وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

خوارزمية السمكة المنتفخة المعدلة للاستخدام في السحابة

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة ماجستير علوم في
علوم الحاسوب

من قبل

شامل عزالدين نجم عبدالله

بإشراف

م.د. عدي هاشم سعيد

1444 هـ

2023 م

الملخص

التشفير هو وسيلة تُستخدم لحماية المعلومات، من السرقة أو التزوير أو أي حدث غير شرعي من قبل الأشخاص غير المخولين، يحتل هذا العلم اليوم مكانة بارزة بين العلوم، وله الكثير من التطبيقات في مجالات الحياة المختلفة. التشفير الكتلي هو أحد أنواع أنظمة التشفير الحديثة حيث يشفر كتلة بحجم ثابت من البيانات، تعد خوارزمية السمكة المنتفخة Blowfish من أبرز خوارزميات التشفير الكتلي، حيث تشفر كتلة بحجم 64 بت، بمفتاح متناظر متغير الطول (32–448 بت). الحوسبة السَحابِية هي وَسيلة لنشْر خَدمات الكُمبيوتر مثل الخَوادْم والتَخزين وقَواعد البَيّانات عَبر الإنتَرنِت من أجل تَوفير إبتكار أسرع ومَوارد أكثر مُرونة، وإقتصادية في الحَجم والكُلفة. أصبحت الخدمات التي توفرها السَحابة أكثَر أهمية، وتَكتَسب زخمًا في العالَمَين الأكاديمي والتِقَني. على الرغم مِن وجود مَزايا عَديدة في إستخدام التقنيات السَحابية، إلّا أنه يواجه بَعض العَوائق الكبيرة، يُعد الأمن أحد أهم العَوائق التي تَحوّل دونَ إستخدامها بِصورة فعالة، تَلعب خَوارزميات التشفير دوراً رئيسياً في أنظمة الحِمايَة في السَحابة. ولكن العَمليات داخل السَحابة تَتَطَلَّب سُرعة عالية في عمليات التَشفير و فَك التَشفير، لأن الخَوادم الخاصة بالسَحابة تُعالج كَمية كَبيرة مِن البَيانات، فضلاً عن أنهُ يَتَطَلب مِستوى عالٍ مِن الأمنية.

يهدُف البَحِث إلى إقتراح نَهج مُعدل لخوارزمية السَمَكة المُنتفِخة (Blowfish) تمت تسميته بـ Modified Blowfish Algorithm (MBA)، لتُلائم قيود العمْل في السَحابةِ مِن ناحية السُرعة والأمان لتَوفير الأمن السَحابي. وذلك بالتَعديلِ عَلى وَظيفة الخَوارزمية والمُتمثلة بِصناديقِ الاستبدال (S–Boxes)، فضلاً عن تَعديل بُنية الخَوارزمية والمُتمثلة بشَبكة فيستل Feistel. في هذا البَحث تم تَنفيذ خوارزمية Blowfish الأصلية، كما تم إجراء تَجارب الأداء للحصول عَلى النتائج مِثل وَقت التَشفير ووَقت فَك التَشفير والإنتاجية. ومن ثمَّ تم إقتراح الخوارزمية المعدلة (MBA) بِما يُلائِم العَمَل في البيئة السَحابية، تَمَ تَنفيذ خوارزمية (MBA) فضلاً عن إجراء تجارب الأداء والفُحوص الأمنية وِفق مَقاييس الأمان القِياسية العالَمية مِثل مَقاييس التَحليل الإحصائي (NIST) و تأثير الإنهيار للحصول على النتائِج الّتي تُحدد مَعايير الأداء مِثل وَقت التَشفير ووَقت فَك التشفير ومعدل الإنتاجية.

أظهرت النتائِج تَفوق الخَوارزمية المُعدلة (MBA) بِالمُقارنة مع الخَوارزمية الأصلية مِن حَيث وَقت التَشفير ووقت فَك التَشفير والإنتاجية. فضلاً عن ذلك فَقَد بينت نتائِج مَقاييس الأمان أن الخَوارزمية المُعدلة ذات مستوى أمني عالٍ، بِما يَخدم الهَدَف مِن هذا البَحث.

Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and Mathematics
Department of Computer Science

A Modified Blowfish Algorithm to be Used in the Cloud

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul**

**as a Partial Fulfillment of Requirements
for the Degree of Master of Science
in
Computer Science**

By

Shamil Ezadeen Najim Abdullah

Supervised by

Lecturer Dr. Auday Hashim Saeed

2023 A.D. **1444 A.H.**

Abstract

Encryption is a method used to protect information from theft, forgery, or any illegal event by unauthorized persons. Today, this science occupies a prominent place among sciences, and it has many applications in different fields of life. A block cipher is one of the types of modern cryptographic systems that encrypts a fixed size block of data. The Blowfish algorithm is one of the most prominent block cipher algorithms, as it encrypts a 64-bit block, with a symmetric key of variable length (32-448 bits). Cloud computing is a means of deploying computer services such as servers, storage, and databases over the Internet in order to provide faster innovation, more flexible resources, and economics in scale and cost. The services provided by the cloud are becoming more important and gaining momentum in the academic and technical worlds. Although there are many advantages in using cloud technologies, it faces some major obstacles. Security is one of the most important barriers that prevent its effective use. Encryption algorithms play a major role in protection systems in the cloud. But operations within the cloud require high speed in encryption and decryption operations, because cloud servers process a large amount of data, in addition to that it requires a high level of security.

The thesis aims to propose a modified approach to the Blowfish algorithm, called the Modified Blowfish Algorithm (MBA), to fit the limitations of working in the cloud in terms of speed and security to provide cloud security. This is done by modifying the algorithm's function represented by S-Boxes, as well as modifying the structure of the algorithm represented by the Feistel network. In this research, the original Blowfish algorithm was implemented, and performance experiments were performed to obtain results such as encryption time, decryption time, and throughput. Hence, the modified algorithm (MBA) was proposed to suit the work in the cloud environment. The (MBA) algorithm was implemented, as well as performance experiments and security tests were conducted in accordance with international standard security measures such as the Statistical Analysis Standards (NIST) and the avalanche effect to obtain the results that define the measures. Performance such as encryption time, decryption time, and throughput.

The results showed the superiority of the modified algorithm (MBA) compared to the original algorithm in terms of encryption time, decryption time and throughput. In addition, the results of the security measures showed that the modified algorithm has a high security level, which serves the purpose of this research.