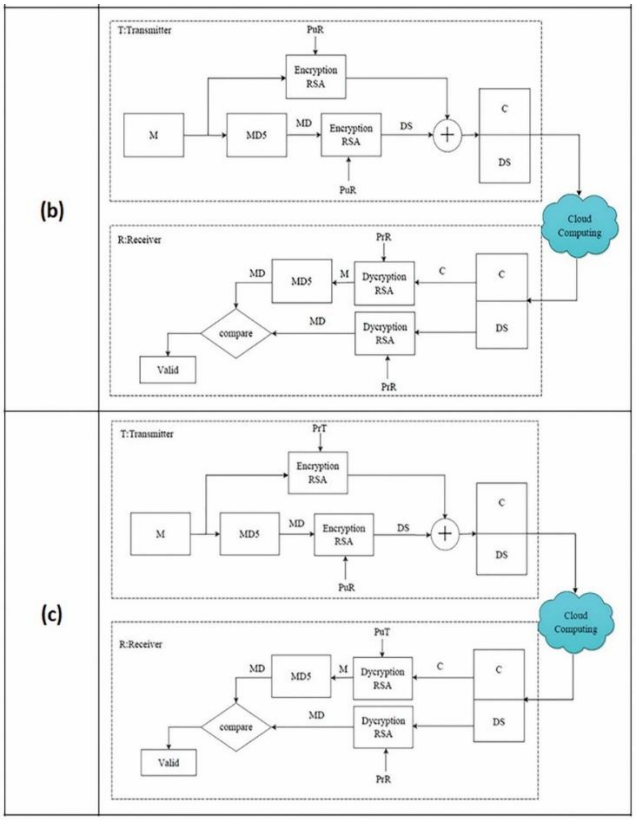
يمكن تلافي إمكانية الاطلاع على الرسالة من قِبل غير مستخدمي الحوسبة السحابية بإجراء عملية تشفير للرسالة باستخدام خوارزمية AES، كما هو مبين بالشكل 2(a)، وهو يطابق في عمله مبدأ عمل النموذج المبين بالشكل 1(b)، إلا أنه يقوم بتشفير الرسالة ودمج الشيفرة الناتجة (C) مع التوقيع الرقمي (DS).

حيث يؤمّن النموذج المبين بالشكل 2(a) خاصية عدم الاطلاع على الرسالة من قِبل غير مستخدمي الحوسبة السحابية، فضلاً عن الخصائص التي يؤمّنها النموذج المبين بالشكل 1(b)، إلا أنَّ الرسالة تبقى عُرضة للاطلاع من قِبل جميع مستخدمي الحوسبة السحابية لامتلاكهم المفتاح السري، ولا يؤمن النموذج السابق خصوصية بين المستخدمين المتراسلين، ويمكن تلافي هذ السلبية بتشفير الرسالة باستخدام خوارزمية غير متناظرة، حيث يتم تشفير الرسالة بالمفتاح العام للمستقبل PuR عند طرف الإرسال؛ ليتم فك تشفيرها بالمفتاح الخاص PrR عند طرف الاستقبال، كما هو مبين بالشكل 2(b) الذي يؤمّن أغلب متطلبات الحوسبة السحابية، إلا أنه لا يؤمّن إمكانية التحقق من هوية المرسل T، وبالتالي، عدم معرفة المُوثِّق، ومنه يمكن لمُرسل الرِّسالة إنكار أنه قام بإرسالها، حيث يمكن لأي مستخدم في الحوسبة السَّحابية إرسال مثل هذه الرسالة إلى المستقبل R؛ لامتلاك جميع مستخدمي الحوسبة السحابية المفتاح العام للمستقبل.

يمكن تحقيق الخاصيات الثلاث السابقة: (التوثيق، والتحقق، وعدم الإنكار للمرسل) باستخدام مفتاح التشفير الخاص للمرسل بدلاً من المفتاح العام للمستقبل، واستخدام المفتاح العام للمرسل لفك التشفير بدلاً من المفتاح الخاص للمستقبل، كما هو مبين بالشكل 2(c)، إلا أنه يُفقد النموذج خاصية عدم الاطلاع الداخلي على الرسالة؛ وذلك لأنَّ عملية فك تشفير الرسالة تتم باستخدام المفتاح العام للمرسل حصراً، مما يتيح للمستقبل التحقق من هوية المرسل ومعرفة المُوثِّق الذي لا يمكن له إنكار أنه قام بإرسال هذه الرسالة، لكن بما أنَّ المفتاح العام للمُرسِل موجود لدى جميع مستخدمي الحوسبة السحابية، فيمكن لهم الاطلاع على الرسالة.

الشكل (2): (a) نموذج توقيع رقمي آمن لنظام الحوسبة السحابية (Harini *et al.*, 2017).
(b) نموذج توقيع رقمي آمن لنظام الحوسبة السحابية يؤمّن خاصية عدم الاطلاع على الرسالة
(c) نموذج توقيع رقمي آمن لنظام الحوسبة السحابية يؤمّن: خواص التوثيق، والتحقق، وعدم الإنكار للمرسل

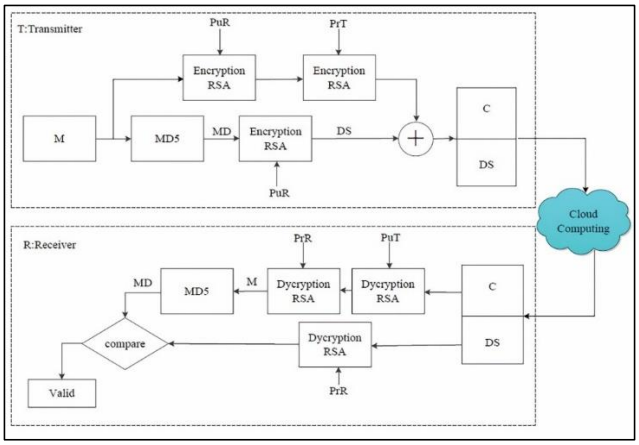




يمكن الحصول على نموذج توقيع رقمي آمن ومتكامل يؤمّن جميع المواصفات والمزايا العشر المطلوبة، وذلك من خلال إجراء عمليتي تشفير للرسالة: مرة باستخدام المفتاح العام للمُستقبِل، ومرة باستخدام المفتاح الخاص للمُرسِل، كما هو مبين بالشكل (3)، الذي يبين نموذج توقيع رقمي آمن ومتكامل، فهو يؤمّن عدم الاطلاع على الرسالة أو العبث بها داخلياً أو خارجياً مع توثيقها، وبما أنَّ تشفير الرسالة يتم بالمفتاح العام للمُستقبِل، ومنه لا يمكن الاطلاع على مضمونها إلا من قبله لامتلاكه هو فقط المفتاح الخاص، كما يؤمّن النموذج المبين بالشكل (3) التحقق من وصول الرسالة إلى المُستقبِل R، ويؤمّن خاصية عدم الإنكار من قِبل المستخدم R.

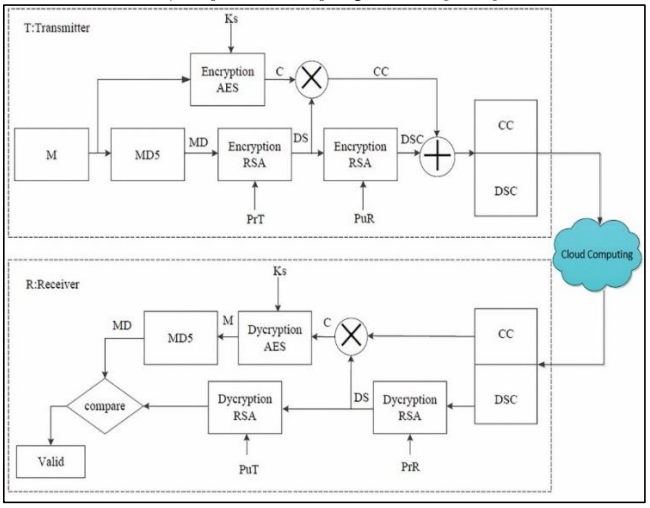
كما أنَّ تشفير الرِّسالة يتم بالمفتاح الخاص للمُرسِل، مما يتطلب بالضرورة استخدام المفتاح العام للمُرسِل عند إجراء فك التَّشفير في طرف المُستقبِل، مما يتيح للمُستقبِل معرفة مُوثِّق الرِّسالة، وبالتالي، التحقق من هوية المرسل T، ولا يمكن للمُرسِل إنكار أنَّه قام بإرسال هذه الرِّسالة لعدم امتلاك المفتاح الخاص للمُرسِل T إلا من قِبله.

الشكل (3): نموذج توقيع رقمي آمن لنظام الحوسبة السَّحابية يؤمّن خواص التَّوثيق والتَّحقق وعدم الإنكار للمُرسل



إنَّ النَّموذج المبين بالشكل (3) هو نموذج آمن مُتكامل من حيث المواصفات والمزايا، إلا أنَّه يتطلب زمناً كبيراً نسبياً، وبالأخص لأنَّ الرسالة M يتم تشفيرها مرتين باستخدام خوارزمية RSA البطيئة نسبياً بالمقارنة مع خوارزمية AES، لذلك بغية تلافي هذا العيب تمَّ اقتراح نموذج آمن ومتكامل يؤمن جميع المواصفات والخواص العشر المطلوبة منه بزمن قياسي نسبياً، كما هو مبين بالشكل (4)، حيث يتم في هذا المخطط تشفير الـ MD مرتين باستخدام خوارزمية RSA بدلاً من تشفير الرسالة، حيث إنَّ خلاصة الرسالة تكون أصغر حجماً بكثير من الرسالة M، بينما يتم تشفير الرسالة باستخدام خوارزمية AES السريعة نسبياً لتأمين حماية الرّسالة والحصول على الشيفرة (C)، ثم يتم إجراء عملية (XOR) بين الشيفرة (C) والتوقيع الرقمي (DS) الناتج عن خلاصة الرسالة (MD) باستخدام خوارزمية RSA والمفتاح الخاص للمرسل PrT، فنحصل على الشيفرة المعقدة نسبياً (Complex C)، ويتم تشفير التوقيع الرقمي (DS) بالمفتاح العام للمستقبل PuR لنحصل على التوقيع الرقمي المعقد نسبياً ((DS(C))، ثم دمج (CC) مع DS(C) وإرسال الناتج عبر الحوسبة السحابية.

الشكل (4): النموذج المُقترح لإجراء توقيع رقمي آمن ومتكامل في نظام الحوسبة السحابية



إنَّ النموذج السابق المبين بالشكل (4) لا يقوم بإرسال شيفرة الرسالة (C)، إنَّما الشيفرة الناتجة عنها (CC)، ولا يقوم بإرسال التوقيع الرقمي مباشرة، بل يقوم بإرسال التوقيع الرقمي المعقد ((DS (C) الذي يتم الحصول عليه من تشفير التَّوقيع الرقمي (DS) بالمفتاح العام للمستقبل PuR، مما يضمن عدم إمكانية الحصول على (DS) إلا من قِبل المُستقبل، لأنَّه هو الوحيد الذي يمتلك المفتاح الخاص PrR، ومنه عدم إمكانية الحصول على (C) إلا من قبله، مما يتيح للنموذج حماية أعلى مع عدم إمكانية الاطلاع على الرسالة أو العبث بها داخلياً أو خارجياً، ويؤمّن التحقق من وصولها إلى المستقبل R حصراً الذي لا يمكنه إنكار؛ ذلك لأنه لا يمكن الاطلاع على هذه الرسالة إلا من قبله، كما يؤمن النموذج المقترح توثيق الرسالة من قِبل المرسلT، وذلك لتشفير الMD بالمفتاح الخاص له، مما يتيح للمستقبل التحقق من هوية المرسل، وذلك عند إجراء فك التشفير بالمفتاح العام للمرسل PuT الذي لا يمكن له إنكار أنه قام بإرسال هذه الرسالة.

3. النتائج والمناقشة

إنَّ نتائج البحث تتعلق بالمزايا والمواصفات التي يحققها نموذج التوقيع الرقمي المُقتَرح مقارنة مع النَّماذج المدروسة؛ بغية تحقيق التَّكاملية في الأداء، ثمَّ مناقشة النَّتائج بالاعتماد على عشرة معايير (مواصفات ومزايا) تعد أسس متطلبات الحوسبة السَّحابية لتحقيق الأمن والتكاملية (Khan and Sharma, 2019; Kumar and Badal, 2019; Tabrizchi and Rafsanjani, 2020; Yahya *et al.*, 2019) وهذه المعايير هي:

- عدم الاطِّلاع الداخلي على الرسالة: ويُقصد به عدم إمكانية الاطِّلاع الدَّاخلي على الرِّسالة لأي مستخدم إلا من قِبل المستخدمين المتراسلين في الحوسبة السحابية.
- عدم الاطِّلاع الخارجي على الرِّسالة: ويُقصد به عدم إمكانية أي مُستخدم من خارج الحوسبة السَّحابية الأطلاع على أي رسالة في الحوسبة السحابية.
- توثيق الرسالة إمكانية الحصول على آلية تجعل الرسالة مُوثَّقة (موقعة إلكترونياً) مع عدم معرفة الموثق.
- حماية مضمون الرسالة من العبث الداخلي.
- حماية مضمون الرسالة من العبث الخارجي.
- توثيق الرسالة من قِبل المُرسِل T ومعرفة هويته.
- التَّحقق من هوية المرسلT.
- خاصية عدم إنكار المُرسِلT أنه قام بإرسال الرِّسالة.
- التَّحقق من وصول الرِّسالة حصراً إلى المستقبل R.
- خاصية عدم إنكار المستقبل R أنه استقبل الرسالة.

يبين الجدول (1) مقارنة المعايير والمواصفات التي تحققها النماذج المقترحة والنماذج المرجعية المدروسة.

جدول (1): مقارنة متطلبات الأمن في الحوسبة السحابية (المعايير والمواصفات) بين النماذج المقترحة والنماذج المرجعية المدروسة

النماذج المقترحة والنماذج المرجعية المدروسة	الشكل(1)		الشكل(2)			الشكل (3)	الشكل (4)
متطلبات الأمن في الحوسبة السحابية (المعايير والواصفات)	الشكل 1(a)	الشكل 1(b)	الشكل 2(a)	الشكل 2(b)	الشكل 2(c)		
الاطلاع على الرسالة داخلي	×	×	×	√	×	√	√
الاطلاع على الرسالة خارجي	×	×	√	√	√	√	√
توثيق الرسالة (مع عدم معرفة الموثق)	√	√	√	√	√	√	√
الحماية من العبث الداخلي	√	√	√	√	×	√	√
الحماية من العبث الخارجي	×	√	√	√	√	√	√
توثيق من قبل T	×	×	×	×	√	√	√
توثيق من هوية T	×	×	×	×	√	√	√
عدم الإنكارT	×	×	×	×	√	√	√
تحقق من وصولها إلى R	×	√	√	√	√	√	√
عدم الإنكارR	×	√	√	√	√	√	√

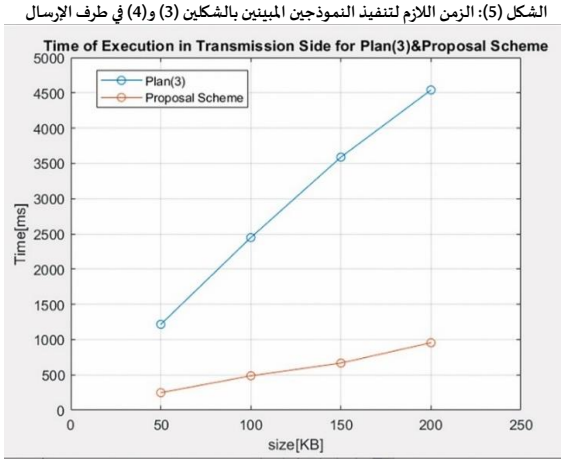
تمَّت دراسة أزمنة التنفيذ للنموذجين الموضحين في الشكلين (3) و(4)؛ لأنهما يحققان متطلبات الأمن اللازمة للحوسبة السحابية بشكل كامل، حيث يبين الجدول (2) أزمنة التنفيذ للنموذجين السابقين عند طرفي الإرسال والاستقبال لملفاتٍ بأحجام مختلفة.

جدول (2): مقارنة أزمنة التنفيذ للنماذج المقترحة للتوقيع الرقمي في طرفي الإرسال والاستقبال

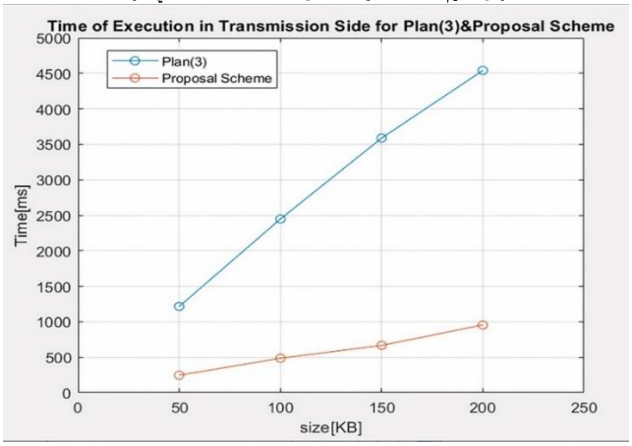
حجم الملف (KB)	الزمن اللازم للتنفيذ عند المرسل [ms]		الزمن اللازم للتنفيذ عند المستقبل [s]	
	النموذج المقترح بالشكل (3)	النموذج المقترح بالشكل (4)	النموذج المقترح بالشكل (3)	النموذج المقترح بالشكل (4)
50KB	1216ms	247.2ms	4.632s	0.9432s
100KB	2448ms	486.4ms	8.8s	1.806s
150KB	3587ms	667.4ms	14.17s	2.647s
200KB	4540ms	955.6ms	18.05s	3.575s

كما يبين الشكلين (5) و(6) المنحنيات البيانية لأزمنة التنفيذ في طرفي الإرسال والاستقبال على الترتيب لكل من النموذجين في الشكلين (3) و(4).

الشكل (5): الزمن اللازم لتنفيذ النموذجين المبينين بالشكلين (3) و(4) في طرف الإرسال



الشكل (6) الزمن اللازم لتنفيذ النموذجين المبينين بالشكلين (3) و(4) في طرف الاستقبال



يتميز النموذج المقترح المبين بالشكل (4) بزمن تنفيذ أقل بكثير من النموذج المبين بالشكل (3)، ويرجع السبب إلى أنَّ النموذج المبين بالشكل (4) يُشفِّر الرِّسالة مرتين: مرة باستخدام خوارزمية AES، ومرة باستخدام المعامل XOR، بينما يُشفِّر النموذج المبين بالشكل (3) الرسالة باستخدام خوارزمية RSA مرتين، وبما أنَّ كل من AES وXOR تحتاجان إلى زمنٍ أقل بكثير من الزمن اللازم لتنفيذ RSA مرة ثانية، مما يفسر تفوق النموذج المُقترح المبين بالشكل (4) على النموذج المبين بالشكل (3) من جهة زمن التنفيذ، أما وجود خوارزمية RSA مرتين في النموذج المقترح، فهو لتشفير الـ128bit فقط، وليس لتشفير الرسالة كاملة، مما يختزل زمن التنفيذ، وبما أنَّ النموذج المقترح في الشكل (4) هو الذي يتفوق زمنياً على النموذج المُبيَّن في الشكل (3)، تمَّت مقارنة هذا النموذج مع نموذج مرجعي Adeshina. (2020) من جهة زمن التنفيذ.

يبيّن الجدول (3) مقارنة زمن التنفيذ ككل في طرف المرسل والمستقبل للنموذج المُقترح في الشكل (4) والنموذج المرجعي (Adeshina. 2020) الذي يتضمن: أزمنة توليد المفاتيح، والتوقيع، والتحقق بدون أزمنة التشفير، وفك التشفير.

جدول (3): مقارنة زمن التنفيذ الناتج عن زمن توليد المفاتيح وزمن التوقيع والتحقق في النموذج المقترح والنموذج المرجعي (Adeshina. 2020).

حجم الملف (KB)	زمن التنفيذ للنموذج المقترح	زمن التنفيذ للنموذج المرجعي (Adeshina. 2020)
50KB	120ms	1693ms
150KB	230ms	1773ms
200KB	420ms	1748ms

يرجع السبب في تفوق النموذج المقترح إلى استخدام خوارزمية RSA ذاتها مرتين؛ لإجراء التوقيع الرقمي والتحقق، الأمر الذي يتطلب توليد مفاتيحها مرة واحدة فقط، بينما يحتاج النموذج المرجعي إلى زمن إضافي لتوليد مفاتيح خوارزمية Elliptic Curve El-Gamal، أي: إنَّ استخدام النَّموذج المرجعي خوارزميتي RSA وElliptic Curve El-Gamal لإجراء التوقيع الرقمي يتطلب أزمنة تنفيذ إضافية ناتجة عن توليد المفاتيح اللازمة لخوارزمية Elliptic Curve El-Gamal، فضلاً عن الأزمنة اللازمة لتوليد مفاتيح RSA.

4. الخاتمة

تمَّ في هذا البحث اقتراح نموذج جديد لإجراء التوقيع الرقمي في الحوسبة السحابية يحقق متطلبات الأمن والتكامل كافة في الحوسبة السحابية من جهة التوثيق والتحقق وعدم الإنكار من قِبل المُرسِل والمُستقبِل، فضلاً عن حماية البيانات بأقل زمن تنفيذ ممكن، حيث تفوَّق النموذج المقترح على النماذج المرجعية المدروسة في البحث، من جهة المتطلبات وزمن التنفيذ، كما بينت ذلك المقارنة المجراة في هذا البحث، مما يجعل استخدام هذا النموذج مطلباً أساسياً في الحوسبة السحابية لجعلها أكثر أماناً ووثوقية.

نبذة عن المؤلفين

نيروز الزين

قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا، nairouzalzin@gmail.com, 00963944926555

طالبة دراسات عليا (دكتوراه): قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا،عضو هيئة فنية (تدريس في جامعة حلب) - (مدير أعمال في جامعة حلب)، حاصلة على ماجستير في هندسة الحاسبات من جامعة حلب، سوريا، نشر العديد من الأبحاث في مجال التحكم بالازدحام وجودة الخدمة وفي مجال أمن المعلومات في الحوسبة السحابية-مديرة مركز المعلوماتية الطبي في جامعة حلب حالياً.

زكريا مهروسة

قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا، dr_z_mahrousa@doctor.com, 00963932338637

الدكتور المشرف: قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا، أستاذ مساعد في قسم هندسة الحواسيب، رئيس قسم هندسة الحواسيب سابقاً، مشرف على مخبر البرمجة، مشرف على مخبر النظم المنطقية، خريج جامعة كارديف – مدرسة الهندسة، نشر العديد من الأبحاث في مجال الذكاء الصنعي وأمن المعلومات والحوسبة السحابية.

محمود محمد رحال

قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا، mrahhal2000@hotmail.com

الدكتور مساعد المشرف: قسم هندسة الحواسيب، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب، سوريا، عضو هيئة تدريسية في جامعة حلب، رئيس قسم هندسة نظم الشبكات والحواسيب في كلية الهندسة المعلوماتية، رئيس قسم هندسة الحواسيب في كلية الهندسة الكهربائية والالكترونية في جامعة حلب حالياً، يحمل اختصاص خوارزميات ضغط وتشفير المعطيات، نشر العديد من الأبحاث في مجال أمن المعلومات ومعالجة الصور الرقمية باستخدام خوارزميات التعلم العميق والذكاء الصنعي.

المراجع

Abdulla, M. and Rana, M.E. (2020). Vulnerabilities in public key cryptography. *International Journal of Psychosocial Rehabilitation*, **24**(5), 3881–6. DOI:10.37200/IJPR/V24I5/PR202 096

Adeshina, A.M. (2020). Evaluation of Elliptic Curve El-Gamal and RSA public-key cryptosystems for digital signature. *Journal of Information Science, Systems and Technology*, **4**(1), 36–49.

Al-Kaabi, S.S. and Belhaouari, S.B. (2019). Methods toward enhancing RSA algorithm: A survey. *International Journal of Network Security & Its Applications*, **11**(3), 53–70. DOI: 10.5121/ijnsa.2019.11305

Fauzan, M.A. and Paulus, E. (2018). A framework to ensure data integrity and safety. *Journal of Computing and Applied Informatics*, **2**(1), 1–11. DOI: 10.32734/jocai. v2.i1–90

Harini, M., Gowri, K.P., Pavithra, C. and Selvarani, M. P. (2017). A novel security mechanism using hybrid cryptography algorithms. In: *IEEE International Conference on Electrical, Instrumentation and Communication Engineering*, Karur, India, 27–28/04/2017.

Iwasokun, G. B., Akinyokun, O. C., Alawode, S. J. and Omomule, T. G. (2019). An RSA algorithm for securing financial data on the cloud. *Journal of Advances in Mathematics and Computer Science*, **34**(3), 1–11. DOI: 10.9734/JAMCS/2019/v34i330215

K, Leela. and Vinod, S. (2018). Implementation of digital signature using hybrid cryptosystem. *International Journal of Engineering & Technology*, **7** (3.4), 34–7.

Kareem, S.M. and Rahma, A.M.S. (2019). A new hybrid (MD5 and RC4) cryptography algorithm using multi-logic states. In: *IEEE Ninth International Conference on Intelligent Computing and Information Systems,* Cairo, Egypt, Egypt, 8–10/12/2019. DOI: 10.1109/

ICICIS46948.2019.9014819

Khakim, L., Mukhlisin, M. and Suharjono, A. (2020). Security system design for cloud computing by using the combination of AES256 and MD5 algorithm. In: *IOP Conference Series Materials Science and Engineering*, Pandharpur, Maharashtra, India, 02–04/01/2020. DOI: 10.1088/1757-899X/732/1/012044

Khan, S. and Sharma, S. (2019). Analysis of cloud computing for security issues and approaches. *International Journal on Emerging Technologies*, **10**(1), 68–73.

Khatri, V. and Agarwal, V. (2020). Modified MD5 algorithm for low end IoT Edge devices. In: *IEEE 10th International Conference on Computing, Communication and Networking Technologies,* Kanpur, India, India, 6–8/07/ 2019. DOI: 10.1109/ICCCNT45670.2019. 8944533

Kumar, L. and Badal, N. (2019). A review on hybrid encryption in cloud computing. In: *IEEE 4th International Conference on Internet of Things: Smart Innovation and Usages,* Ghaziabad, India, India, 18–19/04/2019. DOI: 10.1109/IoT-SIU.2019.8777503

Miao, Y., Jia, H., Liu, X., Zhang, Y. and Tan, W. (2019). The Research and Application of Cloud Printing Platform Based on Improved AES-RSA Encryption Algorithm. In: *Scientific Conference on Network, Power Systems and Computing,* Guilin, China, 16–17/11/2019.

Mohan. D. N., Kumar, V. H. and Shashank, N. (2020). Enhancement of cloud computing security with secure data storage using AES. *International Journal of Research in Engineering, Science and Management*, **3**(1), 586–7.

Panjwani, M., Satpute, A., Kamble, A., Ukey, N., Makde, V. and Mehere, Y. (2020). Securing data in a cloud using AES. *International Journal of Research and Analytical Reviews*, **7**(1), 296–8.

Parthasarathy, R., Yee, H.W., Loong, S.S., Rajamanickam, L. and Ayyappan, P.P. (2019). Implementation of RSA algorithm to secure data in cloud computing. *International Journal of Innovative Science, Engineering & Technology*, **6**(4), 61–8.

Rao, A. and Suma, D. (2018). A novel image encryption algorithm with image integrity check. In: *IEEE 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions,* Bengaluru, India, India, 20–22/12/2018. DOI: 10.1109/CSITSS. 2018.8768797

Sadikin, M.A. and Wardhani, R.W. (2016). Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application. In: *IEEE International Seminar on Intelligent Technology and Its Applications*, Lombok, Indonesia, 28–30/07/2016. DOI: 10.1109/ISITIA.2016.7828691

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*, 7th edition. United States: Pearson Education.

Tabrizchi, H. and Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, **76**(n/a), 9493–532.

Yahya, F., Chang, V., Walters, R.J. and Wills, G.B. (2019). A security framework to protect data in cloud storage. In: *Proceedings of the 4th International Conference on Internet of Things, Big Data and Security*, Heraklion, Crete, Greece, 2–4/05/2019. DOI: 10.5220/ 0007737603070314