ملخص رسالة ماجستير بعنوان

تعزيز أمن التخزين السحابي باستخدام التشفير وإخفاء المعلومات

اسم الطالب

م.مريم عمّار يوسف

المشرف

د.وسيم موسى السمارة

المشرف المشارك

لايوجد

القسم والاختصاص

هندسة الحواسيب والأتمتة

حواسيب وأتمتة

الملخـــــص

يهدف البحث إلى تعزيز أمن التّخزين السّحابي باستخدام التّشفير وإخفاء المعلومات و يتناول البحث دراسة أداء خوارزميات التّشفير AES,DES,RSA ودرجة الأمان الناتجة عن استخدام هذه الخوارزميات في تشفير الملفات حيث تمّ اقتراح وتنجيز نظامين مختلفين لتعزيز أمن تخزين الملفات على السّحابة، الأوّل من أجل إدارة الملفات الخاصة بالمستخدم نفسه يتعامل مع الرّقم التّسلسلي الخاص بالهاتف المحمول للمستخدم كمفتاح لتشفير وإدارة الملفات على السحابة باستخدام التّشفير المختلط بعد تقسيم الملف أمّا الثاني من أجل إدارة الملفات المشتركة بين مجموعة المستخدمين ضمن مجموعة العمل حيث تم بناء نظام مخدّم وعميل يستخدمون التشفير والتوقيع الرقمي لتبادل الملفات بينهما وتم تعريف مجموعة عمل وإضافة مستخدمين ضمن المجموعة حيث لا يمكن لأي مستخدم من خارج مجموعة العمل الوصول إلى الملفات الخاصة بالعمل وعند قيام أي مستخدم ضمن مجموعة العمل بإجراء تعديل على الملفات الخاصة بالعمل وتوقيعها يتم إظهار صاحب آخر تعديل على الملفات ممّا يضمن عدم تعديل أي ملف وتشفيره دون معرفة صاحب آخر تعديل والمالك الأصلي للملف ويمكن فك تشفير الملفات لأي شخص ضمن مجموعة العمل دون الرّجوع لمالك الملف الأصلي علماً أنّه في كل مرة يتم فيها القيام بأي عمليّة من العمليات المتاحة ضمن النظام يتم التّحقق من عدم تعديل الملف في الفترة بين توقيع الملف والتحقق منه.

أثبت البحث أنّه يمكن حماية مفاتيح التشفير المتبادلة باقتراح بروتوكول لجعل عمليّة تبادل المفاتيح أكثر أماناً مع زيادة الزمن اللازم لكسر التّشفير، بالإضافة إلى فعاليّة استخدام التّشفير المختلط والتوقيع الرّقمي وتأمين الحمايات الأمنيّة الضّروريّة للحد من الوصول غير المشروع للملفات لأي شخص خارج مجموعة العمل أو القيام بأي تعديل على الملفات دون معرفة مالك الملف الأصلي بالإضافة إلى المرونة في التّعامل مع تشفير وفك تشفير الملفات المشتركة.

Master's thesis summary entitled

Enhancing Cloud Storage Security using Cryptography and Steganography

Student Name

Maryam Ammar Yousef

Co-Supervisor

-

Supervisor

Dr. Eng. Wasim Samara

Department

Computer and Automation Engineering

Summary

The research deals with studying the performance of AES, DES, and RSA encryption algorithms and the degree of security resulting from using these algorithms to encrypt files.Two different systems were proposed and implemented to enhance the security of storing files on the cloud, the first is for managing the user's own files, which treats the user's mobile phone serial number as a key to encrypt and manage files on the cloud using hybrid encryption after splitting the file, the second is to manage files shared between a group of users within the work group, where a server and client system was built that uses encryption and digital signature to exchange files between them. A work group was defined and users were added within the group, as no user from outside the work group can access the work files. If any user within the work group makes a modification to the work files and signs them, the owner of the last modification to the files is shown, which ensures that no file is modified and encrypted without the knowledge of the owner of the last modification and the original owner of the file. Files can be decrypted by anyone within the work group without consulting the original file owner. Note that every time any of the operations available within the system is performed, it is verified that the file has not been modified in the period between signing the file and verifying it.