بسم الله الرحمن الرحيم
Omdurman Islamic University Journal(OIUJ)
مجلة جامعة أم درمان الاسلامية
https://journal.oiu.edu.sd/index.php/oiuj
https:// DOI 10.52981/oiuj.v19i2.3082.
2023; 19(2);264 – 278
ISSN: 5361-1858

تحسين أمن وسرية الحوسبة السحابية من خلال دمج صفات خوارزمية Blowfish و (RSA)

Enhancing the Integrity and Confidentiality of Cloud Computing by Merge Blowfish and RSA Cryptography Algorithm

رندا محمد عبدالحليم مختار[1] ، د. الطيب السماني عبدالجبار[2]

[1] قسم الحاسبات و تقنية المعلومات ، كلية علوم الحاسوب ، جامعة النيلين – السودان
[2] قسم الحاسبات و تقنية المعلومات ، كلية علوم الحاسوب ، جامعة النيلين – السودان

[1] البريد الالكتروني: randa@kku.edu.sa
[2] البريد الالكتروني: tayebasamani@neelain.edu.sd

للاستشهاد بهذا المقال:–

رندا محمد عبدالحليم مختار[1] ، د. الطيب السماني عبدالجبار[2]، تحسين أمن وسرية الحوسبة السحابية من خلال دمج صفات خوارزمية Blowfish و (RSA)، مجلة جامعة أم درمان الاسلامية

ISSN: 5361-1858

.https:// DOI 10.52981/oiuj.v19i2.3082

المستخلص

الحوسبة السحابية هي تكنولوجيا حديثة تستخدم الإنترنت ، وخوادم مركزية لتنظيم البيانات والتطبيقات ، التي تمكن العملاء من استخدامها ، كما تمكن الشركات والمؤسسات بمختلف أشكالها وأحجامها ومجالاتها بالخدمات السحابية للوصول الى موارد وخدمات كبيره ، مثل الاحتفاظ بنسخة احتياطية من البيانات، واستخدام الاميل ، وتحديث البرامج واختبارها، وتحليل البيانات الكبيرة، ولكن بالمقابل تواجه الحوسبة السحابية العديد من المشاكل وواحدة من أهم هذه المشاكل هي أمن المعلومات المخزنة فيها ، فيتم التحكم في المعلومات بالكامل من قبِل مقدم الخدمة وليس بواسطة العميل ونتيجة لذلك تكون معلومات العميل غير آمنة على جانب الخادم .يغطي هذا البحث الأهداف الأساسية لأمن البيانات وهي : السرية وسلامة البيانات بإستخدام هجين من خوازميات التشفير المتماثلة وغير متماثلة (RSA-Blowfish) بهدف تحسن الأمان وضمان البيانات من قبل مزودي الخدمات السحابية حيث تم مقارنة مشاكل خوارزمية BlowFish مثل الوقت البطئ المستغرق في التشفير وفك التشفير والهجوم المعتاد لها والذي يجعلها وسيلة مستهدفة سهلة الكسر ولكن عن طريق الخوارزمية الهجينة المقترحة إذا اراد المستخدم رفع ملف ، أو تنزيله من التخزين السحابي فيقوم بتنفيذ الخوارزمية المهجنة

التي تأخد مزايا RSA و Blowfish و يتم تطبيقها علي الملفات المرسلة بصورة عشوائية لتشفير هذا الملف وايضا يقوم البرنامج بعملية فك التشفير باسترجاع معلومات عملية التشفير لفك تشفير الملف بعد تنزيله من التخزين السحابي مما حسن من مستوى أمان البيانات مقارنة بخوارزميات التشفير المنفردة في الحوسبة السحابية.

الكلمات المفتاحية: الحوسبة السحابية ،تشفير البيانات، أمن الحوسبة السحابية، خوارزمية التشفير ، RSA،Blowfish

Abstract

Cloud computing is a modern technology that uses the Internet and central servers to organize data and applications that enable customers to use them. It also enables companies and institutions of all shapes, sizes, and fields with cloud services to access large resources and services, such as backing up data, using email, updating and testing programs, and analyzing big data, but on the other hand, cloud computing faces many problems, and one of the most important of these problems is the security of the information stored in it, so the information is completely controlled by the service provider, not by the client, and as a result, the client's information is not secure on the server side. This study covers the basic objectives of data security, namely: Confidentiality and data integrity using a hybrid of symmetric and asymmetric encryption algorithms (RSA-Blowfish) with the aim of improving security and ensuring data by cloud service providers, where each of the problems of the Blowfish algorithm, such as the slow time spent in encryption, were compared and discussed. And the usual decryption and attack make it a target method that is easy to break through the proposed hybrid algorithm. If the user wants to upload a file or download it from the cloud storage, then he implements the hybrid algorithm that takes the advantages of RSA and Blowfish and applies it to randomly sent files to encrypt this file as well. The program performs the decryption process by retrieving the encryption process information to decrypt the file after downloading it from the cloud storage, which has improved the level of data security compared to the single encryption algorithms in cloud computing.

1. مقدمة :

هنالك مشكلة كبيرة تواجه عملية تخزين البيانات عند اعتماد الحوسبة السحابية، وهي أمان البيانات حيث تحتوي السحابة على العديد من التحديات والقضايا ، والتحديات الأمنية التي تغطي الأهداف الرئيسية للحوسبة وأمن البيانات هي: التوفر ، السرية، والنزاهة. حيث سلطت هذه المنهجية الضوء على سرية البيانات، باستخدام تقنيات التشفير وذلك لحماية سرية البيانات حيث ان الخوارزميات أصبحت غير مواكبة للتطور مما جعلها غير أمنة بشكل كافي لذلك أقترح هذا البحث تقنية تتوافق مع التطورات والهجمات التي تظهر يوميا علي سرية البيانات المشفرة ،حيث يوضح هذا الفصل المنهجية الجديدة المقترحة التي توفر سرية اكثر لتخزين الملفات في السحابة العامة باستخدام دمج افضل خوارزميات التشفير المتماثل وغير المتماثل من حيث وقت التشفير وفك التشفير وقوة المفتاح وطوله وهما خوارزميتا (Blowfish-RSA)(Belguith et al., 2015,p5).

2. اهداف البحث :

يهدف البحث الى التوصل لمنهجية جديدة تعالج مشكلة تخزين البيانات

3. مشكلة البحث :

تاتي مشكلة البحث للاجابة عن السؤال الرئيسي

هل اصبحت الخوارزيمات غير فعالة في امن البينات ؟

4. **الدراسات السابقة**

1. 2 دراسةGaurav R. Patel (Patel and Panchal, 2014)واخرون بعنوان "Hybrid Encryption Algorithm " المنشورة بمجلة "International Journal of Engineering Development and Research " عام 2014 استخدم الباحثون خوارزمية تبادل المفاتيح RSA و Diffie Hellman حيث تُستخدم خوارزمية RSA لتوفير أمان الرسالة باستخدام عملية التشفير وفك التشفير. تُستخدم خوارزمية Diffie Hellman لإنشاء المفتاح السري للمرسل والمستقبل للاتصال. توفر خوارزمية RSA مزيدًا من الأمان مقارنة بالخوارزمية الأخرى.

2. 2 دراسةEr. Ashima Pansotra1 (Pansotra and Singh, 2015)واخرون بعنوان "Cloud Security Algorithms " المنشورة بمجلة "International Journal of Security and Its Applications "عام 2015 خلصت الدراسة الي ان رغم وجود العديد من الخوارزميات المتاثلة لأمن البيانات مثل DES و AES و .Triple DES والخوارزميات غير متماثلة RSA و Diffie-Hellman Key Exchange وHomomorphic الا ان هذه الخوارزميات ليست آمنة وما زالت هناك حاجة لتعزيز أمن الخوارزميات.

3. 2 في دراسةPriyadarshini Patil (Panda, 2022.)واخرون بعنوان " A Comprehensive Evaluation of DES, AES, RSA and Blowfish3Cryptographic Algorithms: DES," المنشورة في مؤتمر " International Conference on Information Security & Privacy (ICISP2015) " عام2015 قامو بمقارنة هذه الخوارميات من حيث وقت التشفير وفك التشفير وحجم الذاكرة المستخدمة وقوة تشفير الخوارزمية بالإضافة الي قياس العشوائية في التشفير عن طريق استخدام لغة الجافا توصلو الي ان كل من تقنيات التشفير لها نقاط القوة والضعف الخاصة بها. من نتائج التجربة ، يتضح أن الذاكرة المطلوبة للتنفيذ هي الأصغر في Blowfish بينما هي الأكبر في .RSA تتظهر النتائج أن RSA يستهلك وقتًا أطول للتشفير وفك التشفير مقارنة بالآخرين بينما Blowfish

أقل وقت بين الجميع كما تتميز بالكفاءة في البرامج إذا كان الوقت والذاكرة عاملين رئيسيين في التطبيق ، فإن Blowfish هي الخوارزمية الأنسب.

4. 2 دراسة سناء بلغيث (Belguith et al., 2015) واخرون بعنوان " Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm" المنشورة في مؤتمر " The Eleventh International Conference on Autonomic and Autonomous Systems" عام 2015 قام الباحثون بتجربة خوارزمية متماثلة وجمعها مع خوارزمية غير متماثلة لزيادة الأمان الفعال للتشفير غير المتماثل والأداء السريع للتشفير المتماثل مع الحفاظ على حقوق المستخدمين للوصول إلى البيانات بطريقة آمنة ومصرح بها. قام الباحثون بعمل مقارنة بين الخوارزميات في سرعة الأداء وطول المفتاح الذي يزيد من امن البيانات والذي تتميز به الخوارزميات المتامثلة وتم اختيار الخوارزمية الغير متماثلة (AES) مع الخوارزمية المتماثلة (RSA) حيث كانت الخوارزمية المهجنة اسرع في التشفير واقوي امانا.

5. 2 في دراسة بعنوان (Amalarethinam and Leena, 2017) "Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud " المنشورة في مجلة World Congress on Computing and Communication Technologies في العام 2016 ناقش الباحثون خوارزميات التشفير المستخدمة في امان بيانات الحوسبة السحابية واقترحو ان خوارزمية RSA يمكن تغيير حجم المفتاح لجعل عملية التشفير قوية. ومن ثم يؤدي الي زيادة الوقت المستغرق في عملية التشفير وفك التشفير حيث تقلل الخوارزمية المقترحة من وقت عمليات التشفير وفك التشفير عن طريق تقسيم الملف إلى كتل وتعزز قوة الخوارزمية عن طريق زيادة حجم المفتاح.

6. 2 دراسة Fortine Mata (Mata et al., 2015) في دراسة بعنوان" Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)" المنشورة في مجلة " International Journal of Science and Research (IJSR) " الصادرة عام 2017 قام الباحث بعمل مقارنة للبيانات اثناء تشفيرها بخوارزمية AES ثم تشفيرها بخوارزمية Blowfish ولزيادة امان البيانات اثناء نقلها في السيرفر اعتمد علي ان استخدام الخوارزمية الاولي للتشفير ثم مرة اخري استخدام الخوارزمية الثانية علي نفس البيانات المشفرة سابقا قد زاد من الموثوقية للبيانات وذلك كما ذكر الباحث قد عالج مشكلة ضمان سرية البيانات في السحابة ضد عمليات الوصول التي تتجاوز الحقوق المصرح بها.

7. 2 في دراسة (Panda, 2022.) Priyadarshini Pati))بعنوان " A Comprehensive Evaluation of Cryptographic Algorithms: DES, AES, RSA and Blowfish" المنشورة في مجلة " International Journal of Scientific Research in Computer Science Applications and Management Studies " عام 2018 تقدم هذه الورقة تقييمًا لكل من خوارزميات التشفير المتماثلة (AES، DES ، السمكة المنتفخة) وكذلك غير المتماثلة (RSA) ومقارنة لخوارزميات التشفير هذه باستخدام معلمات التقييم مثل وقت التشفير ووقت فك التشفير والإنتاجية وقد توصل البحث الي ان افضل الخوارزميات في التشفير من حيث الوقت هي AES اما افضلها من حيث فك التشفير وقتا هي RSA وان خوارزمية Blowfish هي الثانية من ناحية الإنتاجية .

8. 2 في دراسة(Chinnasamy and Deepalakshmi, 2018) بعنوان " Design of Secure Storage for Health-care Cloud using Hybrid Cryptography" المنشورة في المؤتمر الثاني " International Conference on Inventive Communication and Computational Technologies (ICICCT 2018) " عام 2018 ناقش الباحثون أهمية حماية البيانات الطبية التي تكون علي شكل سجلات صحية إلكترونية (EHR) والتي تتوفر على الإنترنت في أي وقت(السحابة الالكترونية)حيث يعتبر امان هذه البيانات الحساسة مهم جدا ولحل هذه المشكلة اقترحوا تشفير

البيانات من خلال خوارزمية متماثلة وتشفير المفاتيح باستخدام خوارزمية غير متماثلة. تم قياس تقييم الأداء ، وكذلك أمان الطريقة المقترحة ، ومقارنتها حيث أظهرت نتائج البحث ان الطريقة المقترحة توفر أمانًا أفضل من أي خوارزميات هجينة أخرى، تم اقتراح طريقتين مختلفتين لتوليد المفاتيح من خوارزمية مفتاح متماثلBlowfish وخوارزمية RSA مما ادي الي تقليل وقت تشفير وفك تشفير مقارنةً بالتقنيات المتماثلة الأخرى مثل AES و Blowfis كما انها قدمت مزايا اخري مثل التشفير السريع والأعداد الأولية الكبيرة لتوليد المفاتيح والإدارة الفعالة للمفاتيح.

2. 9 دراسة K. R. Sajay واخرون (Sajay et al., 2019) بعنوان " Enhancing the security of cloud data using hybrid encryption algorithm " المنشورة في مجلة "Journal of Ambient Intelligence and Humanized Computing " في العام 2019 جمع الباحثون بين التشفير المتجانس"Homographic " وتشفير Blowfish لتعزيز أمان السحابة وذلك أولا بتحويل البيانات الي بت وذلك ليتمٍتطبيق التشفير في الطبقة الاولي عن طريق التشفير المتجانسHomographic "" ثم ارسال البيانات المشفرة الي الطبقة الثانية وتشفيرها عن طريق خوارزمية " Blowfish " لتحسين امن السحابة واستنتجت الدراسة الي ان العمل بهذه الطريقة قد حسن من الامن في السحابة .

2. 10 دراسة خباب مصطفى واخرون(Mohammed and Supervisor, 2019) بعنوان " Confidentiality of Data in Public Cloud Storage Using Hybrid Encryption Algorithms" المنشورة عام 2019 كرسالة تكميلية لبحث الماجستير بجامعة السودان للعلوم والتكنلوجيا قام الباحثون باختيار ثلاثة خوارزميات متماثلة (AES مع المفتاح (128) ، AES مع المفتاح (256) والسمك المنتفخ) ويمرر الملف الي برنامج يقوم بتقسيم الملف إلى ثلاث كتل بأحجام مختلفة واختيار خوارزميات عشوائياً لتشفير كتل من الملف قبل تحميل وحفظ معلومات عملية التشفير في قاعدة البيانات المحلية ، كما يقوم البرنامج بعملية فك التشفير عن طريق استرداد معلومات التشفير عملية فك تشفير الملف بعد تنزيله من التخزين السحابي، وقد ذكر الباحثون ان الأسلوب المقترح يوفر سرية البيانات بواسطة البرنامج .

2. 11 في دراسة Dheyab Salman Ibrahim (Ibrahim, 2019) بعنوان" Enhancing Cloud Computing Security using Cryptography & Steganography" المنشورة في مجلة " Iraqi Journal of Information Technology. V.9 N.3" العام 2019 ناقش الباحث بناء نظام برمجي يقوم بتشفير ثم إخفاء المعلومات الحساسة في الصور قبل ارسالها الى مركز تخزين البيانات في الحوسبة السحابية حيث استخدم خوارزميات DES & RSA لتشفير البيانات ثم إخفاء هذه البيانات المشفرة داخل الصور باستخدام تقنيات إخفاء المعلومات لإنتاج ملف صورة جديد يسمى stego-images مما ادي الي أمان عالٍ من أي هجمات من قبل المعارضين.

2. 12 في دراسة P. Chinnasamy & P. Deepalakshmi (Ponnusamy and Deepalakshmi, 2022) بعنوان "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud" المنشورة في مجلة "Journal of Ambient Intelligence and Humanized Computing " عام 2021 قام الباحثون بالتركيز علي السجلات الصحية إلالكترونية (EHRs) وتوفير آليات مناسبة للتحكم في الوصول الي هذه السجلات ولتوفير تخزين سحابي آمن ،اقترحو تنفيذ خوارزمية تشفير هجينة نستخدم فيها خوارزمية محسّنة لتوليد المفاتيح من RSA (IKGSR) لتشفير البيانات الصحية وخوارزمية السمكة المنتفخة لتشفير المفتاح ولك لإخفاء المعلومات لمشاركة المفاتيح عن طريق فهرسة السلسلة الفرعية وآلية البحث عن الكلمات الرئيسية لاسترداد البيانات

المشفرة بكفاءة، وبقياس الأداء والأمان فان الطريقة المقترحة مقارنة مع الطرق السابقة تؤكد النتائج بوضوح أنها توفر أمانًا أفضل وتسترد البيانات أيضًا بكفاءة.

13. 2 دراسة Ishaq Muhammed (Muhammed et al., 2021)واخرون بعنوان " Advanced Encryption Standard (AES) combined with Bit-Level Embedding for Securing Cloud Data" المنشور في مجلة " African Scholar Journal of African Sustainable Development (JASD-2)" عام 2021 قام الباحثون ولزيادة الأمان في الحوسبة السحابية باستخدام هجين من خوارزمية AES وتقنية Text Steganography وهي تقنية إخفاء رسالة في غلاف دون ترك مسار للرسالة الأصلية حيث يتم إخفاء المعلومات عن المراقب لإنشاء اتصال غير مرئي حيث اقترح الباحثون أولا تشفير البيانات بالخوارزمية AES ثم استخدام التقنية Text Steganography لاخفاء النص المشفر مما زاد عملية الأمان علي البيانات.

14. 2 في دراسة R. Denis (Denis and Madhubala, 2021) واخرون بعنوان " Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems" المنشورة في مجلة "Multimedia Tools and Applications "عام 2021 ناقش الباحثون ان انظمة التشفير الحالية وحدها ليست كافية للتعامل مع هذه المشكلات فتم اقتراح استخدام خوارزمية AES مع الخوارزمية RSA فاظهرت النتائج أن الخوارزمية المقترحة قادرة على نقل البيانات الطبية بأمان وذلك بمقارنة نتائج الخوارزمية الهجينة مع خوارزميات التشفير المفردة الأخرى من حيث المقاييس الإحصائية المختلفة ، أظهرت النتائج تفوق الخوارزمية المقترحة ، يمكن للنموذج المقترح أيضًا منع الهجمات ، مثل steganalysis أو هجمات RS .

15. 2 في دراسة P. Chinnasamy واخرون (Chinnasamy et al., 2021) بعنوان "on Cloud Computing " المشورة في كتاب Inventive Communication and Computational Technologies عام 2021 استخدم الباحثون لتحقيق أمان وسرية بيانات عالية في الحوسبة السحابية خوارزمية هجينةECC و Blowfish حيث تم مقارنة أداء النظام الهجين بالطريقة الهجينة الحالية ويظهر أن الطريقة المقترحة توفر أمانًا عاليًا وسرية للبيانات.حيث تم اقتراح استخدام التشفير الهجين للتغلب على عيوب الخوارزميات المتماثلة وغير المتماثلة.

5. مقارنة للدراسات السابقة

الجدول (1)يوضح مقارنة للدراسات السابقة

م	الكاتب	عنوان الدراسة	سنة النشر	خوارزميات التشفير	ملخص البحث
.1	Gaurav R. Patelواخرون	Hybrid Encryption Algorithm	2014	RSA Diffie Hellman	توفير مزيدًا من الأمان مقارنة بالخوارزميات الفردية التقليدية
.2	Er. Ashima Pansotra1 (Pansotra and Singh,	Cloud Security Algorithms	2015	DES - AES - Triple DES. RSA - Diffie-Hellman Key	خلصت الدراسة بعد المقارنة بين الخوارزميات والهجمات المستحدثة الي ان الخوارزميات

	(2015واخرو ن			Exchange Homomorphic	ليست آمنة وما زالت هناك حاجة لتعزيز أمن الخوارزميات.
.3	Priyadarshi ni Patil واخرون	2015	A Comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish	DES,3DES, AES, RSA and Blowfish	تم مقارنة الخوارزميات والتوصل الي ان الاكفأ هي RSA تميز Blowfish بالكفاءة في البرامج إذا كان الوقت والذاكرة عاملين رئيسيين في التطبيق
.4	**سناء بلغيث** واخرون	2015	Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm	AES RSA	توصلو الي ان الخوارزمية المهجنة اسرع في التشفير واقوي امانا
.5	Dr. D.I. George Amalarethi nam	2016	Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud	RSA	اقترح الباحثون طريقة تزيد من طول المفتاح المستخدم في خوارزمية RSA لجعل عملية التشفير قوية
.6	Fortine Mata	2017	Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)	AES Blowfish	بالخوارزمية الهجينة زادو من الموثوقية للبيانات كما تمت معالجة مشكلة ضمان سرية البيانات في السحابة ضد عمليات الوصول التي تتجاوز الحقوق المصرح بها.
.7	Madhumita Panda	2018	"A Comprehensive Evaluation of Cryptographic Algorithms: DES,	AES Blowfish DES RSA	تقدم هذه الورقة تقييمًا لكل من خوارزميات التشفير المتماثلة (AES، DES ، السمكة المنتفخة) وكذلك غير

		AES, RSA and Blowfish المنشورة " في مجلة " Internationl Journal of Scientific Research in Computer Science Applications and Management Studies			المتماثلة (RSA
.8	P.Chinnasa واخرون	"Design of Secure Storage for Health-care Cloud using Hybrid Cryptogrphy "	2018	RSA- Blowfish	ناقش الباحثون أهمية حماية البيانات الطبية والتي تتوفر على السحابة الالكترونية عن طريق استخدام تقنية تشفير هجينة من خلال دمج خوارزمية متماثلة وتشفير المفاتيح باستخدام خوارزمية غير متماثلة. أظهرت نتائج البحث ان الطريقة المقترحة توفر أمانًا أفضل من أي خوارزميات هجينة أخرى،كمان ان وقت تشفير وفك تشفير أقل مقارنةً بالتقنيات المتماثلة الأخرى
.9	K. R. Sajay واخرون	Enhancing the security of cloud data using hybrid encryption	2019	"التشفير المتجانس Homographic" وتشفيرBlowfish	استنتجت الدراسة الي ان العمل بهذه الطريقة قد حسن من الامن في السحابة

			algorithm		
.10	خباب مصط فى واخرون	Confidentiality of Data in Public Cloud Storage Using Hybrid Encryption Algorithms	2019	AES(128) AES(256) Blowfish	
.11	في دراسة Dheyab Salman Ibrahim	Enhancing Cloud Computing Security using Cryptography & Steganography	2019	استخدم خوارزميات DES & RSA لتشفير البيانات	إخفاء المعلومات لإنتاج ملف صورة جديد يسمى stego-images مما ادي الي أمان عالٍ من أي هجمات من قبل المعارضين.
.12	في دراسة P. Chinnasamy & P. Deepalakshmi	HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud	2021	RSA (IKGSR)	الطريقة المقترحة تؤكد بوضوح أنها توفر أمانًا أفضل وتسترد البيانات أيضًا بكفاءة
.13	Ishaq Muhammed واخرون	Advanced Encryption Standard (AES) combined with Bit-Level Embedding for Securing Cloud Data	2021	خوارزمية AES وتقنية Text Steganography	أولا تشفير البيانات بالخوارزمية AES ثم استخدام التقنية Text Steganography لاخفاء النص المشفر زاد عملية الأمان علي البيانات.
.14	Denis . واخرون	Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical	2021	خوارزمية AES مع الخوارزمية RSA	أظهرت النتائج تفوق الخوارزمية المقترحة في البيانات المختبرة يمكن للنموذج المقترح أيضًا منع الهجمات

			data communication over cloud-based healthcare systems		
15.	في دراسة P. Chinnasamy واخرون	Blowfish و ECC	2021	Efficient Data Security Using Hybrid Cryptography on Cloud Computing	قارن الباحثون بين طرق التشفير المعتادة والطريقة المهجنة حيث خلصو الا انها تحقق أمان وسرية بيانات عالية في الحوسبة السحابية.

6. **منهجية البحث:**

في هذا الورقة تم الوصول الي طريقة لدمج خوارزمية تأخذ نفس خصائص خوارزمية Blowfish كخوارزمية متماثلة تمتاز بالكثير من الخصائص و ولكنها تمتلك مفتاح عام يسهل التنبؤ به بعد عدد من المحاولات ولذلك لجأت محاولة دمج خوارزمية غير متماثلة RSA والتي تمتلك مفتاحين للتشفير وعند الدمج تم الوصول الي الخوارزمية التي تأخذ خصائص خوارزمية Blowfish من حيث السرعة واستخدام الذاكرة القليل ومن خوارزمية RSA طريقة توليد المفاتيح ويتم توليد المفاتيح بطريقة عشوائية متغيرة في كل مرة يتم تحميل الملف مما يجعل كسر هذا المفتاح والحصول عليه من قبل المهاجمين المتطورين اصعب كما يبين الجدول 1.

تم اختيار هذه الخوارزميتين وذلك بعد مراجعة الدراسات السابقة التي اثبت ان هذه الخوارزميتين هما الأسرع في عملية التشفير كما يتميز المفاتيح المولدة بها بانها تمتاز بسرية عالية كما انها من افضل الخوارزميات عندما يتم نقل البيانات ككتلة Packet بهذه الطريقة من اختيار الخوارزميتين ودمج تقنياتهما على تحسين المرحلة الأمنية العليا لتشفير قاعدة بيانات النص العادي ذات 64 بت. إلى جانب ذلك فأن طريقة تشفير Blowfish تتميز بالسرعة مما يجعل الخوارزمية الهجينة بها اسرع من التجارب السابقة وافضل من حيث الأمان والوقت اللازم للمعالجة حتي عند تغيير حجم Packet ولأنها تستغرق وقتًا قليلاً فهي تستهلك أقل قدر من الطاقة مما يجعلها من افضل الخوارزميات الهجينة من حيث الأداء.

7. **الخوارزمية المقترحة الهجينة RSA&Blowfish**

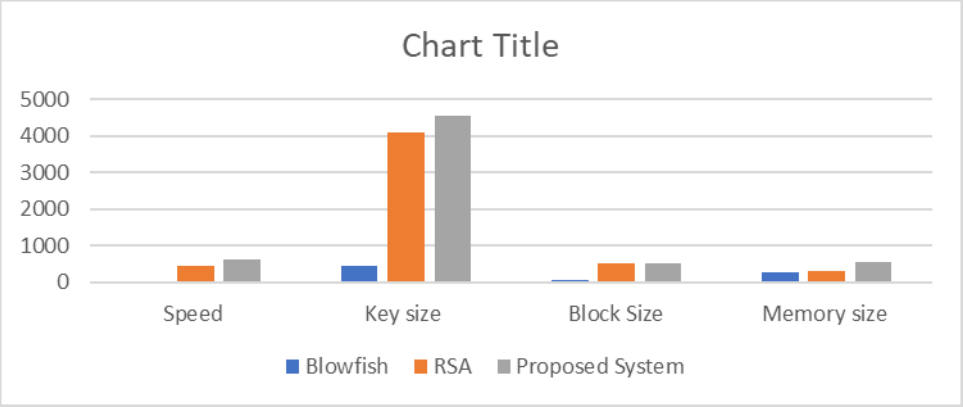
رغم قوة خوارزمية Blowfish الا انها تتعرض لهجوم عندما يكون حجم البلوك كبير نسبيا يتجاوز64 بت وعند مراجعة بعض الادبيات السابقة التي تم ذكرها في الباب الأول التي اوصت بعدم استخدام هذه الخوارزمية للمفات التي يتجاوز حجمها 4 قيقا ولذلك فقد تم التفكير في خوارزمية اخري تستخدم طريقة توليد المفاتيح في خوارزمية RSA وذلك بالتركيز علي المفتاح المستخدم بمضاعفة عدد المفاتيح في الجدول التالي4-1 تم توضيح الاختلاف بين 3 خوارزميات Blowfish و RSA بالإضافة الخوارزمية المطورة الجديدة New Blowfish.

تم انشاء ملف نص عادي وتشفيره باستخدام خوارزمية Blowfish ثم تشفيره باستخدام خوارزمية RSA ثم أخيرا تشفيره بالخوارزمية المهجنة للتوصل الي الاختلافات ما بين الخوارزميتين السابقتين والخوارزمية المهنجنة المقترحة.

جدول (2) الاختلافات بين الخوارزميات المقترحة المستخدمة مع الخوارزمياتBlowfish و RSA

الاختلافات	Blowfish	RSA	Proposed System
Speed	Slow encryption / decryption (1nn for 5kb file)	Fast in decryption and encryption(0.43nn for 5kb file)	Medium speed in decryption and encryption(0.62nn for 5kb file)
Memory size	9.38 kb	31.5 kb	6kb
Key size	From 32 bytes to 448 bytes,	From 515 to 4096	1088bytes
Block Size	64	variable-length block sizes	variable-length block size

في الجدول التالي3-1 تم توضيح الاختلاف بين الخوارزميات Blowfish و RSA بالإضافة الخوارزمية المطورة الهجينة حيث نجد ان توليد المفتاح يستغرق وقتًا أقل وذاكرة أقل ويتغير في كل مرة عند إرسال الملف في السحابة مما يمنح البيانات أمانًا قويًا ضد العديد من الهجمات ويجعل من عملية الاختراق حتي وان تمت مرة وعلي ملف واحد فأنه يجب تكرارها في كل مرة من جديد وعلي كل ملف بطريقة منفردة كما يوضحه الشكل (4-1).



الشكل(1) تحليل مقارنة الخوارزميات مع الخوارزمية الهجينة المقترحة

8. طريقة التشفير

يُنشئ النظام الجديد المقترح مفتاحين (لتطبيق عملية التشفير مرتين) لاستخدامهما في عملية التشفير وفك التشفير عن طريق إنشاء مثيل من فئة إنشاء المفاتيح ثم تحويل المفاتيح إلى مفاتيح سرية وهي إحدى تقنيات RSA. هذا مفيد للمفاتيح السرية الخام التي يمكن تمثيلها كمصفوفة بايت وليس لها معلمات رئيسية مرتبطة بها. عندما يقوم المستخدم بإدخال البيانات ليتم تشفيرها ، يطبق النظام المهجن المقترح عملية التشفير حيث في الاستدعاء الأول يتم تمرير المفتاح الأول والنص العادي. ثم في الاستدعاء الثاني يتم تمرير المفتاح الثاني والنص الذي يعود من عملية التشفير الأولى.

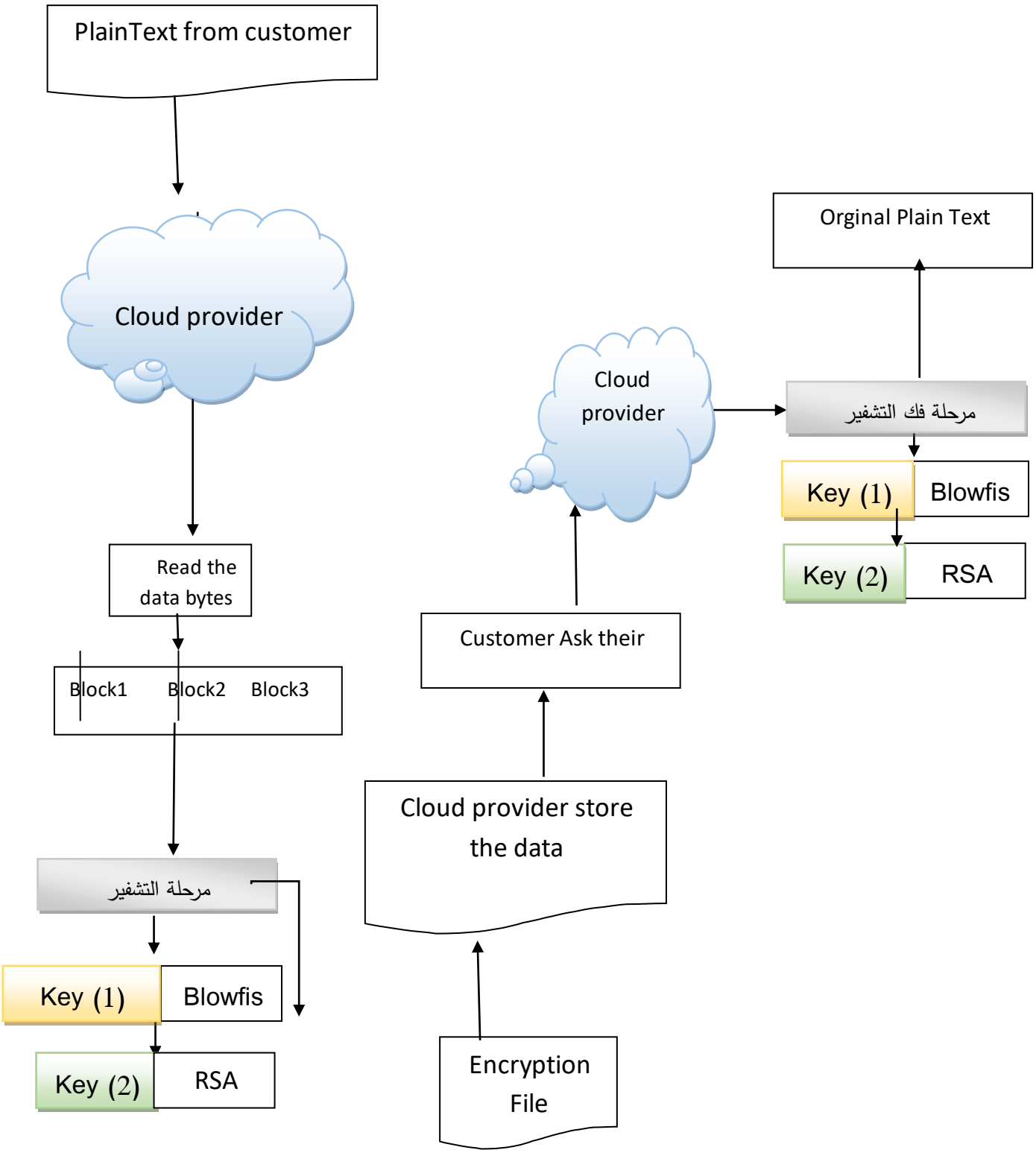
بعد الانتهاء من عملية التشفير ، يجب إعادة تهيئة مثيل التشفير في وضع فك التشفير عن طريق استدعاء دالة init (). تأخذ وظيفة Init () معلمتين: أوضاع التشفير: تحدد تفاصيل حول كيفية فك تشفير الخوارزمية و مفاتيح فك التشفير.

في فك التشفير ، تنطبق الوظيفة مرتين كما في عملية فك التشفير ففي الاستدعاء الأول لهذه الوظيفة يتم تمرير المفتاح الثاني والنص المشفر وفي الاستدعاء الثاني لهذه الوظيفة يتم تمرير المفتاح الأول والنص الذي يعود من عملية فك التشفير الأولى .

9. خطوات عملية التشفير

عندما يرغب مستخدم في التحميل أو تنزيل ملف من الحوسبة السحابية يجب أن يتم تمريره إلى برنامج تشفير حيث يتم تنفيذ عملية ترميز الملف عن طريق Blowfish ومفتاحها الوحيد ثم استخدام مفتاحين للتشفير يتم توليدهم عن طريق خوارزمية RSA وعند فك التشفير يتم استخدام المفاتيح التي تم استخدامها قبلا من خوارزمية RSA ثم المفتاح العام الخاص بخوارزمية Blowfish كما هو مبين في الشكل (2) بالخطوات التالية :

قراءة البيانات ثم تقسيم كتل البيانات ثم توجيه البيانات ثم توليد المفاتيح : يتم توليد مفتاح من خوارزمية blowfish بطول 64 bits ومفتاحين من خوارزمية RSA بطول bits1024 حيث ان المفتاحين يستخدما اطوال مناسبة لتقليل الزمن اثناء التشفير وفك التشفير وتقليل استخدام الذاكرة ثم يتم تطبيق الخوارزمية : يتم أولا إستخدام خوارزمية Blowfish المكتوبة بلغة جافا ،ثم يتم تطبيق عملية التشفير مرة اخري بتطبيق مفتاحين يتم توليدهم باستخدام خطوات خوارزمية RSA واستخدامهما في عملية التشفير وفك التشفير عن طريق إنشاء كائن من فئة إنشاء المفتاح واستدعاء دالة () getinstance لإنشاءه وفقًا لخوارزمية RSA حيث يتم تحديدها من خلال تمرير اسم الخوارزمية إلى دالة () getinstance. ثم تحويل المفاتيح الخاصة بخوارزمية RSA إلى مفاتيح سرية يتم بإنشاء كائنين من فئة التشفير لتشفير البيانات مرتين في جافا. استدعاء دالة () getinstanceمع تمرير إسم الخوارزمية المراد إستخدامها وقبل أن تتمكن من استخدام كائن تشفير ، يجب التهيئة في وضع التشفير عن طريق استدعاء دالة () init تأخذ الدالة () Init معاملين وهما: أوضاع التشفير: يحدد تفاصيل حول كيفية تشفير الخوارزمية. و مفتاح التشفير الأول، يتم فتح الملف الذي يوجد بداخله البيانات المراد تشفيرها.ويتم فتحه على نمط القراءة في هذه الخطوة يتم استدعاء الدالة () dofinal مرتين لتطبيق عملية التشفير مرتين. الاستدعاء الأول لهذه الدالة يتم تمرير المفتاح الأول والملف الذي يحمل البيانات المراد تشفيرها. الاستدعاء الثاني لهذه الدالة يتم تمرير المفتاح الثاني والبيانات التي تم تشفيرها في عملية التشفير الأولى ، بعد الانتهاء من عملية التشفير ، يجب إعادة التهيئة لكائن التشفير في وضع فك التشفير عن طريق استدعاء دالة() init تأخذ الدالة () Init معاملين وهما: أوضاع التشفير: يحدد تفاصيل حول كيفية فك تشفير الخوارزمية مفاتيح فك التشفير، يتم بعدها استدعاء الدالة () dofinal مرتين لتطبيق عملية فك التشفير مرتين. الاستدعاء الأول لهذه الدالة يتم تمرير المفتاح الثاني والنص المشفر. الاستدعاء الثاني لهذه الدالة يتم تمرير المفتاح الأول والنص الذي يعود من عملية فك التشفير الأول، ثم أخيرا حفظ بينات التشفير :يتم ارسال بيانات التشفير وتحميلها في قاعدة بيانات داخل السيرفر حيث يحتوي الملف المرسل علي طول كتلة البيانات ومفاتيح التشفير المستخدمة بالإضافة الي كتلة البيانات .



الشكل (2) يوضح منهجية البحث

10. النتائج

أسفرت نتائج البحث الي ما يلي :

1. تناول البحث مشاكل الأمان التي تواجه الخدمات السحابية وطرق التشفير المعتادة التي تتم علي البيانات للحفاظ علي سريتها وصحتها وقد اقترح الباحث لرفع مستوي السرية والتعقيد والتغلب علي مشكلة المفتاح الواحد الذي تتميز بها الخوارزميات المتماثلة عامة بدمج خصائص RSA مع Blowfish في توليد المفاتيح .
2. تم اختبار الملف المشفر بطريقة التشفير المهجنة المقترحة وكان أكثر حماية ضد هجوم القوة الغاشمة وهجوم (التشفير النصي فقط) بنسبة متوسطة (2.5%).
3. كما انه اقوي عند تعرضه لهجوم التعرف علي المفاتيح المستخدمة بنسبة متوسطة (1.9%) وذلك بعد اختباره باستخدام نظام kali لتنفيذ الاختبارات .
4. تم الاستخلاص الي ان طريقة التشفير المهجنة المقترحة توفر تحسين وحماية وضمان لصحة البيانات ضد الهجمات المعروفة لأن الطريقة المقترحة جمعت ما بين مميزات Blowfish و RSA من حيث طريقة توليد المفاتيح مما جعل طول المفتاح اكبر كما ان ميزة تغير المفتاح في كل عملية تشفير جديدة إضافة ميزة امان اكبر علي الملف بنسبة متوسطة (4%).

11. التوصيات :

بناءً على نتائج البحث ، هناك عدة توصيات تم التوصل إليها وهي:

1. دمج خوارزمية Blowfish مع خوارزمية أخرى ومقارنة الخوارزمية الجديدة مع الخوارزمية المقترحة من حيث الأداء والسرعة.
2. استخدام أدوات أخرى لقياس سرعة واداء الخوارزمية المقترحة وذلك للتأكد من مميزات الخوارزمية الهجينة.
3. تعزيز هذا العمل من خلال زيادة اختبارات مستوى أمان الخوارزمية الهجينة عند تعرضها لانواع هجوم اخري غير التي تواجه الخوارزميتنين RSA و Blowfis باستخدام طرق إحصائية للعثور على قوة الأمان.
4. اقتراح مخطط توزيع رئيسي جديد يهدف إلى منح كل مستخدم مصرح له مفتاح التشفير دون تفاعل مزود السحابة مما يزيد من مستوي الثقة للانتقال الي السحابة .
5. دمج طريقة لإخفاء المفاتيح في المستقبل، لحل مشكلة توزيع المفاتيح اثناء فك التشفير وذلك بدمج خوارزمية لإخفاء المعلومات ومقارنته بالطريقة الهجينة الحالية.

المراجع

1. Belguith, S., Jemai, A., Attia, R., 2015. Enhancing data security in cloud computing using a lightweight cryptographic algorithm, in: 11th International Conference on Autonomic and Autonomous Systems. pp. 98–103.

2. Chinnasamy, P., Deepalakshmi, P., 2018. Design of secure storage for health-care cloud using hybrid cryptography, in: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, pp. 1717–1720.

3. Chinnasamy, P., Padmavathi, S., Swathy, R., Rakesh, S., 2021. Efficient Data Security Using Hybrid Cryptography on Cloud Computing, in: Inventive Communication and Computational Technologies. Springer, pp. 537–547.

4. Denis, R., Madhubala, P., 2021. Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimed. Tools Appl. 80, 21165–21202. https://doi.org/10.1007/s11042-021-10723-4

5. Full Text, n.d.Ibrahim, D.S., 2019. Enhancing Cloud Computing Security using Cryptography & Steganography. Iraqi J. Inf. Technol. V 9, 2018.

6. Mata, F., Kimwele, M., Okeyo, G., 2015. Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish) 6, 8.

7. Mohammed, K.M.A.-K., Supervisor, -Faisal Mohammed, 2019. Confidentiality of Data in Public Cloud Storage Using Hybrid Encryption Algorithms (Thesis). Sudan University of Science & Technology.

8. Muhammed, I., Abubakar, F.A., Jibrin, A.A., Aliyu, A.Y., Yusuf, S., Abashe, U.S., 2021. Advanced Encryption Standard (AES) combined with Bit-Level Embedding for Securing Cloud Data 10

9. Panda, M., n.d. A Comprehensive Evaluation of Cryptographic Algorithms: DES, AES, RSA and Blowfish 7, 4.

10. Pansotra, E., Singh, S.P., 2015. Cloud Security Algorithms. Int. J. Secur. Its Appl. 9, 353–360. https://doi.org/10.14257/ijsia.2015.9.10.32

11. Patel, G.R., Panchal, K., 2014. Hybrid Encryption Algorithm 2, 7.

12. Ponnusamy, C., Deepalakshmi, P., 2022. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. J. Ambient Intell. Humaniz. Comput. 13, 1–19. https://doi.org/10.1007/s12652-021-02942-2

13. Sajay, K.R., Babu, S.S., Vijayalakshmi, Y., 2019. Enhancing the security of cloud data using hybrid encryption algorithm. J. Ambient Intell. Humaniz. Comput. 1–10.