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

Enhancing Homomorphic Encryption for Privacy Service in Cloud Computing

**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 Doctor of Philosophy in
Computer Science**

By

Saja Jasem Mohammed Kado

Supervised by

Prof. Dr. Dujan Basheer Taha

2022 A.D. **1443 A.H.**

Abstract

Homomorphic encryption is one of the most popular technologies that assist in keeping the confidentiality and privacy of user data on cloud computing storage. It has the ability to apply a mathematical operations on the ciphertext and return the same result when applying the same operation on the plaintext. Paillier's cryptosystem is one of the partial homomorphic encryption algorithm that used to ensure data privacy in cloud storage. Paillier cryptosystem suffers from some drawbacks that makes some researchers avoid it. One of these drawbacks is its bottleneck, which appears clearly in the decryption process and affects its performance due to the delay that is caused, especially when deals with large amount of information.

This thesis offers solutions to the problem of the Paillier cryptosystem (using Python 3.8 programming language) that operates to improve its performance. As well, it adds other levels of secrecy to increase the strength of the algorithm. The improvements have adopted several directions and formed four proposed algorithms to improve the performance of Paillier algorithm. EPEA-1 is the first version, and it was designed to improve the security of the Paillier cryptosystem. It enhances the original Paillier method by selecting the best-expected key to utilize in the process and scattering the resulting ciphertext using a proposed technique based on chaotic system. EPEA-2 was designed to enhance algorithm speed by utilizing many collected concepts. EPEA-3 is a hybrid of the two preceding versions (EPEA-1 and EPEA-2). It combines the extra secrecy and the time speed up in a single algorithm to produce a fast and strong new method. Last but not least, EPEA-4 eliminated the delay produced by long key pairs, which reflects on the time of decryption and exacerbates the bottleneck problem of the original Paillier. One of the proposed algorithms (EPEA-3) was chosen to be used in the development of a cloud-based system for managing a secure Electricity Bills Payment Management System (EBPMS). It has been practically and effectively applied on a real cloud.

The proposed algorithms were tested by a number of measures to determine the efficiency of the proposed algorithms. According to the results of the test, EPEA-1 algorithm achieves (in various cases) a

randomness p-value (0.0590) as a minimum and a negative correlation (0.1242) as a worst-case, which proved the high randomization occurred to the ciphertext. When time reduction is taken into consideration, results showed that the proposed algorithms EPEA-2, EPEA-3, and EPEA-4 achieved the desired goal of decryption time reduction, EPEA-2 and EPEA-3 in key size less than 1024 bit, and EPEA-4 in larger key sizes up to 4kb. In key size 265 (for example) the decryption time in EPEA-2 and EPEA-3 was 0.001sec, whereas it was in EPEA-4, 6.83 e-05 sec (with 4 primes). EPEA-3 can be the best-proposed algorithm because it achieves secrecy with low consumed time, which can qualify it for use in practical implementations to secure the cloud storage.

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

تحسين التشفير المتماثل لخدمة الخصوصية في الحوسبة السحابية

اطروحة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة دكتوراه فلسفة في
علوم الحاسوب

من قبل

سـجى جـاسم محمد قـدو

بإشراف
أ.د. دجـان بشـير طـه

١٤٤٣ هـ ٢٠٢٢ م

الخلاصة

يعد التشفير المتجانس أحد أكثر التقنيات شيوعًا والتي تساعد في الحفاظ على سرية وخصوصية بيانات المستخدم في بيئة التخزين السحابية. اذ يتميز بقدرته على تطبيق العمليات الرياضية على النص المشفر وإرجاع الناتج للمستخدم بحيث يكون مطابق للناتج فيما لو تم تطبيق نفس العملية على النص الصريح. نظام Paillier للتشفير هو احد خوارزميات التشفير المتجانس الجزئي والذي يستخدم لضمان خصوصية البيانات في السحابة. يعاني نظام التشفير Paillier من بعض العيوب التي تجعل عدد من المستخدمين يتجنبون استخدامه. أبرز هذه العيوب هو عنق الزجاجة الذي يظهر بوضوح في عملية فك التشفير ويؤثر على أدائها بسبب التأخير الذي يحدث ، خاصة عند التعامل مع كمية كبيرة من المعلومات.

تقدم هذه الأطروحة حلولاً لمشكلة نظام تشفير Paillier (باستخدام لغة بايثون البرمجية الاصدار 3.8) بحيث تعمل على تحسين أدائه. بالإضافة إلى ذلك ، أضافت مستويات أخرى من السرية لزيادة قوة الخوارزمية. اعتمدت التحسينات عدة اتجاهات وشكلت أربع خوارزميات مقترحة لتحسين أداء خوارزمية Paillier .خوارزمية EPEA-1 هو الإصدار الأول ، تم تصميمه لتحسين أمان نظام تشفير Paillier فهو يعمل على تعزيز سرية الخوارزمية الأصلية عن طريق اختيار أفضل مفتاح متوقع لاستخدامه في العملية وتشتيت النص المشفر الناتج باستخدام تقنية مقترحة معتمدة على نظام الفوضى. EPEA-2 تم تصميمها لتحسين السرعة من خلال استغلال مجموعة من المفاهيم ، اما EPEA-3 فهي مزيج من الخوارزميتين السابقتين EPEA-1 و EPEA-2 فهي تجمع بين تعزيز السرية وتسريع الوقت في خوارزمية واحدة لإنتاج طريقة جديدة سريعة وقوية. أخيرًا وليس اخراً، ألغى EPEA-4 التأخير الناتج في الخوارزمية اثناء استخدام المفاتيح الطويلة في عملية التشفير، والذي ينعكس على وقت فك التشفير ويؤدي إلى تفاقم مشكلة عنق الزجاجة في خوارزمية Paillier الأصلية. تم اختيار إحدى الخوارزميات المقترحة (EPEA-3) لاستخدامها في تطوير نظام قائم على السحابة لإدارة نظام إدارة سداد فواتير الكهرباء اذ تم تطبيقه عمليًا وبفاعلية على سحابة حقيقية.

تم اختبار الخوارزميات المقترحة عمليًا واعتماد عدد من الإجراءات لتحديد كفاءة الخوارزميات المقترحة. وفقًا لنتائج الاختبار ، تحقق خوارزمية EPEA-1 وفي حالات مختلفة مدى عشوائية 0.0590 كحد أدنى وارتباط (0.1242-) كأسوأ حالة ، مما أثبت ارتفاع نسبة العشوائية التي حدثت للنص المشفر. عند أخذ تقليل الوقت في الاعتبار ، أظهرت النتائج أن الخوارزميات المقترحة EPEA-2 و EPEA-3 و EPEA-4 حققت الهدف المنشود لتقليل وقت فك التشفير و EPEA-2 و EPEA-3 في حجم مفتاح أقل من 1024 بت ، و EPEA-4 بأحجام مفاتيح أكبر تصل إلى 4 كيلوبايت. في حجم المفتاح 265 (على سبيل المثال) ، كان وقت فك التشفير في خوارزميتي EPEA-2 و EPEA-3 مساوي لـ0.001 ثانية ، بينما كان في EPEA-4، 6.83 e-05 ثانية (مع 4 أعداد أولية). يمكن أن تكون EPEA-3 هي أفضل خوارزمية مقترحة لأنها تحقق السرية مع انخفاض الوقت المستهلك، مما يجعلها مؤهلة للاستخدام في التطبيقات العملية لتأمين التخزين السحابي.