Journal of Engineering Sciences and Information Technology
Volume (5), Issue (4) : 30 Dec 2021
P: 59 - 80

ISSN: 2522-3321

مجلة العلوم الهندسية وتكنولوجيا المعلومات
المجلد (5)، العدد (4) : 30 ديسمبر 2021م
ص: 59 - 80

Hybrid Secure Model for Securing Data in The Cloud Computing System by Combining RSA, AES and CP-ABE

Zakria Mahrousa
Mahmoud Rahhal
Nairouz Alzin
Faculty of Electrical and Electronic Engineering || Aleppo University || Syria

Abstract: The cloud healthcare system represents an important application for cloud computing, as it uses the cloud for the operations of storing patient medical data and sharing it between health care service providers and patients, making the security and privacy of e-health system data the main concern of researchers.

This paper presents an integrated secure model for the healthcare system in cloud computing that achieves the security and confidentiality of data transferred through cloud computing, by combining the two algorithms AES and RSA with the access control algorithm CP-ABE in order to use the advantages of each of them, where the encryption process is done by a proposed algorithm which is based on the RSA algorithm, the XOR parameter, and the AES algorithm; the secrecy of the AES algorithm has been increased by generating a dynamic key, and the confidentiality of this key has been secured with two encryption levels, the first level using the CP-ABE algorithm and the second level using the RSA algorithm.

The proposed model is characterized by meeting the requirements of access control, authentication, and verification for both the transmitter and the receiver, and the results of the application of this model proved its ability to meet the security requirements of the health care system in cloud computing with the lowest possible implementation time, as the execution times were at the transmitter's end (43.2, 43.83, 45.11, 48. 23, 50.77, 52.16, 57.95, 63.2, and 63.35)ms for variable file sizes (37, 50, 100, 150, 200, 256, 512, 1000, and 1024)KB, respectively. The results also showed its superiority in terms of security requirements in cloud computing and the necessary implementation times on studied reference models.

Keywords: Authentication and Verification, Data Security, Data Privacy, Data Confidentiality, Hybrid Encryption, access control.

نموذج هجين آمن لحماية البيانات في الحوسبة السحابية بدمج RSA وAES وCP-ABE

زكريا مهروسة
محمود رحال
نيروز الزين
كلية الهندسة الكهربائية والإلكترونية || جامعة حلب || سوريا

المستخلص: يمثل نظام الرعاية الصحية السحابي تطبيق مهم للحوسبة السحابية، فهو يستخدم السحابة لعمليات تخزين البيانات الطبية للمريض ومشاركتها بين مقدمي خدمات الرعاية الصحية والمرضى مما يجعل أمن وخصوصية بيانات نظام الصحة الإلكتروني هو الشاغل الرئيسي للباحثين.

يقدم هذا البحث نموذج آمن متكامل لنظام الرعاية الصحية في الحوسبة السحابية يحقق أمن وسرية البيانات المنقولة عبر الحوسبة السحابية، من خلال دمج خوارزميتي AES وRSA مع خوارزمية التحكم في الوصول CP-ABE بغية الاستفادة من مزايا كل منها، حيث تتم عملية التشفير عن طريق خوارزمية مقترحة تعتمد على خوارزمية RSA والمعامل XOR وخوارزمية AES، كما تم زيادة سرية خوارزمية AES عبر توليد مفتاح ديناميكي، وتأمين سرية هذا المفتاح بمستويي تشفير، المستوى الأول باستخدام خوارزمية CP-ABE والمستوى الثاني باستخدام خوارزمية RSA.

يتميز النموذج المقترح بتلبية متطلبات التحكم بالوصول والتوثيق والتحقق لكل من المرسل والمستقبل، وأثبتت نتائج تطبيق هذا النموذج قدرته على تلبية متطلبات الأمن في نظام الرعاية الصحية في الحوسبة السحابية بأقل زمن تنفيذ ممكن، فقد كانت أزمنة التنفيذ في طرف المرسل ms (43.2 و43.83 و45.11 و48.23 و50.77 و52.16 و57.95 و63.2 و63.35) لأحجام ملفات متغايرة KB (37 و50 و100 و150 و200 و256 و512 و1000 و1024) على الترتيب. كما أظهرت النتائج تفوقه من ناحية متطلبات الأمن في الحوسبة السحابية وأزمنة التنفيذ اللازمة على نماذج مرجعية مدروسة.

الكلمات المفتاحية: التشفير الهجين، التوثيق والتحقق، أمن البيانات، خصوصية البيانات، سرية البيانات، التحكم بالوصول.

1- المقدمة.

ازداد استخدام الحوسبة السحابية في الآونة الأخيرة، لكونها تقدم العديد من الخدمات في مختلف المجالات وبالرغم من المزايا التي تمتع بها خدمات الحوسبة السحابية إلا أن معظم المؤسسات تخشى قبولها بسبب مشكلات الأمان والتحديات التي تواجهها مع السحابة.

لقد أجريت العديد من الأبحاث في مجال أمن نظام الصحة الإلكترونية السحابي، ومن هذه الأبحاث من ناقش متطلبات أمن بيانات الصحة الإلكترونية وخصوصيتها في السحابة[7]، حيث بيّن الباحثون الحاجة إلى تعزيز أمن وخصوصية البيانات الصحية السحابية وذلك من خلال الدمج بين آليات التشفير وآليات التحكم في الوصول، كما بينوا أن تقنية ABE هي الأكثر كفاءة من بين تقنيات التحكم في الوصول، ومن الأبحاث من حلل الحلول الأمنية الحالية في أنظمة الصحة الإلكترونية السحابية وبيّن متطلبات الأمن لنظام الصحة الإلكترونية السحابية[3]، فقد ناقش الباحث تحديات أمن وخصوصية السجلات الصحية الإلكترونية السحابية، ثم استنتج أنه يجب السعي لتحقيق معظم متطلبات الأمن لنظام الرعاية الصحية السحابية من خلال اقتراح نماذج لحماية البيانات وخصوصيتها من الوصول غير المصرح به إلى بيانات المريض الحساسة، ومن الأبحاث من حدد أهم متطلبات الأمن والخصوصية لنظام الرعاية الصحية السحابي[2]، فقد بيّن الباحثون قصور معظم الحلول الأمنية الحالية لكونها تعنى بمطلب أو أكثر من متطلبات الأمن لنظام الرعاية الصحية السحابي، وأكدوا على الحاجة الماسة لاقتراح حل شامل يحقق جميع متطلبات الأمن المطلوبة.

2- مشكلة البحث:

تفرض متطلبات أمن البيانات السحابية تصميم النماذج التي تضمن سرية وخصوصية البيانات، وتحتاج هذه النماذج إلى تقديم سياسات الأمان التي تهدف إلى حماية البيانات من الوصول غير المصرح به إلى البيانات المخزنة في السحابة، وتعتبر أنظمة الصحة الإلكترونية السحابية من أهم الأنظمة التي تتطلب تلبية جميع المتطلبات الأمنية، حيث يحتاج نظام الصحة الإلكترونية المستند إلى السحابة بالإضافة إلى توافر البيانات في أي مكان وفي أي وقت، إلى التوثيق والتحقق، وتأمين سلامة وخصوصية البيانات وسريتها أثناء نقل البيانات عبر الشبكة وتطبيق التحكم في الوصول لحماية بيانات الصحة الإلكترونية من الوصول غير المصرح به، للحفاظ على بيانات المريض آمنة أثناء مشاركة البيانات عبر الشبكة.

3- تساؤلات البحث:

يعتبر اقتراح حل شامل يحقق جميع متطلبات الأمن المطلوبة في نظام الحوسبة السحابية هو غاية مطلوبة للباحثين، وقد نجح العديد من الباحثين في تحقيق مطلب أو أكثر من متطلبات الأمن في الحوسبة السحابية، وبينوا الحاجة الماسة إلى اقتراح نماذج هجينة آمنة لحماية البيانات تحقق معظم متطلبات الأمن في الحوسبة السحابية، لهذا شرعنا في هذا البحث لاقتراح نموذج هجين آمن لحماية البيانات في الحوسبة السحابية وناقشنا فيه الإجابة عن التساؤلات التالية:

1- هل حقق النموذج المقترح سرية البيانات؟
2- كيف حقق النموذج المقترح الخصوصية والتكاملية؟
3- كيف حقق النموذج المقترح مطلب التحقق والتوثيق؟
4- هل حقق النموذج المقترح مطلب عدم الإنكار؟
5- هل استطاع النموذج المقترح أن يحقق التحكم في الوصول؟
6- هل تمكن النموذج المقترح من تحقيق زمن تنفيذ مقبول؟

4- فرضيات البحث:

يفترض هذا البحث أن النموذج الهجين الآمن المقترح لحماية البيانات في نظام الحوسبة السحابية يجب أن يلبي متطلبات الأمن في الحوسبة السحابية بأقل زمن تنفيذ ممكن.

5- هدف البحث:

يهدف هذا البحث إلى إيجاد نموذج لحماية بيانات المرضى في الحوسبة السحابية سواء المخزنة ضمن السحابة أو المنقولة بين مستخدميها.

6- أهمية البحث:

تنبع الأهمية العلمية لهذا البحث من خلال تحقيق النموذج المقترح متطلبات الأمن في الحوسبة السحابية وهي:

1- سرية البيانات، 2-الخصوصية والتكاملية، 3-التحقق والتوثيق، 4-عدم الإنكار، 5-التحكم في الوصول، 6-زمن تنفيذ مقبول، يعتمد هذا النموذج على دمج خوارزميات RSA وAES وCP-ABE بهدف الاستفادة من مزايا كل منها على حدة:

- مزايا التوثيق والتحقق وعدم الإنكار التي تحققها خوارزمية RSA غير المتناظرة، بالإضافة إلى ميزة إدارة المفاتيح من خلال استخدامها في تشفير المفتاح السري لخوارزمية AES المتناظرة.
- مزايا سرعة التشفير وفك التشفير لخوارزمية AES المتناظرة.
- مزايا التحكم في الوصول لخوارزمية CP-ABE غير المتناظرة، بالإضافة إلى الاستفادة من مزاياها الهامة في استخدامها في تقييد الوصول للبيانات الصحية.

7- مصطلحات البحث:

نعرف المصطلحات الآتية:

T: Transmitter المرسل (مالك البيانات): يلعب مالك البيانات دورًا حيويًا في أي نظام سحابي، فمالكو البيانات هم الذين يشاركون البيانات ويقومون بتخزينها على السحابة، والتي يمكن الوصول إليها من قبل المستخدمين المصرح لهم، فهم الذين يحددون سياسة وصول تصف من يمكنه الوصول إلى بياناتهم، حيث يتم تحديد هذه السياسة عبر مجموعة من السمات بواسطة مالك البيانات، وهم مسؤولون أيضًا عن تحميل البيانات إلى السحابة وتشفيرها بالخوارزمية المقترحة.

R: Receiver المستقبل (مستخدم البيانات): يستخدم مستخدمو البيانات المخزنة على السحابة، كما يقومون أيضًا بفك تشفير ملفات البيانات من خلال مفاتيح المصادقة التي يوفرها مالك البيانات، كما يجب أن يأذن خادم السحابة بناءً على هويتهم وسمات الأذونات للوصول إلى السحابة والبيانات المخزنة فيها.

M: Message الرسالة المطلوب حمايتها (النص الصريح).

AES: (Advance Encryption Standard) معيار التشفير المتقدم[14].

RSA: (Rivest Shamir Adleman) خوارزمية التشفير بالمفتاح العام[15].

CP-ABE:(Ciphertext-Policy Attribute-Based Encryption) التشفير المستند إلى السمات المستند إلى سياسة النص المشفر[4].

Ks: المفتاح السري لخوارزمية AES.

(PuT: Public Transmitter Key)، (PrT: Private Transmitter Key): المفتاحان العام والخاص للمرسل بخوارزمية RSA.

(PuR: Public Receiver Key)، (PrR: Private Receiver Key): المفتاحان العام والخاص للمستقبل بخوارزمية RSA.

C: Cipher text النص المشفر.

CC: Complex Cipher text النص المشفر المعقد.

CSP: Cloud Service Provider مزود الخدمة السحابية: يتم تخزين جميع البيانات من أصحاب البيانات والمستخدمين على الخادم السحابي.

AA: Attribute Authority سلطة السمة: وهي مسؤولة عن إنشاء مفاتيح سرية للمستخدمين وفقًا لسماتهم لفك تشفير البيانات بخوارزمية CP-ABE بالإضافة إلى ذلك، فهي مسؤولة عن إنشاء المفتاح العام والمفتاح الرئيسي لخوارزمية CP-ABE.

(PK: Public Key): المفتاح العام لخوارزمية CP-ABE.

(MSK: Master Secret Key): المفتاح السري الرئيسي لخوارزمية CP-ABE.

(SK: Secret Key): المفتاح السري لخوارزمية CP-ABE (الخاص بالمستقبل (المستخدم)).

8- هيكلية البحث:

تم إنجاز هذا العمل وفق الخطوات التالية:

1- دراسة أهم النماذج المرجعية المقترحة من قبل الباحثين لتطوير نماذج آمنة في الحوسبة السحابية.
2- دراسة وتلخيص أهم متطلبات الأمن في الحوسبة السحابية.
3- شرح النموذج الهجين المقترح وطريقة عمله.
4- تحليل النتائج ومناقشتها.

5- المقارنة مع النماذج المرجعية المدروسة.
6- الخاتمة.

1-8 دراسة أهم النماذج المرجعية المقترحة لتطوير نماذج آمنة في الحوسبة السحابية:

يوجد الكثير من الدراسات المرجعية التي تقوم بدمج خوارزمية AES مع خوارزمية التحكم في الوصول CP-ABE، أو دمج خوارزمية RSA مع خوارزمية CP-ABE، أو دمج كل من خوارزميتي RSA وAES مع CP-ABE بغية تحقيق سرية أعلى للبيانات وتلبية متطلبات الأمن في الحوسبة السحابية، فمن الأبحاث من درس وقارن بين دراسات مرجعية متنوعة تلبي مطلب أو أكثر من متطلبات الأمن لأنظمة الرعاية الصحية في الحوسبة السحابية[9]، وتمت المقارنة من خلال اقتراح الباحثان خمسة أسئلة تتعلق بالسرية وضمان التحكم في الوصول والخصوصية والسلامة والتوافر لبيانات الرعاية الصحية في الحوسبة السحابية، وحدد الباحثان من خلالها المتطلبات التي تحققها كل دراسة من الدارسات المرجعية المدروسة في بحثهما واستنتجا ضرورة تحقيق جميع متطلبات الأمن لنظام الرعاية الصحية في الحوسبة السحابية لحماية البيانات الحساسة للمريض.

ومن الأبحاث من درس دراسة مرجعية لتقنيات متنوعة تؤمن حماية بيانات الصحة الإلكترونية في السحابة [20]، فقد شرح الباحثان مزايا كل تقنية وأوصى الباحثان باقتراح النماذج الهجينة التي تجمع بين أكثر من تقنية لتعزيز الخصوصية والأمن لنظام الصحة الإلكتروني السحابي وتحقق جميع متطلبات الأمن لنظام الصحة الإلكترونية السحابي، واقتراحا استخدام تقنيات AES وRSA و ABE في هذه النماذج، حيث بيّنا أن التشفير المتماثل بخوارزمية AES آمنًا وسريعًا وقادرًا على تحقيق سرية البيانات، لكنه يحتاج إلى تقنية إضافية للتحكم في وصول المستخدمين إلى البيانات المخزنة في السحابة، كما بيَّن الباحثان أن تقنية التشفير بالمفتاح العام RSA لا تؤمن تحكم في الوصول، بالرغم من أنها تؤمن التوثيق والتحقق فهي تستخدم للتوقيع الرقمي وكذلك لمشاركة وإدارة المفاتيح السرية لخوارزمية AES، وكذلك بيّنا أن تقنية التشفير المستند إلى السمة ABE تتمتع بميزة منح الامتيازات القائمة على الأدوار، حيث يتم تشفير البيانات بالاعتماد على سمة معينة يجب مطابقتها مع المستخدمين لفك تشفير الملفات.

واتجه الباحثون لدمج أكثر من تقنية لتلبية متطلبات الأمن والخصوصية في نظام الصحة الإلكترونية السحابي، فمنهم من اقترح نموذج هجين لحماية البيانات[10] بدمج خوارزميتي RSA مع خوارزمية AES ويستخدم هذا النموذج الهجين خوارزمية RBAC للتحكم في الوصول المستند إلى الدور لتوفير الوصول وفقاً لدور المستخدم لمنح حق الوصول لأدوار محددة حسب حاجة المؤسسة، وبالتالي حماية البيانات من الوصول غير المصرح به، حيث يقوم نموذجهم المقترح على تشفير البيانات باستخدام خوارزمية AES وحلوا مشكلة إدارة المفاتيح فيها من خلال تشفير المفتاح السري لخوارزمية AES باستخدام خوارزمية RSA، حيث يستخدم المرسل(مالك البيانات) المفتاح العام للمستقبل لتشفير البيانات وتحميلها في السحابة ويقوم المستقبل بمفتاحه الخاص بفك تشفير المفتاح السري لخوارزمية AES، ومن ثم فك تشفير البيانات المشفرة بخوارزمية AES حيث يتم تحميل البيانات المشفرة حسب الدور بخوارزمية RBAC، وبرهن الباحثون فعالية نموذجهم المقترح لأنه ينفذ سياسات الوصول القائمة على الدور حسب حاجة المؤسسة بطريقة مرنة، ويحقق حماية البيانات المنقولة من وإلى السحابة، إلا أن نموذجهم المقترح لا يلبي جميع متطلبات الأمن في الحوسبة السحابية، كما أن تقنية RBAC تعتبر من التقنيات التقليدية في التحكم في الوصول[4].

بينما استطاع الباحثان [13] تأمين سرية البيانات وسلامتها من خلال ثلاث خوارزميات CP-ABE و AESوRSA، حيث يختار المستخدم الخوارزمية المناسبة وفقاً للزمن الذي يحدده المستخدم لتشفير الملفات، حيث أن CP-ABE

مناسبة للملفات ذات الأحجام الكبيرة فهي تستغرق زمن أقل من RSA وAES، واستنتجا أن خوارزميات AES وRSA تؤمن تشفيرًا سريعًا عندما يكون حجم الملف أقل من (100 ميغابايت) بينما يوفر CP-ABE تشفيرًا سريعًا لحجم ملف أكبر.

اقترح باحثون آخرون[16] نموذجاً لحماية البيانات المنقولة من وإلى السحابة، وذلك من خلال دمج خوارزميتي RSA و CP-ABE لتحقيق مستوى أفضل من الأمن والخصوصية للبيانات السحابية، حيث بيّن الباحثون أن تشفير CP-ABE يحقق التحكم في الوصول إلى البيانات السحابية إلا أنه لا يحقق سرية البيانات، لذلك استخدموا خوارزمية RSA لتأمين سرية البيانات قبل نقلها إلى السحابة، واعتمدوا في سياسة الوصول على سمتين فقط (الموقع– الجنس)، ولا يمكن فك التشفير النص المشفر إلا في حال تطابق سمات المستخدم مع سمات مالك البيانات إلا أن نموذجهم لا يحقق جميع المتطلبات الأمنية في الحوسبة السحابية.

أما الباحثون [19] فقد اقترحوا نموذجاً لتأمين حماية وخصوصية البيانات السحابية المخزنة علىdrobox ، وذلك من خلال اقتراحهم نموذج مطور يعتمد على نموذج للتحكم في الوصول CP-ABE، حيث سيتم تشفير البيانات قبل تخزينها علىdropbox، ويتم التشفير المتعدد حسب نوع الملف باستخدام أربعة خوارزميات مختلفة وهي AES وBlowfish وRSA وTriple DES، بينما يتم تشفير المفاتيح لهذه الخوارزميات بخوارزمية CP-ABE، وقارن الباحثون نموذجهم المطور مع النظام الحالي في drobox وهو التشفير الهرمي المستند إلى مجموعة HASBE مع خوارزمية معيار التشفير المتقدم AES المستخدمة لتشفير الملفات، واستنتجوا أن(HASBE) غير فعال لتأمين سرية البيانات ففيه مشاكل تتعلق بالخصوصية والسرية، وبالتالي فهو لا يلبي جميع متطلبات الأمن في الحوسبة السحابية، أما نموذجهم المقترح فقد حل المشاكل المتعلقة بسرية البيانات وخصوصيتها فقط، حيث يوفر نموذجهم المطور أمان البيانات مع زمن تنفيذ أقل من نظام HASBE الحالي، وذلك بسبب استخدامهم مخطط CP-ABE في نموذجهم، والذي يتميز بكفاءة عالية في معالجة أمن البيانات.

كما اقترح الباحثون [8] نموذجين مختلفين للتشفير الهجين لتأمين سرية البيانات وخصوصيتها من خلال الجمع بين خوارزميات التشفير المتماثل وغير المتماثل، النموذج الأول يجمع بين خوارزمية التشفير المتماثل DES وخوارزمية التشفير غير المتماثل RSA، حيث يتم تشفير البيانات باستخدام خوارزمية DES بينما يتم تشفير مفتاح خوارزمية DES السري باستخدام خوارزمية RSA لما لها من مزايا في إدارة المفاتيح، أما نموذج التشفير الهجين الثاني المقترح في دراستهم فهو يجمع بين خوارزمية AES وخوارزمية CP-ABE، ويقوم نموذجهم المقترح على توليد مفتاح جلسة عشوائي (S) لخوارزمية AES ومن ثم يتم تشفير الرسالة (M) بالمفتاح السري(S) لخوارزمية AES، مما ينتج عنه نص مشفرC1 كما يتم تشفير المفتاح السري(S) باستخدام خوارزمية CP-ABE بالاعتماد على سياسة الوصول المتضمنة السمات، مما ينتج عنه نص مشفرC2 ، يمثل C1 مع C2 النص المشفر الكلي C ، ثم يتم توليد ملخص الرسالة للنص المشفر C باستخدام تابع الاختزال المناسب، ومن ثم يتم إرسال C إلى طرف المستقبل والذي يقوم بدور بفك التشفير الهجين وذلك بفك تشفيرC2 أولاً، باستخدام مجموعة السمات الخاصة به، من أجل الحصول على المفتاح السري(S)، ثم يستخدم (S) لفك تشفير C1 إلى الرسالة M باستخدامAES ،

ومن ثم يتم توليد ملخص الرسالة من الرسالة المستلمة باستخدام تابع الاختزال، ويتم التحقق من خلال مقارنة ملخص الرسالة المولد مع ملخص الرسالة المستلم.

اقترح باحثان آخران[11] نموذج هجين يجمع بين خوارزميتي AES وخوارزمية التحكم في الوصول CP-ABE، حيث اقترحا تشفير الرسالة بخوارزمية AES من قبل المرسل (مالك البيانات)، حيث يقوم المرسل (مالك البيانات) بتحديد سياسة الوصول المتضمنة سماته، ويستخدم المرسل خوارزمية CP-ABE لتشفير المفتاح السري

لخوارزمية AES قبل إرسال البيانات إلى السحابة، وبذلك لن يتمكن المستقبل (المستخدم) من فك تشفير الرسالة إلا في حال تطابق سماته في سياسة الوصول مع السمات المحددة في سياسة الوصول من قبل المرسل (مالك البيانات)، كما بيّن الباحثان أن نموذجهما المقترح يمكن استخدامه لمشاركة البيانات بسرية مع مستخدمين آخرين من خلال تحديد سياسة وصول بدلاً من مشاركة مفتاح التشفير، إلا أنه لا يحقق جميع متطلبات الأمن في الحوسبة السحابية.

بينما اقترح باحث آخر[18] نموذج هجين متعدد الطبقات لحماية البيانات السحابية يجمع بين خوارزميتي RSA و AES بالإضافة إلى تقنية التحكم في الوصول المستند إلى الشبكة، حيث يمنح التحكم بالوصول المستند إلى الشبكة سياسة للوصول بالاعتماد على مالك البيانات والأدوار المختلفة لأولئك المؤهلين للوصول إلى البيانات، حيث يقوم نموذجه المقترح على إنشاء سياسة التحكم في الوصول في المستوى الأول وذلك في طرف المرسل (مالك البيانات)، حيث يسمح للمرضى بتخزين البيانات بعد تأمينها بنموذج حماية هجين يجمع بين خوارزميتي RSA وAES مما يحقق التكامل في مرحلة تخزين البيانات، يقوم التشفير الهجين في نموذجه المقترح على توليد مفتاح AES بطريقة عشوائية، ومن ثم تشفيره باستخدام خوارزمية RSA بالمفتاح العام للمستقبل، ومن ثم تشفير البيانات بخوارزمية AES للحصول على ملف الخرج الذي يعاد تشفيره بخوارزمية RSA ومن ثم يرسل إلى المستقبل، أما في طرف المستقبل في مرحلة فك التشفير واسترجاع البيانات يتم في المستوى الأول، إجراء فحص مستوى الأمان باستخدام مصفوفة التحكم في الوصول وذلك من أجل أي مستخدم يطلب الوصول إلى البيانات المتاحة في السحابة، وحسب نتيجة التحقق من صحة سياسة الوصول المتفق عليها يتم منح الشخص حق الوصول أو رفضه، وفي حال منح المستخدم حق الوصول يتم السماح بفك التشفير واسترجاع البيانات بخوارزمية RSA ومن ثم بخوارزمية AES، إلا أن نموذجه المقترح لا يحقق جميع متطلبات الأمن في الحوسبة السحابية وذلك لأن تقنية التحكم في الوصول المعتمدة في نموذجه هي إحدى تقنيات التحكم في الوصول التقليدي فهي تعتبر أحد نماذج الـ MAC.

كما استطاع الباحثون [12] تأمين البيانات السحابية وخصوصيتها من الوصول غير المصرح به، من خلال اقتراح نموذجاً يدمج بين خوارزميتيAES وCP-ABE، حيث يقوم المرسل (مالك البيانات) بتشفير البيانات قبل إرسالها إلى السحابة بخوارزمية AES، كما يقوم بتشفير المفتاح السري لخوارزمية AES بخوارزمية CP-ABE التي تحقق التحكم في الوصول حيث يقوم المستقبل (مستخدم البيانات) بفك تشفير مفتاح AES ويحصل عليه فقط عندما تتطابق السمات في سياسة الوصول له مع السمات في سياسة الوصول للمرسل (مالك البيانات)، إلا ان نموذجهم المقترح لا يحقق عدم الإنكار والتوثيق والتحقق، وبالتالي لا يحقق جميع متطلبات الأمن في الحوسبة السحابية .

يمكن أن نلخص جهود الباحثين السابقة في سعيهم إلى إيجاد نموذج يحقق سرية أعلى لبيانات المرضى في نظام الرعاية الصحية السحابي، بالإضافة إلى تحقيقه أغلب أو جميع متطلبات الأمن في الحوسبة السحابية، من خلال اقتراحات مختلفة للدمج بين الخوارزميات المتناظرة وغير المتناظرة، مع خوارزميات التحكم في الوصول بغية تحقيق سرية أعلى للبيانات وتلبية متطلبات الأمن في الحوسبة السحابية بأقل زمن تنفيذ ممكن، غير أننا سنخص بالدراسة، النماذج المرجعية الثلاثة التالية لاتسامها بالحداثة بغية مقارنة نتائجها مع النتائج التي سنحصل عليها من النموذج المقترح في هذا البحث من حيث متطلبات الأمن في الحوسبة السحابية وزمن التنفيذ.

1- النموذج المرجعي المدروس الأول: [17]

اقترح الباحثون[17] نموذجاً هجيناً لحماية البيانات الحساسة للوقت يجمع بين خوارزمية التحكم في الوصول المستند إلى السمة CP-ABE وخوارزميتيAES وRSA، فقد اقترحوا مرحلتين لحماية البيانات المنقولة من وإلى السحابة:

- في المرحلة الأولى تتم حماية البيانات من خلال نموذج هجين يجمع بين خوارزميتي CP-ABE وخوارزمية RSA، حيث يتم في مرحلة التسجيل في السحابة التحقق من تطابق السمات في سياسة الوصول لكل من المرسل (مالك البيانات) والمستقبل (المستخدم) وفي حال التطابق يحصل كل منهما على المفتاح السري المولد بخوارزمية RSA، حيث يرسل المفتاح الخاص بالمستقبل (المستخدم) عن طريق الإيميل، أما المفتاح العام للمرسل (مالك البيانات) فيعتمد كمفتاح عام أساسي لخوارزمية CP-ABE.
- أما في المرحلة الثانية لحماية البيانات فقد قام الباحثون باقتراح نموذج هجين لتشفير الملفات المنقولة من وإلى السحابة، يجمع بين خوارزميتي AES وخوارزمية التحكم في الوصول المستند إلى كلمة المرور PBE، حيث يتم تشفير الملف باستخدام خوارزمية AES بينما يتم تشفير المفتاح السري لخوارزمية AES بخوارزمية PBE، يتم إنشاء مفتاح (128bit) لتشفير الملفات، يستخدم لتشفير الملف بخوارزمية AES إلا أن نموذجهم المقترح استغرق زمن كبير نسبياً، كما أنه لا يحقق خاصية عدم الإنكار من قبل المرسل وبالتالي لا يحقق جميع متطلبات الأمن في الحوسبة السحابية، ولقد بيّنَّا ذلك في مبحث المقارنة.

2- النموذج المرجعي المدروس الثاني: [6]

اقترح الباحثون[6] نموذج تشفير هجين (AES – CP – IDABE Cipher-text Policy-Identity-Attribute-Based Encryption) حيث يتم في المرحلة الأولى تشفير البيانات باستخدام النموذج الهجين CP- IDABE، ويتم فيه تشفير البيانات بموجب سياسة الوصول من قبل المرسل (مالك البيانات) قبل إرسالها إلى السحابة بنموذج هجين يجمع بين خوارزمية CP-ABE وهوية المستخدم حيث يدمج النموذج الهجين CP- IDABE بين كلٍ من هوية المستخدم والسمات، حيث تتكون هوية المستخدم من اسم المستخدم وكلمة المرور، أما مجموعة السمات الخاصة بالمستخدمين فتتضمن مجموعة من الإجابات عن الأسئلة الخمسة التي تم استخدامها في نموذجهم المقترح، والتي يتم طرحها بشكل عشوائي للتحقق من المستخدمين أثناء المصادقة للسماح لهم بالوصول إلى البيانات الموجودة في السحابة، ثم يتم تطبيق التوقيع الرقمي باستخدام هوية المستخدم وسياسة الوصول المتضمنة مجموعة السمات المقترحة، كما يتم تشفير الرسالة بعد تشفير البيانات من خلال نموذجهم CP – IDABE المقترح مرة أخرى بخوارزمية AES بمفتاح سري بحجم (256bit) ثم يتم التحقق من التوقيع الرقمي للمستخدم قبل وصوله للبيانات والتحقق من تطابق السمات في سياسة الوصول، وفي حال التطابق يحصل المستخدم على النص المشفر، ومن ثم يقوم بفك التشفير بخوارزمية CP-IDABE، ثم فك التشفير بخوارزمية AES، وبالتالي استطاعوا من خلال نموذجهم المقترح تأمين خصوصية البيانات السحابية بالإضافة إلى التحكم في الوصول باستخدام التوقيع الرقمي عن طريق هوية المستخدم، وقد حققوا حماية من هجوم DOS، إلا أن نموذجهم المقترح لا يحقق خاصيتي عدم الإنكار والتوثيق والتحقق وبالتالي لا يحقق جميع متطلبات الأمن في الحوسبة السحابية كما بينا ذلك في مبحث المقارنة.

3- النموذج المرجعي المدروس الثالث: [5]

اقترح الباحثون[4] مقترح آخر لنموذج تشفير هجين متكامل CP-IDABE يجمع بين خوارزمية التشفير المستند إلى السمات، وهوية المستخدم المكونة من (اسم المستخدم وكلمة المرور) وخوارزمية RSA لتأمين البيانات في النظام

السحابي متعدد المالكين ومتعدد المستخدمين، حيث يتم تزويد كل من المالكين والمستخدمين بالمفاتيح السرية والعامة التي تم إنشاؤها بواسطة هيئة السحابة الآلية(ACA)، التي تستخدم لتسجيل المستخدمين وأصحاب البيانات حيث يتم بواسطتها التمييز بين مستخدم البيانات ومالكها في الوصول إلى البيانات السحابية من خلال سياسة السمات، وتم في نموذجهم المقترح تطبيق ثلاثة خوارزميات لتأمين سرية البيانات المخزنة على السحابة حيث تتكون خوارزمية RSA-CP-IDABE المقترحة من ثلاث خوارزميات مختلفة لضمان أمان البيانات في السحابة:

- الخوارزمية الأولى هي خوارزمية التوقيع الرقمي التي تولد التوقيع الرقمي لكل من المستخدم والمالك في وقت التسجيل في السحابة.
- أما الخوارزمية الثانية هي CP-IDABE التي تقوم بتشفير البيانات باستخدام سياسة الوصول المتضمنة السمات.
- بينما الخوارزمية النهائية هي RSA الخوارزمية التي تقوم بتشفير البيانات المشفرة مسبقًا مرة أخرى قبل تخزينها في السحابة، يجب على المرسل (المالك الأساسي للبيانات) إرسال كلاً من مفتاح RSA ومفتاح CP-IDABE للوصول إلى البيانات للمستخدم والمالكين الثانويين، حيث ميزوا في نموذجهم المقترح بين مالكي البيانات والمستخدمين ولكلٍ منهم توقيع رقمي، عندما يطلب المستقبل (المستخدم) البيانات، يتم التحقق من التوقيع الرقمي للمستخدم وتطابق السمات في سياسة الوصول، ثم يتم فك التشفير بخوارزمية CP-IDABE، ومن ثم بخوارزمية RSA للحصول على البيانات، واستنتجوا أن خوارزميةRSA-CP-IDABE المقترحة في نموذجهم تؤمن حماية البيانات من هجوم الرجل في الوسط(MITM)، إلا أن نموذجهم المقترح يستغرق تنفيذه زمن كبير، وذلك لوجود امتيازات ممنوحة حسب الهوية مع تعدد المستخدمين والمالكين في نموذجهم المقترح، كما أنه لا يحقق جميع متطلبات الأمن في الحوسبة السحابية وقد بيّنَّا ذلك في مبحث المقارنة.

2-8 متطلبات الأمن في الحوسبة السحابية

يوجد العديد من متطلبات الأمن في نظام الرعاية الصحية السحابي وتختلف من مرجع لآخر ومن منظمة لأخرى ويمكن تلخيصها بالمتطلبات التالية[2-3-7-9] :

1- **سرية البيانات**: يتعلق مفهوم السرية بالبيانات كما يمكن تعريفه بأنه عدم الاطلاع على البيانات الصحية للمرضى إلا من قبل مالك البيانات والمستخدمين المصرح لهم بالاطلاع، ولضمان سرية بيانات المريض يكون ذلك بتطبيق خوارزميات التشفير المتناظرة كخوارزمية AES والتي تتميز بسرعة عالية في التنفيذ، كما يتحقق بتطبيق خوارزميات التشفير غير المتناظرة كخوارزمية RSA إلا أنها تمتاز ببطء التنفيذ نسبياً فيما إذا قورنت مع الخوارزميات المتناظرة، كما يتحقق أيضاً بتطبيق خوارزميات التحكم في الوصول كخوارزمية CP-ABE.
2- **الخصوصية والتكاملية**: يتعلق مفهوم الخصوصية بالأفراد فهي تعني حماية حقوق الملكية الفكرية للمرسل (مالك البيانات)، بينما التكاملية تعني التأكيد على أن الأطراف المخولة فقط هي التي يمكنها تعديل البيانات، ويمكن تحقيق الخصوصية والتكاملية بتطبيق خوارزمية RSA غير المتناظرة، إلا أن خوارزمية CP-ABE تضمن خصوصية البيانات وسلامتها بكفاءة أعلى.
3- **التوثيق والتحقق**: يشمل مفهوم التوثيق على إمكانية مرسل البيانات أن يقوم بتوثيق بياناته بحيث يمكن للآخرين معرفة أن هذه البيانات تخص هذا المستخدم دون سواه ولا يمكن لهذه البيانات أن تكون لغيره، أما مفهوم التحقق فيشمل مفهومين أساسيين وهما:

- تحقق المستقبل من جهة الإرسال وإمكانية معرفة المرسل.

- تحقق جهة المرسل من جهة المستقبل وأنه لا يمكن لغير المستقبل الاطلاع على هذه البيانات.

غالباً ما تستخدم الخوارزميات غير المتناظرة لتحقيق خاصيتي التحقق والتوثيق، وذلك من خلال نماذج مختلفة تختلف فيما بينها بكيفية إجراء التشفير من ناحية المفاتيح الخاصة والعامة.

4- **عدم الإنكار**: يشمل مفهوم عدم الإنكار المنحيين التاليين:

- عدم إنكار المرسل بأنه قام بإرسال هذه البيانات.
- عدم إنكار المستقبل بأنه استقبل هذه البيانات.

إن هاتين الخاصيتين يمكن تحقيقهما باستخدام خوارزمية غير متناظرة كخوارزمية RSA، حيث يتحقق المفهوم الأول عند تشفير المرسل بياناته باستخدام مفتاحه الخاص. أما عند تشفير المرسل بياناته بالمفتاح العام يتحقق المفهوم الثاني (المستقبل لا يستطيع الإنكار) وذلك لعدم إمكانية امتلاك المفتاح الخاص إلا من قبل المرسل في الحالة الأولى أو المستقبل في الحالة الثانية.

5- **التحكم في الوصول**: يعني أنه يمكن للمرسل (مالك البيانات) إجراء تقييد انتقائي للوصول إلى بياناته في السحابة، حيث يمكن للمالك أن يصرح للمستخدمين القانونيين للوصول إلى البيانات، بينما لا يمكن للآخرين الوصول إليها بدون أذونات، يعد التحكم في الوصول ضروريًا لضمان التفويض المناسب والسرية لحماية خصوصية سجلات المرضى، حيث يجب على كل من مالك البيانات/ المستخدمين تحقيق سياسة الوصول، ويمكن تحقيق التحكم بالوصول من خلال طرق متعددة، و من أهمها تطبيق خوارزمية التشفير المستند إلى السمات المستند إلى سياسة النص المشفر (CP-ABE) وهي خوارزمية غير متناظرة وتعتبر نوع من أنواع تشفير المفتاح العام تؤمن التحكم في الوصول، حيث يتم تشفير البيانات وفقاً لسياسة الوصول المتضمنة عدد من السمات، حيث تقوم خوارزمية CP-ABE على أربع مراحل:

أولاً- مرحلة الإعداد: تنشئ الخوارزمية المفتاح العام (PK: Public Key) والمفتاح السري الرئيسي (MSK: Master Secret Key).

ثانياً- مرحلة توليد المفاتيح (PK,A, MSK):تقوم سلطة السمات (AA) في هذه المرحلة بتوليد المفتاح السري (SK: Secret Key) الخاص بالمستقبل (المستخدم)، كما يتم وضع سياسة الوصول الخاصة بكل مستخدم بالاعتماد على السماتA للمستخدم.

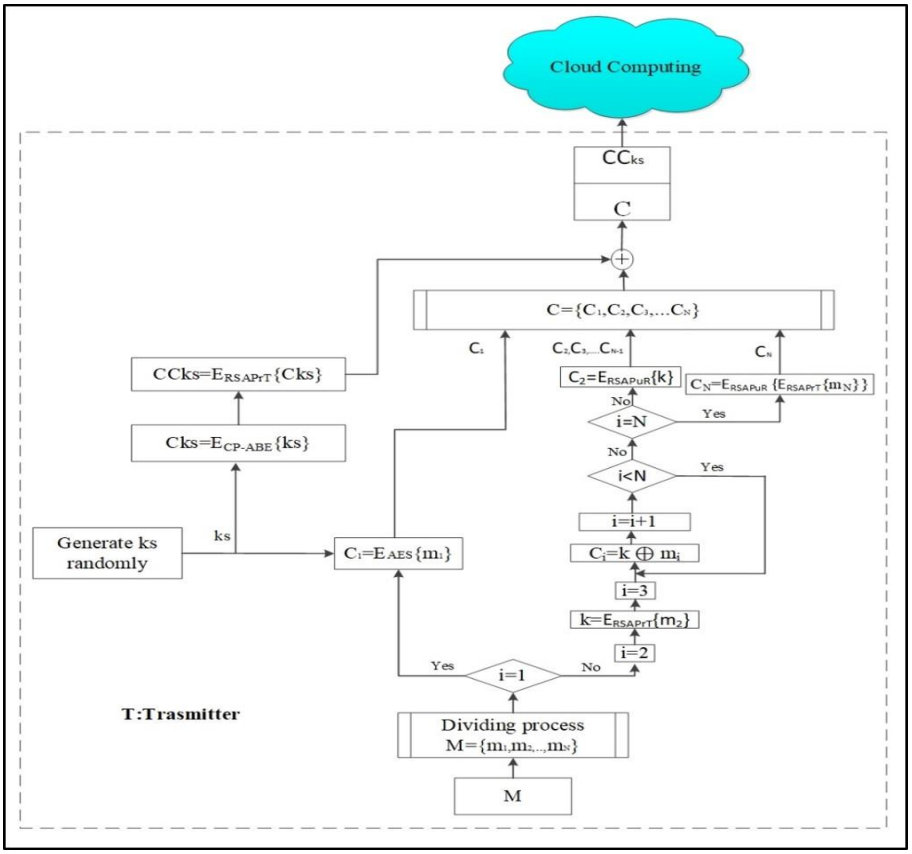
ثالثاً- مرحلة التشفير: يتم التشفير بالمفتاح العام PK وفقاً لسياسة الوصول والحصول على النص المشفر.

رابعاً- مرحلة فك التشفير: يتم فك التشفير في طرف المستقبل (المستخدم) بالمفتاح السري الخاص به SK بعد التحقق من سياسة الوصول الخاصة به.

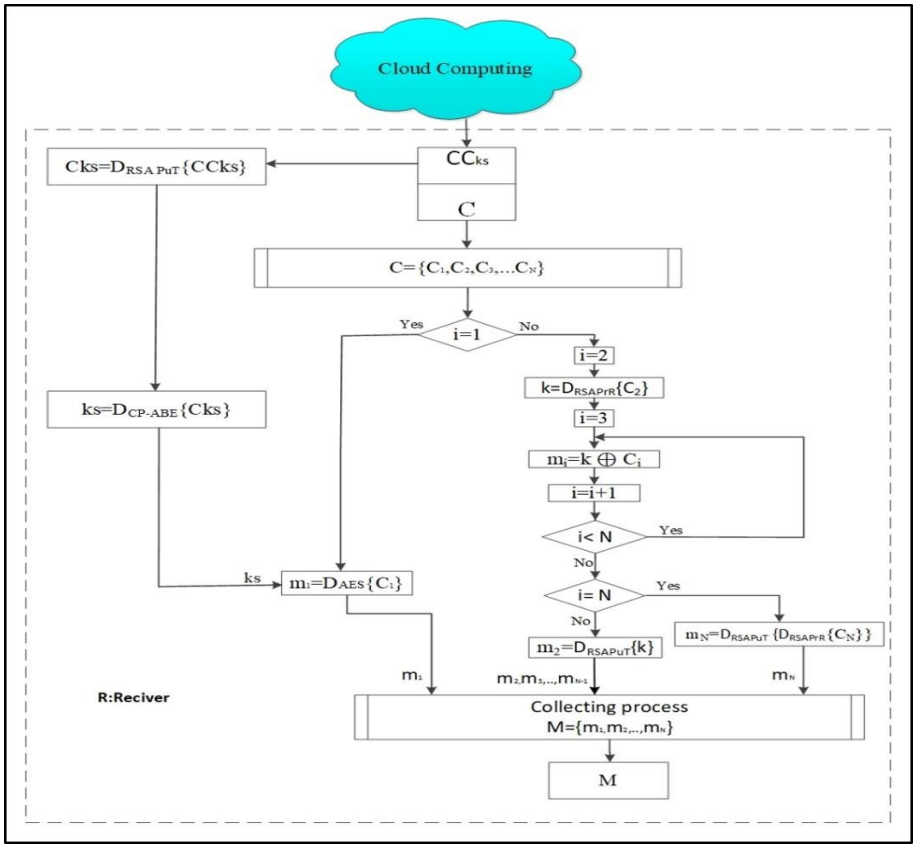
3-8 النموذج الهجين المقترح بدمج خوارزميات RSA وAES وCP-ABE

يبين الشكل (1) النموذج الهجين المقترح لدمج خوارزميتي RSA وAES مع خوارزمية التحكم في الوصول CP-ABE في طرف الإرسال بحيث يمكن الحصول على سرية عالية وضمان خصوصية البيانات الطبية وتحقيق متطلبات الأمن في الحوسبة السحابية بأقل زمن تنفيذ ممكن، وتقوم فكرة النموذج المقترح على تقسيم النص الصريح M إلى (N) كتلة بطول 128bit، وحماية الكتلة الأولى (m_1) من الرسالة بواسطة خوارزمية AES ذات مفتاح ديناميكي (Ks) يتم توليده في كل مرة بشكل عشوائي، وحماية هذا المفتاح بمرحلتي تشفير المرحلة الأولى باستخدام خوارزمية التحكم في الوصول CP-ABE (E_{CP-ABE} (Ks والمرحلة الثانية باستخدام خوارزمية RSA بالمفتاح الخاص للمرسل(CKs) E_{RSAPrT}، كما يتم تشفير كتل الرسالة m_i حيث(i=3,4,....,N-1) بالاعتماد على المفتاح (K) وهو ناتج تشفير الكتلة الثانية

من الرسالة (m_2) باستخدام خوارزمية RSA بالمفتاح الخاص للمرسل($E_{RSAPrT}(m_2)$، وحماية هذا المفتاح مرة أخرى بالمفتاح العام للمستقبل($E_{RSAPuR}(K)$، ثم يتم تشفير الكتلة الأخيرة (m_N) من الرسالة بمرحلتي تشفير باستخدام خوارزمية RSA، مرة باستخدام المفتاح الخاص للمرسل(E_{RSAPrT}) ومرة أخرى بالمفتاح العام للمستقبل($E_{RSAPuR}(m_N)$، ثم يتم إرسال الرسالة المشفرة مع المفتاح المشفر إلى السحابة سواء أكانت العملية تراسل أو تخزين، وفي طرف المستقبل تتم العملية العكسية كما هو مبين بالشكل (2).

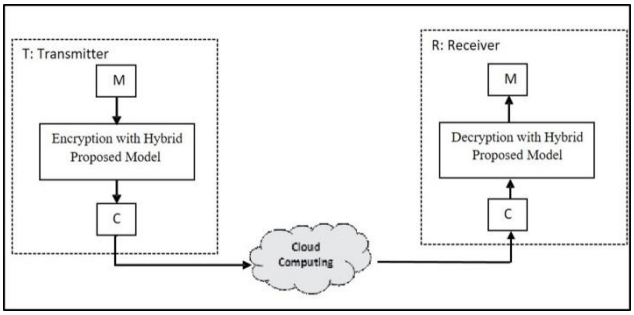


الشكل (1) النموذج المقترح لدمج خوارزميات RSAوAES وCP-ABE في طرف المرسل



الشكل (2) النموذج المقترح لدمج خوارزميات RSAوAES و CP-ABE في طرف المستقبل

يمكن تسخير النموذج الهجين المقترح لحماية البيانات في الحوسبة السحابية، حيث يتم تحميل البيانات المشفرة إلى الحوسبة السحابية من قبل المرسل، ثم يتم إجراء عملية فك التشفير عند استرجاع البيانات من الحوسبة السحابية في طرف المستقبل، كما هو مبين بالمخطط الصندوقي الموضح بالشكل (3).



الشكل (3) المخطط الصندوقي لحماية البيانات باستخدام النموذج الهجين المقترح في الحوسبة السحابية.

4-8 تحليل النتائج والمناقشة.

نناقش متطلبات الأمن في الحوسبة السحابية التي يحققها النموذج المقترح ومدى إمكانية تلبية هذه المتطلبات التي تم شرحها أعلاه كالتالي:

1- **سرية البيانات:** أن النموذج المقترح يؤمن خاصية سرية البيانات حيث لا يمكن الاطلاع على الرسالة إلا من قبل المستقبل، وذلك لأنه لا يمكن الحصول على الرسالة إلا بعد الحصول على (m_1) والتي لا يمكن الحصول عليها إلا بفك تشفير (C_1) باستخدام خوارزمية AES بالمفتاح Ks، وبما أنه لا يمكن الحصول على هذا المفتاح إلا من قبل من يملك سياسة الوصول المطابقة وفقاً لخوارزمية CP-ABE ويملك أيضاً المفتاح العام

للمرسلPuT، كما أن باقي كتل الرسالة mi حيث (i=3,4,....,N-1) لا يمكن الحصول عليها إلا بعد الحصول على المفتاح K وهو عبارة عن الكتلة الثانية مشفرة بخوارزمية RSA مرتين، وبالتالي لا يمكن لأحد سوى المستقبل أن يقوم بفك التشفير بمفتاحه الخاص PrR ومن ثم بالمفتاح العام للمرسل، بالإضافة إلى أن الكتلة الأخيرة أيضاً لا يمكن الحصول عليها إلا من قبل المستقبل حصراً الذي يقوم بفك التشفير بمفتاحه الخاص ومن ثم بالمفتاح العام للمرسل، وبالتالي لا يمكن لأحد أن يطلع على هذه الرسالة غير المستقبل مما يؤمن سرية البيانات وخاصية عدم الاطلاع.

2- **الخصوصية والتكاملية:** بما أن مفتاح فك التشفير Ks لا يمكن الحصول عليه إلا بإجراء فك تشفير CCKs مرتين، والمرة الأولى حصراً عن طريق المفتاح العام للمرسلPuT ، كما أن المفتاح K لا يمكن الحصول عليه إلا من قبل المستقبل بمفتاحه الخاص PrR، وبالتالي لا يمكن لأحد العبث بالرسالة إلا من قبل المستقبل صاحب الرسالة حصراً.

3- **التوثيق والتحقق:** يؤمن النموذج المقترح للمرسل إمكانية توثيق رسالته من خلال تشفيره لكلا المفتاحين (Ks المفتاح السري لخوارزمية AES والمفتاح K الذي يتم تشفير باقي كتل النص به ماعدا الكتلة الأخيرة) بواسطة خوارزمية RSA بالمفتاح الخاص له PrT، والذي يمكن اعتباره توثيق المرسل لرسالته، مما يتيح للمستقبل التحقق من جهة الارسال ومعرفة هويته، إذ لا يمكن للمستقبل الحصول على المفاتيح إلا بإجراء فك التشفير باستخدام خوارزمية RSA بالمفتاح العام للمرسلPuT، ولا يمكن ذلك بغير مفتاحه العام أو باستخدام أحد المفاتيح العامة للمستخدمين الآخرين، كما يتيح النموذج المقترح للمرسل التحقق من وصول الرسالة إلى المستقبل حصراً من خلال تشفيره المفتاح K بالمفتاح العام للمستقبل مما يؤكد للمرسل عدم إمكانية الحصول على المفتاح K إلا من قبل المستقبل (R) حصراً لعدم امتلاك غيره مفتاحه الخاص، كما تم تشفير الكتلة الأخيرة من النص m_N بالمفتاح العام للمستقبل كمستو ثاني للتشفير تأكيداً لذلك.

4- **عدم الإنكار:** بمجرد معرفة نص الرسالة الصريح (M) من قبل غير المرسل في النموذج المقترح لا يمكن للمرسل إنكاره أنه قام بإرسال هذه الرسالة ولا يمكن للمستقبل إنكاره أنه هو من قام بفتح هذه الرسالة حصراً، وذلك لعدم امتلاك غير كل من المرسل والمستقبل مفتاحه الخاص.

5- **التحكم في الوصول:** يؤمن النموذج المقترح التحكم في الوصول من خلال تشفير المفتاح السري Ks لخوارزمية AES باستخدام خوارزمية CP-ABE، حيث لن يتمكن المستقبل من فك تشفير الرسالة إلا في حال تطابق سياسة الوصول للمستقبل مع سياسة الوصول للمرسل (مالك البيانات)، وفي النموذج المقترح افترضنا أن سياسة الوصول تتضمن سمتين فقط وهما (اسم المريض ورقم بطاقة الائتمان) .

أدوات البناء والتشييد:

تم تنفيذ النموذج الهجين المقترح في بيئة ماتلاب (MATLAB) وذلك على معالج (intel Core i7-7500U 2.7GHz with Turbo Boost up to 3.5GHz)بذاكرة (8 GB DDR4).

زمن التنفيذ:

يتم بناء سياسة الوصول لكل من المرسل (مالك البيانات) والمستقبل (المستخدم)، ويتم تنفيذها في مرحلة التسجيل، أثناء التسجيل في السحابة، حين يقدم المستخدمين بيانات اعتمادهم ويتحقق النظام فيما إذا كانت سياسة الوصول للمستخدمين مطابقة لسياسة الوصول المخزنة في السحابة من قبل مالك البيانات.

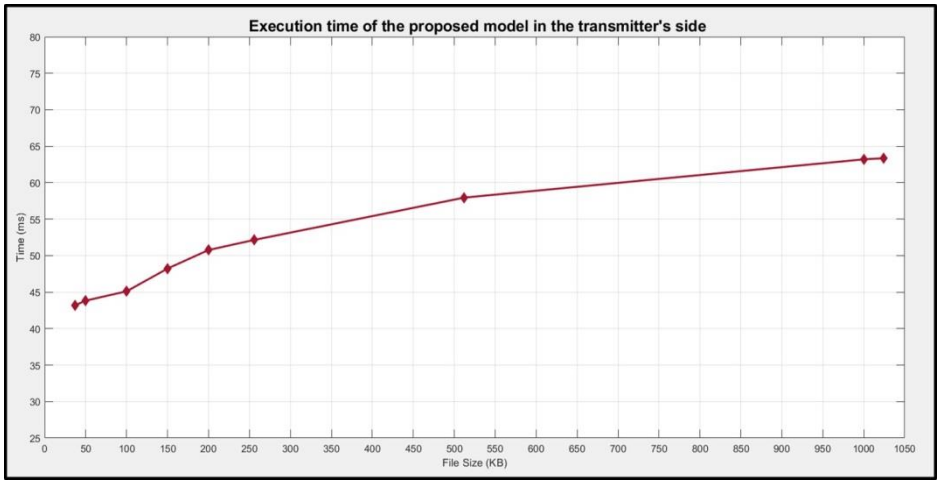
حيث تم اقتراح سمتين يجب التحقق منهما في سياسة الوصول ليتم السماح بالوصول إلى البيانات وهما (اسم المريض ورقم بطاقة الائتمان) عندها يحصل كل من (مالك البيانات/ المستخدم) على المفتاح السري لخوارزمية CP-ABE من السلطة المركزية AA.

يقوم المرسل (مالك البيانات) بتشفير البيانات وفق النموذج المقترح في الشكل (1) حيث يستخدم النموذج المقترح خوارزمية التحكم في الوصول CP-ABE لتشفير المفتاح السري Ks لخوارزمية AES وهو بحجم 128bit كما يستخدم خوارزمية RSA من أجل تشفير المفتاح السري Ks كمستو ثاني وهو بحجم 128bit، وتستخدم خوارزمية RSA مرتين لحماية المفتاح (K) ومرتين أخريين لحماية الكتلة الأخيرة من الرسالة، كما أن خوارزمية AES لا تستخدم إلا لتشفير الكتلة الأولى m_1 والتي هي أيضاً بحجم 128bit وليس لتشفير رسالة كبيرة نسبياً فيما إذا قورنت مع هذا الحجم، مما يؤمن اختزال الأزمنة الأخرى اللازمة لتشفير باقي كتل الرسالة حيث يتم تشفيرها بالاعتماد على المعامل XOR، كما أن هذه العملية تتم في الارسال والاستقبال مما يؤمن اختصار زمن التنفيذ سواء في الارسال أو الاستقبال، يبين الجدول(1) أزمنة التنفيذ للنموذج المقترح وكل من الخوارزمياتRSA وAES وCP-ABE في طرف المرسل من أجل أحجام ملفات متغايرة.

جدول (1) أزمنة التنفيذ للنموذج المقترح وكل من الخوارزمياتRSA وAES وCP-ABE في طرف المرسل من أجل أحجام ملفات متغايرة.

حجم الملف (KB)	زمن تنفيذ النموذج المقترح في طرف المرسل (ms)	زمن تنفيذ خوارزمية AES في طرف المرسل(ms)	زمن تنفيذ خوارزمية RSA في طرف المرسل(ms)	زمن تنفيذ خوارزمية CP-ABE في طرف المرسل(ms)
37	43.2	105	477	73
50	43.83	123	552	85
100	45.11	239	1112	142
150	48.23	306	1630	203
200	50.77	499	2063	335
256	52.16	552	2121	427
512	57.95	675	4587	522
1000	63.2	1325	9645	990
1024	63.35	1388	9695	1002

يبين الشكل (4) المنحني البياني لأزمنة التنفيذ للنموذج الهجين المقترح في طرف المرسل.



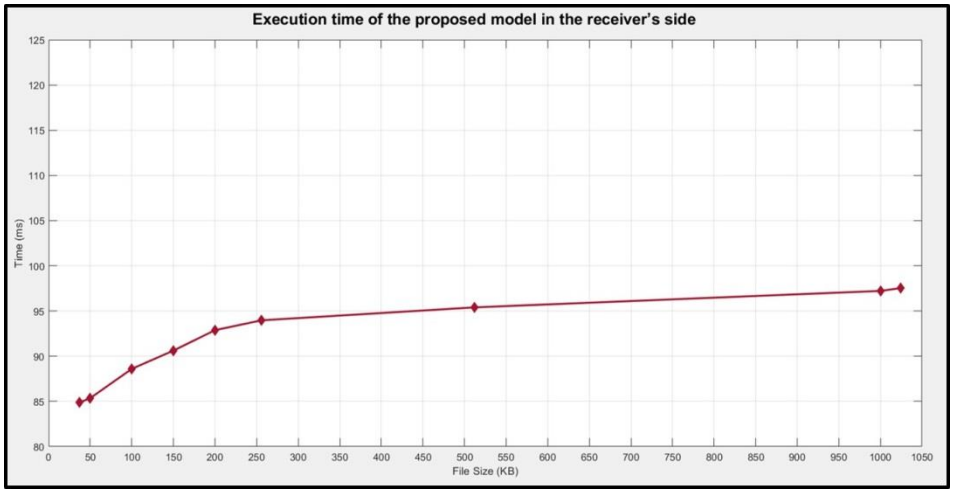
الشكل (4) زمن تنفيذ النموذج الهجين المقترح في طرف المرسل.

يبين الجدول (2) أزمنة التنفيذ للنموذج المقترح وكل من الخوارزميات RSA وِAES وCP-ABE في طرف المستقبل من أجل أحجام ملفات متغايرة.

جدول (2) أزمنة التنفيذ للنموذج المقترح وكل من الخوارزمياتRSA وAES وCP-ABE في طرف المستقبل من أجل أحجام ملفات متغايرة.

حجم الملف (KB)	زمن تنفيذ النموذج المقترح في طرف المستقبل (ms)	زمن تنفيذ خوارزميةAES في طرف المستقبل(ms)	زمن تنفيذ خوارزمية RSA في طرف المستقبل(ms)	زمن تنفيذ خوارزمية CP-ABE في طرف المستقبل(ms)
37	84.87	389	1780	135
50	85.36	470	2103	175
100	88.6	910	4025	237
150	90.62	1220	6440	345
200	92.88	1760	8200	550
256	93.97	2121	11843	789
512	95.4	4150	24560	1580
1000	97.22	9685	29132	3422
1024	97.53	9705	29895	3435

يبين الشكل (5) المنحني البياني لأزمنة التنفيذ للنموذج المقترح في طرف المستقبل.



الشكل (5) زمن تنفيذ النموذج المقترح في طرف المستقبل.

حالة دراسية لتطبيق النموذج المقترح في الحوسبة السحابية:

سنقوم بدراسة الحالة الدراسية التالية لتوضيح عمل النموذج المقترح:

نبين فيما يلي تطبيق النموذج المقترح على الحالة الدراسية بافتراض أن المرسل (مالك البيانات) هو المريض أو أحد الجهات المسؤولة عن علاجه (على سبيل المثال: أهل المريض – مشفى – مركز طبي)، والمستقبل هو (أحد الأطباء المشرفين على المريض)، وباعتبار أن ملف المريض المراد حمايته قبل تخزينه على السحابة هو ملف (word) بحجم 37KB .

أولاً- مرحلة الإعداد: سيتم في مرحلة التسجيل على السحابة وضع سياسة الوصول المتضمنة السمات وقد افترضنا في بحثنا سمتين فقط هما (اسم المريض، ورقم بطاقة الائتمان) حيث يحق لكل من لديه هذه السمات وعلى سبيل المثال أحد الأطباء المشرفين على المريض الوصول لملف المريض المخزن على السحابة، والسمتان المفروضتان للحالة المدروسة هما (محمد عبدو، 9980).

يتم توليد المفتاح السري Ks لخوارزمية AES باستخدام مولد مفاتيح عشوائي، حيث استغرق زمن الإعداد وتوليد المفتاح السري لخوارزمية AES والذي هو بحجم 128bit (0.0012ms) وذلك للحالة المدروسة.

كما يتم توليد المفاتيح العامة والخاصة لخوارزمية RSA والتي هي بحجم 1024bitوذلك لكل المرسل (PuT, PrT) والمستقبل (PuR, PrR)، حيث استغرق الزمن اللازم لتوليد المفتاحان العام والخاص لخوارزمية RSA لكل من المرسل والمستقبل (14.7ms) للحالة المدروسة.

كما يتم توليد مفاتيح خوارزمية CP-ABE وهي المفتاح الرئيسيMK والسري SK الخاص بالمستقبل والعام PK للمرسل (مالك البيانات) وهي مفاتيح يتم توليدها بعد التحقق من سياسة الوصول من قبل سلطة السمات AA، حيث استغرق زمن الإعداد وتوليد المفاتيح لخوارزمية CP-ABE (4.9ms)، وذلك بفرض اعتماد سمتين فقط لتقييد الوصول إلى ملف المريض في الحالة المدروسة، مع ملاحظة أنه كلما زاد عدد السمات كلما زاد الزمن، فقد حاولنا الاستفادة من ميزات خوارزمية CP-ABE بأقل زمن ممكن، فكان إجمالي الزمن لمرحلة الاعداد وتوليد المفاتيح للحالة المدروسة وفق النموذج المقترح (19.6ms).

ثانياً- مرحلة التشفير: يتم تطبيق النموذج المقترح في طرف المرسل (المريض) قبل إرسال ملف المريض إلى السحابة.

سيتم في البداية تجزئة ملف المريض الذي حجمه (37KB) إلى m_N كتلة بحجم 128bit، أي أن ملف المريض (303104 bit) يجزئ إلى (2368) جزء، كل جزء بحجم 128bitوحسب النموذج المقترح سيتم تشفير كل جزء كما يلي:

1- الكتلة الأولى من النص والتي حجمها 128bit سيتم تشفيرها بخوارزمية AES للاستفادة من مزايا التشفير بها، أي أن خوارزمية AESبجميع مراحلها ستطبق مرة واحدة فقط لتشفير كتلة بحجم 128bit فقط مما يفسر الأزمنة في النموذج المقترح، بغية الاستفادة من قوة التشفير بها ومزاياها بأقل زمن ممكن.

$$C_1=E_{AES}(m_1)$$

والمفتاح السري Ks لخوارزمية AES سيتم توليده عشوائياً بحجم 128bit، ثم يتم تشفيره بمستويي تشفير الأول بخوارزمية CP-ABE بالمفتاح العام للمرسل PK للاستفادة من ميزة التحكم في الوصول، وبالتالي فهي أيضاً تم استخدامها في النموذج المقترح لتشفير كتلة بحجم 128bit فقط:

$$CKs=E_{CP-ABE}(Ks)$$

والمستوى الثاني لتشفير المفتاح السري Ks بخوارزمية RSA بالمفتاح الخاص للمرسل E_{RSAPrT} للاستفادة من ميزتها في إدارة المفاتيح لخوارزمية AES، بالإضافة إلى ميزة التوثيق والتحقق وعدم الإنكار، حيث لا يمكن للمرسل إنكار أنه أرسل رسالته لأنه شفرها ووثقها بمفتاحه الخاص.

$$CCKs= E_{RSAPrT}(CKs)$$

2- الكتلة الثانية سيتم تشفيرها حسب النموذج المقترح بالمفتاح الخاص للمرسل، بغية تلبية مزايا التوثيق والتحقق وعدم الإنكار:

$$K=E_{RSAPrT}(m_2)$$

وسيتم اعتمادها كمفتاح لتشفير الكتل (i=3, 4,.... , N-1) من الرسالة والتي يتم تشفيرها بالاعتماد على المعامل XOR والكتلة الثانية على النحو التالي:

$$C_3=K\oplus m_3,\ C_4=K\oplus m_4,\ \ldots\ldots\ldots\ldots,\ C_{2366}=K\oplus m_{2366},\ C_{2367}=K\oplus m_{2367}$$

وهذا مما يفسر الأزمنة في النموذج المقترح، حيث يتم تشفير معظم كتل الرسالة بالاعتماد على المعامل XOR، ثم يتم حماية المفتاح Kوالذي هو عبارة عن الكتلة الثانية من الرسالة مشفرة بالمفتاح الخاص للمرسل وذلك قبل إرسالها للمستقبل بالمفتاح العام للمستقبل PuR كمستو حماية إضافي بغية تحقيق متطلبات التوثيق والتحقق وعدم الإنكار من جانب المستقبل باعتبار لا يملك أحد غيره المفتاح الخاص الذي سيتم فك التشفير به وذلك كما يلي:

$$C_2=E_{RSAPuR}(K)$$

3- أما الكتلة الأخيرة من الرسالة وهي الجزء 2368 سيتم حمايتها بمستويي تشفير بخوارزمية RSA وذلك للتأكيد على متطلبات الخصوصية والتوثيق والتحقق وعدم الإنكار.

$$C_{2368}= E_{RSAPuR}(E_{RSAPrT}(m_{2368}))$$

يتم إرسال الكتل المشفرة ($C_1,C_2,C_3,\ldots\ldots, C_{2368}$) مع مفتاح التشفير المشفر بمستويي تشفير إلى السحابة .

وقد استغرق زمن تشفير كتل الرسالة للحالة المدروسة وفق النموذج المقترح (23.6ms)، أي أن الزمن الكلي لتنفيذ النموذج المقترح على الحالة المدروسة في طرف المرسل هو (43.2ms).

بينما سيكون زمن التنفيذ في طرف المرسل في حال تطبيق خوارزمية AES بمفردها ومراحلها التكرارية على الملف الذي حجمه (37KB) هو(105ms)، وزمن التنفيذ في طرف المرسل في حال تطبيق خوارزمية RSA على الملف الذي حجمه (37KB) هو(477ms)، وزمن التنفيذ في طرف المرسل في حال تطبيق خوارزمية CP-ABE على الملف الذي حجمه (37KB) هو(73ms).

ثالثاً- مرحلة فك التشفير: في حال طلب المستقبل (أي شخص يملك السمات (أحد الأطباء المشرفين على المريض)) الوصول إلى ملف المريض، سيتم في البداية التحقق من تطابق سياسة الوصول المتضمنة سمتين فقط، ومن ثم تتم العملية العكسية في طرف المستقبل بفك تشفير البيانات على النحو التالي:

- في طرف المستقبل يتم استقبال الرسالة من السحابة والتي هي عبارة عن كتل النص المشفر مع المفتاح السري لخوارزمية AES المشفر بمستويي تشفير.

1- سيتم فك تشفير المفتاح السري Ks لخوارزمية AES بالمفتاح العام للمرسل بخوارزمية RSA مما يحقق الاستفادة من مزاياها:

$$CKs= D_{RSAPuT} (CCKs)$$

ثم يتم فك تشفيره بالمفتاح الخاص للمستقبل SK بخوارزمية CP-ABE:

$$Ks =D_{CP-ABE}(CKs)$$

2- سيتم الحصول على الكتلة الأولى من النص m_1 من خلال فك تشفيرها بخوارزمية AES:

$$m_1=D_{AES} (C_1)$$

3- سيتم الحصول على المفتاح K:

$$K=D_{RSAPrR}(C_2)$$

ثم يتم فك تشفير باقي الكتل (i=3, 4,.... , N-1) من الرسالة بالاعتماد على المعامل XOR على النحو التالي:

$$m_3=K\oplus C_3,\ m_4=K\oplus C_4,\ \ldots\ldots\ldots\ldots\ldots,\ m_{2366}=K\oplus C_{2366},\ m_{2367}=K\oplus C_{2367}$$

ثم الحصول على الكتلة الثانية من الرسالة:

$$m_2=D_{RSAPuT}(K)$$

4- أما الكتلة الأخيرة من الرسالة وهي الجزء 2368 في الحالة المدروسة:

$$m_{2368}= D_{RSAPuT} (D_{RSAPrR}(C_{2368}))$$

ثانياً- يتم تجميع كتل الرسالة في طرف المستقبل للحصول على M:

$$(m_1, m_2, m_3, \ldots\ldots\ldots, m_{2368})$$

وقد استغرق الزمن الكلي لفك تشفير الملف المدروس وفق النموذج المقترح (84.87ms).

بينما سيكون زمن التنفيذ في طرف المستقبل في حال تطبيق خوارزمية AES بمفردها ومراحلها التكرارية لفك تشفير الملف الذي حجمه (37KB) هو(389ms)، وزمن التنفيذ في طرف المستقبل في حال تطبيق خوارزمية RSA لفك تشفير الملف الذي حجمه (37KB) هو(1780ms)، وزمن التنفيذ في طرف المستقبل في حال تطبيق خوارزمية CP-ABE لفك تشفير الملف الذي حجمه (37KB) هو(135ms).

حساب معدل الإنتاجية (Throughput):

أن آلية التشفير المتبعة في النموذج المقترح تؤثر على نقل المعلومات عبر نظام الحوسبة السحابية من المرسل إلى المستقبل وبالعكس، لذلك قمنا بحساب معدل الإنتاجية للنموذج المقترح وكل خوارزمية من الخوارزميات المستخدمة RSA وAES وCP-ABE على حدة عند إنجاز عملية تشفير وفك تشفير البيانات، وذلك باعتبار:

- معدل إنتاجية التشفير لخوارزمية بأنها كمية المعلومات التي يمكن تشفيرها في وحدة الزمن:

معدل إنتاجية التشفير (Encryption Throughput) = مجموع أحجام الملفات المستخدمة(KB) / مجموع أزمنة التشفير (ms)

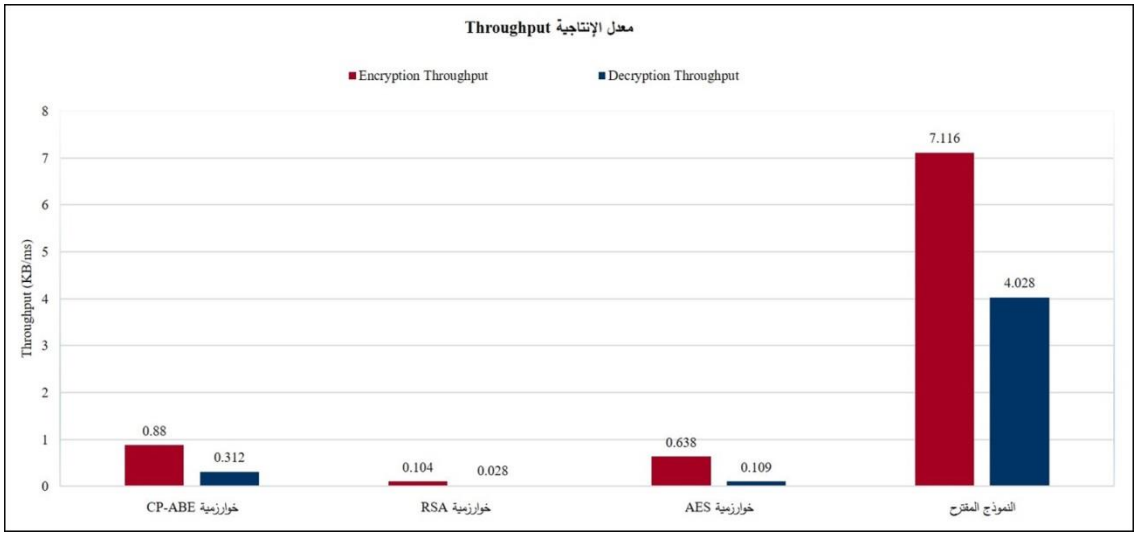
- معدل إنتاجية فك التشفير لخوارزمية بأنها كمية المعلومات التي يمكن فك تشفيرها في وحدة الزمن:

- معدل إنتاجية فك التشفير (Decryption Throughput) = مجموع أحجام الملفات المستخدمة(KB) / مجموع أزمنة فك التشفير (ms)

جدول (3) معدل الإنتاجية (Throughput) للتشفير وفك التشفير للنموذج المقترح وكل من الخوارزميات RSAوAES وCP-ABE

النموذج المقترح والخوارزميات المستخدمة / معدل الإنتاجية Throughput(KB/ ms)	النموذج المقترح	خوارزمية AES	خوارزمية RSA	خوارزمية CP-ABE
معدل إنتاجية التشفير	7.116	0.638	0.104	0.88
معدل إنتاجية فك التشفير	4.028	0.109	0.028	0.312

نلاحظ من الجدول (3) ارتفاع معدل إنتاجية التشفير وفك التشفير للنموذج المقترح بالمقارنة مع كل خوارزمية من الخوارزميات RSA وAES وCP-ABE على حدة، وذلك بالنسبة لأحجام الملفات المستخدمة في بحثنا، ويرجع ذلك لاستخدام هذه الخوارزميات في النموذج المقترح لتشفير كتل معينة من الرسالة وليس لكامل الرسالة مما حقق الاستفادة من ميزات هذه الخوارزميات وسرعة في إنجاز عمليتي التشفير وفك التشفير للنموذج المقترح، كما هو مبين في المخطط البياني لمعدل الإنتاجية الشكل (6).



الشكل (6) معدل الإنتاجية (Throughput) للنموذج المقترح وكل من الخوارزمياتRSA وAES وCP-ABE

نلاحظ من الشكل (6) أن النموذج الهجين المقترح يحقق أداء أفضل من حيث معدل الإنتاجية واستهلاك الطاقة، باعتبار أن معدل الإنتاجية للنموذج الهجين المقترح وكل من الخوارزميات RSA وAES وCP-ABE يتناسب عكسًا مع استهلاك طاقة وحدة المعالجة المركزية CPU، أي كلما زاد معدل الإنتاجية، ينخفض استهلاك طاقة وحدة المعالجة المركزيةCPU [1].

5-8 المقارنة:

بغية إجراء المقارنة بين النموذج المقترح والنماذج المرجعية المدروسة [17-6-5]، تم تطبيق النموذج المقترح على ملفات بأحجام متغايرة مطابقة لأحجام الملفات المستخدمة في النماذج المرجعية المدروسة الثلاثة، كما تمت مقارنة النموذج المقترح مع النماذج المرجعية المدروسة الثلاثة[17-6-5] من ناحية متطلبات الأمن في الحوسبة السحابية ومن ناحية زمن التنفيذ.

يبين الجدول (4) مقارنة أزمنة التنفيذ بين النموذج المقترح والنماذج المرجعية المدروسة [17-6-5]، وذلك لأحجام ملفات متغايرة، حيث يلاحظ تفوق النموذج المقترح على النماذج المرجعية بزمن التنفيذ، وذلك لأنه في النموذج المقترح يتم تنفيذ خوارزمية AES بحلقاتها التكرارية مرة واحدة لحماية الكتلة الأولى (m_1) من النص، وخوارزمية RSA مرة من أجل حماية المفتاح السري لخوارزمية AES، ومرتين أخريين من أجل حماية المفتاح (K) ومرتين لحماية الكتلة الأخيرة (m_N) من النص وخوارزمية CP-ABE مرة واحدة أيضاً لحماية المفتاح السري لخوارزمية AES وذلك لكتلة بحجم ثابت قدره 128bit في كل من طرفي المرسل والمستقبل، بينما في النماذج المرجعية المدروسة الثلاثة تقوم بتنفيذ خوارزميتي AES و RSAوCP-ABE بعدد أكبر بكثير من العدد المطلوب لتنفيذ النموذج المقترح في هذا البحث، مما يتطلب أزمنة تنفيذ إضافية للنماذج المرجعية المدروسة[17-6-5]، باعتبار أن زمن التنفيذ للمقارنة هو مجموع الأزمنة في طرفي المرسل والمستقبل.

جدول (4) مقارنة زمن التنفيذ بين النموذج المقترح والنماذج المرجعية المدروسة الثلاثة[17-6-5]

حجم الملف(KB)	زمن التنفيذ للنموذج المقترح	زمن التنفيذ للنموذج المرجعي الأول [17]	زمن التنفيذ للنموذج المرجعي الثاني [6]	زمن التنفيذ للنموذج المرجعي الثالث [5]
51.2	129.55ms	1.02 Sec	-	-
64	130.24ms	-	-	3000ms
128	136.63ms	-	-	3724ms
256	146.13ms	-	-	6592ms
512	153.35ms	-	-	8520ms
1000	160.42ms	-	178ms	-
1024	160.88ms	-	-	15.792ms

يبين الجدول (5) مقارنة بين متطلبات الأمن في الحوسبة السحابية التي يحققها النموذج المقترح والتي تحققها النماذج المرجعية المدروسة الثلاثة [17-6-5].

جدول (5) مقارنة المتطلبات التي يحققها كل من النموذج المقترح والنماذج المرجعية المدروسة الثلاثة[17-6-5].

النموذج المقترح والنماذج المرجعية / متطلبات الأمن في الحوسبة السحابية		النموذج المقترح	النموذج المرجعي المدروس الأول [17]	النموذج المرجعي المدروس الثاني [6]	النموذج المرجعي المدروس الثالث [5]
سرية البيانات		√	√	√	√
الخصوصية والتكاملية		√	√	√	√
التوثيق		√	×	×	×
التحقق	من المرسل	√	×	×	×
	من المستقبل	√	√	√	√
عدم الانكار	من المرسل	√	×	×	×
	من المستقبل	√	√	√	√
التحكم في الوصول		√	√	√	√

حيث نلاحظ من المقارنة المبينة في الجدول (5) بين إمكانية تلبية متطلبات الأمن في الحوسبة السحابية للنموذج المقترح والنماذج المرجعية الثلاثة [17-6-5]، تفوق النموذج المقترح على النماذج المرجعية الثلاثة في موضوع

التوثيق والتحقق من المرسل وعدم إنكاره إرسال الرسالة، وذلك بسبب وجود مرحلة تشفير إضافية لمفتاح الجلسة عن طريق المفتاح الخاص للمرسل في طرف الإرسال.

6-8 الخاتمة.

تم في هذا البحث اقتراح وتصميم نموذج آمن متكامل لنظام الرعاية الصحية في الحوسبة السحابية، حيث حقق النموذج المقترح متطلبات الأمن لنظام الرعاية الصحية في الحوسبة السحابية بأقل زمن تنفيذ ممكن من خلال دمج خوارزميتي RSA وAES مع خوارزمية التحكم في الوصول CP-ABE، وذلك بالاستفادة من مزايا خوارزمية RSA في تحقيق التوثيق والتحقق وعدم الإنكار، والاستفادة من التحكم في الوصول المستند إلى السمات الذي تحققه خوارزمية CP-ABE، بالإضافة إلى اعتماد خوارزمية AES على مفتاح تشفير ديناميكي يولد عشوائياً في كل جلسة، وذلك من أجل كتل ثابتة الحجم من الرسالة(128bit)لا يتجاوز عددها أربع كتل، وقد حقق هذا النموذج زمن تنفيذ أقل من النماذج المرجعية المدروسة الثلاثة [5-6-17].

9-قائمة المراجع.

[1] Adedeji, K. B. and Famoriji, J. O. "Investigating the Effects of varying the Key Size on the Performance of AES Algorithm for Encryption of Data over a Communication Channel ". *International Journal of Applied Information Systems*, 7(8), 6-10. (2014).

[2] Al-Issa, Y., Ottom, M.A. and Tamrawi, A. "eHealth Cloud Security Challenges: A Survey". *Journal of Healthcare Engineering*. https:/ / doi.org/ 10.1155/ 2019/ 7516035. (2019).

[3] BAJRIĆ, S. "Data Security and Privacy Issues in Healthcare". *Applied Medical Informatics*, 42(1), 19-27. (2020).

[4] Bhajantri, L. B. and Mujawar, T.N. "A Comprehensive Review of Access Control Mechanism Based on Attribute Based Encryption Scheme for Cloud Computing". *International Journal of Advanced Pervasive and Ubiquitous Computing*,11(3), 33-52. DOI: 10.4018/ IJAPUC.2019070103. (2019).

[5] Chandel, S., Yang, G. and Chakravarty, S. "A-CP-IDABE: A Secure Framework for Multi-User and Multi-Owner Cloud Environment". *information*, 11(8), 1-13. doi:10.3390/ info11080382. (2020).

[6] Chandel, S., Yang, G. and Chakravarty, S. "AES–CP–IDABE: A privacy protection framework against a DoS attack in the cloud environment with the access control mechanism". *information*, 11(8), 1-15. https:/ / doi.org/ 10.3390/ info11080372. (2020).

[7] Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F. "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing". *IEEE Access*, Vol. 7, 74361 – 74382. https:/ / doi.org/ 10.1109/ ACCESS.2019.2919982. (2019).

[8] Dev, S., Jose, A. P. and Joseph, J. "Security on cloud using hybrid encryption algorithm". *International Journal of Advance Research and Innovative Ideas in Education(IJARIIE)*, 4(3),1059-1063. (2018).

[9] Jain, J. and Singh, A. "A Survey on Security Challenges of Healthcare Analysis Over Cloud". *International Journal of Engineering Research & Technology (IJERT)*, 6(4), 905-912. (2017).

[10] Jayant, B., Swapnaja, U., Subhash, P., Kailash, K. and Sulabha, A. "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model". I*nternational Journal of Computer Applications*. 118(12), 47-52. (2015).

[11] Jyotheeswari, P. and Jeyanthi, N. "Hybrid encryption model for managing the data security in medical internet of things". *Int. J. Internet Protocol Technology*, 13(1), 25-31. (2020).

[12] Kumari, J. and krishnaveni, R.Y.S. "Preserving Privacy and Deduplication on Cloud with Attribute-Based Encryption and AES". *International Journal of Engineering and Techniques*, 4(2), 962-972. (2018).

[13] Mahajan, M. and Dharmadhikari, S. C. "Secure cloud storage of text and image files by giving access control to users". *International Journal of Recent Technology and Engineering (IJRTE)*, 8(4), 4618-4622. DOI:10.35940/ ijrte.C5172.118419. (2019).

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

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

[16] Radhakrishnan, P., Panicker, N.N., John, S.S., Varghese, N. P. and Divya, S. B. "Attribute and time factors combined CP-ABE and RSA based access control scheme for public cloud". *International Journal of Information Systems and Computer Sciences*, 8(2), 124-127. https:/ / doi.org/ 10.30534/ ijiscs/ 2019/ 29822019. (2019).

[17] Rahila, K.N., Nivedha, L., Narayani, R. and Banu, W.A. "Time based secure data handling in public cloud". *International Journal of Advanced Research (IJAR)*, 6(4), 887-895. DOI:10.21474/ IJAR01/ 6925. (2018).

[18] Saravanan, N. and Umamakeswari, A. "Lattice based access control for protecting user data in cloud environments with hybrid security". *Computers & Security*, 100(n/ a),1-9. https:/ / doi.org/ 10.1016/ j.cose.2020.102074. (2021).

[19] Shinde, A., Kangane, R., Deshmukh, P. and Kuchiwale. S.L. "Access control model with attribute based multiple encryption". *International Journal for Research in Engineering Application & Management (IJREAM)*, 3(1), 42-46. (2017).

[20] Yadav, D. K. and Behera, S. "A Survey on Secure Cloud-Based E-Health Systems". *EAI Endorsed Transactions on Pervasive Health and Technology*, 5(20), 1-21. doi: 10.4108/ eai.13-7-2018.163308. (2019).