University of Mosul
College of Computer Science
and Mathematics

Developing a Cloud-Based Banking Application using Paillier Homomorphic Encryption

Muna Mohammed Saeed Altaee

M.Sc. / Thesis

Computer Science

Supervised by

Assistant Prof. Dr. Mafaz Mohsin Khalil Alanezi

2020 A.D. 1442 A.H.

Abstract

The Cloud Computing refers to provide services of storing, managing, and processing data and programs over the networks such as “Internet”. In recent years, the trend has increased for the use of Cloud Computing, which provides broad capabilities with sharing resources, and thus it is possible to store and process data in the cloud remotely, but this (cloud) is untrusted because some parties can connect to the network such as the internet and read or change data because it is not protected. Therefore, protecting data security and privacy is one of the challenges that must be addressed when using Cloud Computing. Encryption is interested in the field of security and privacy of information that are sent by a secure connection between individuals or institutions regardless of the method used to prepare this connection. But using the traditional encryption methods to encrypt the data before sending it will force the data provider to send his private key to the server to decrypt the data to perform computations on it. In this work we present a proposal to secure banking data transmission through the cloud by using partially Homomorphic Encryption algorithm (paillier algorithm) that allows performing mathematical operations on encrypted data without the need for decryption. A proxy server will be also used for performing Re-encryption process to enhance the security.

Banking application was implemented using the Python programming language. An application is designed for the bank through which the banker sends the database of customers to the cloud and is stored inside the storage server as encrypted data using the Paillier algorithm by 128 bit key.

As for the second party, the application of the customer which communicates with the cloud and through which the customer can know his balance or make withdrawing process from his balance and what follows this process from

mathematical operations that are executed on encrypted data without the need to decrypt it.

The proxy server was used to improve security as it only connects to the storage server and does not communicate with any other party. It is also performs the process of re-encrypting data with the customer's public key so that only the customer can decrypt the data because he is the only one who has the private key.

After implementation and analyzing the results, this model demonstrated its ability to overcome the security problems experienced by banks that rely on Cloud Computing, such as privacy and security problems. Thus, Cloud Computing services were invested in shorter time.

جامعة الموصل

كلية علوم الحاسوب والرياضيات

تطوير تطبيق مصرفي قائم على السحابة

باستخدام تشفير بايلر المتماثل

منى محمد سعيد خليل الطائي

رسالة ماجستير

علوم الحاسوب

بإشراف

أ. م. د. مفاز محسن خليل العنزي

١٤٤٢هـ ٢٠٢٠ م

الخلاصة

تعتبر الحوسبة السحابية حوض غني بالمصادر التي يمكن استخدامها ومشاركتها عبر شبكة اتصال داخلية او خارجية مثل "الانترنت"، حيث يمكن الاستفادة منها للحصول على خدمات تخزين وإدارة ومعالجة البيانات وتصميم التطبيقات ونشرها عبر المنصات. في السنوات الأخيرة اتجهت الشركات والمؤسسات بصورة متزايدة لاستخدام الحوسبة السحابية، ولكن السحابة تعتبر طرف ثالث غير موثوق بسبب امكانية العديد من الاطراف من الاتصال بالشبكة وقراءة البيانات أو تغييرها لأنها غير محمية ، وبالتالي فإن حماية أمن البيانات وخصوصيتها هي أحد اهم التحديات التي يجب معالجتها عند استخدام الحوسبة السحابية.

يهتم التشفير بمجال أمن وسرية المعلومات التي يتم إرسالها بين الأفراد أو المؤسسات بغض النظر عن الطريقة المستخدمة لإعداد هذا الاتصال. ولكن استخدام طرق التشفير التقليدية لتشفير البيانات قبل إرسالها سوف يجبر مزود البيانات على إرسال مفتاحه الخاص إلى الخادم لفك تشفير البيانات لإجراء عمليات رياضية عليها. من خلال هذا العمل، نقدم اقتراحًا لتأمين نقل البيانات المصرفية عبر السحابة باستخدام خوارزمية التشفير المتماثل (خوارزمية Paillier) التي تسمح بتنفيذ العمليات الرياضية على البيانات المشفرة دون الحاجة إلى فك التشفير. سيستخدم خادم الوكيل أيضًا لإجراء عملية إعادة التشفير لتعزيز الأمان.

تم تنفيذ التطبيق المصرفي باستخدام لغة البرمجة Python حيث تم تصميم تطبيق للبنك الذي يرسل من خلاله المصرفي قاعدة بيانات العملاء إلى السحابة ويتم تخزينه داخل خادم التخزين كبيانات مشفرة باستخدام خوارزمية Paillier بواسطة مفتاح طوله ١٢٨ بت.

أما بالنسبة للطرف الثاني (تطبيق العميل) الذي يتواصل مع السحابة ومن خلاله يمكن للعميل معرفة رصيده أو إجراء عملية سحب مبلغ من رصيده وما يلي هذه العملية من العمليات الرياضية التي يتم تنفيذها على البيانات المشفرة دون الحاجة إلى فك تشفيرها.

تم استخدام الخادم الوكيل لتحسين الأمان لأنه يتصل فقط بخادم التخزين ولا يتواصل مع أي طرف آخر وينفذ عملية إعادة تشفير البيانات باستخدام المفتاح العام للعميل، حيث يمكن للعميل فقط فك تشفير البيانات لأنه هو المالك الوحيد للمفتاح الخاص.

بعد تنفيذ النتائج وتحليلها ، أظهر هذا النموذج قدرته على التغلب على مشاكل الأمان والخصوصية التي تواجهها البنوك التي تعتمد على خدمات الحوسبة السحابية، وبالتالي تم استثمار خدمات الحوسبة السحابية للحصول على نتائج افضل في وقت اقصر وجهد اقل.