جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تعزيز أمن التخزين السحابي باستخدام التشفير وإخفاء المعلومات

Enhancing Cloud Storage Security using Cryptography and Steganography

م.مريم عمار يوسف
د.وسيم موسى السمارة

الملخص

يهدف البحث إلى تعزيز أمن التخزين السحابي 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.

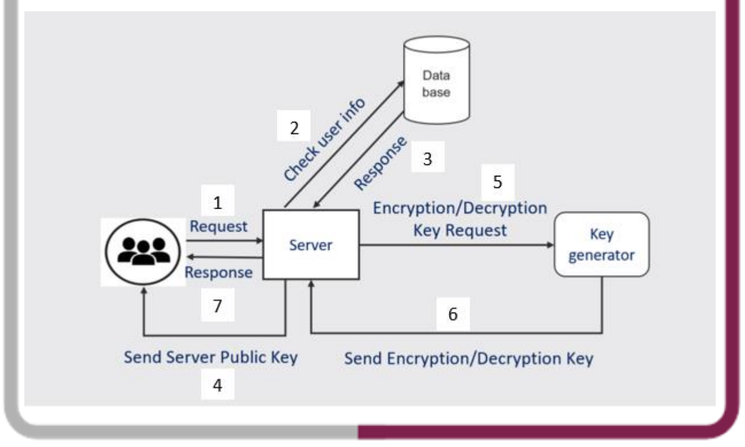
القسم العملي

تم بناء نظام للاستخدام الشّخصي حيث تم استخدام الرقم التسلسلي الخاص بالهاتف من أجل توليد مفاتيح التشفير بحيث يتم استدعاء توابع محدّدة بناء على خيار المستخدم وذلك باستخدام لغة البرمجة python، حيث أنّ الخيارات المتاحة عبر واجهة المستخدم هي التّشفير Encrypt، فك التّشفير Decrypt، رفع ملف إلى الحساب السّحابي Upload file بالإضافة إلى تحميل ملف من الحساب السّحابي Download file.

تم بناء نموذج يتيح تشفير الملفات والتّحقّق منها وتوقيعها وفك تشفيرها ضمن الصّلاحيات المُتاحة دون الرّجوع لمالك الملف الأصلي بالإضافة إلى التّحقّق من الملفات باستخدام توقيع محفوظ وتحديث الملفات لأي شخص ضمن مجموعة العمل المحدّدة فقط مع بيان صاحب آخر تعديل على الملف ولا يتيح لأي شخص خارج مجموعة العمل بالوصول إلى الملفات الخاصة بمجموعة العمل أو إجراء أي تعديل، بالإضافة إلى إمكانيّة إضافة مستخدم جديد وتحميل أو رفع الملفات من وإلى السّحابة علماً أنّه تم استخدام قناة إتصال مشفّرة آمنة بين المخدّم والعميل.

القسم العملي

يوضّح الشّكلمخطّطاً لعمل النّظام المنجز بشكل عام حيث يقوم العميل بتسجيل الدّخول وإرسال طلب إلى المخدّم بناء على الخيارات المتاحة فيقوم المخدّم بالتّحقّق من معلومات العميل من خلال قاعدة البيانات الموجودة لديه، فإذا نجحت عمليّة التّحقّق من معلومات العميل يقوم المخدّم بإرسال مفتاح التّشفير العام الخاص بالمخدّم للعميل ومن ثم توليد مفاتيح التّشفير أو فك التّشفير وفقاً لطلب العميل من خلال مولّد المفاتيح وإرسال المفاتيح للمخدّم والذي يقوم بإرسال مفاتيح التّشفير للعميل لاستكمال عمليّة التّشفير أو فك التّشفير.



القسم النظري

تزايد إستخدام الحوسبة السحابية مؤخراً، حيث توجهت كبرى شركات تكنولوجيا المعلومات إلى تبني وتطبيق فكرة الحوسبة السحابية، فأصبحت تؤجر موارد الحوسبة وموارد التخزين الموجودة في مراكز البيانات الخاصة بها، وكانت أولى هذه الشركات شركة أمازون Amazonذات سحابة EC 2 تلتها شركة مايكروسوفت Microsoftالتي زودت مستخدميها بمنصة سحابية عرفت بـ Windows Azure، بعدها جاءت شركة Apple بخدمة الحوسبة السحابية iCloud ثم حذا حذوهم شركة أوراكل Oracleو شركة غوغل Googleوغيرهم من الشركات الأخرى.

النتائج والمناقشة

النتائج المستخلصة في هذه المرحلة من البحث تبيّن أنّ: استخدام الخوارزميات AES,DES في نظام هجين Hybridلن يؤدّي إلى تغير زمن التشفير وفك التشفير وهذه النتائج متوافقة مع الدراستين البحثيتين [(Maitri. P, Verma.A, 2016)، (Padmavathi. B, Ranjitha. S, 2013)

تم 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 يتم إظهار صاحب أخر تعديل على الملفات ممّا يضمن عدم تعديل أي ملف وتشفيره دون معرفة صاحب أخر تعديل والمالك الأصلي.

المراجع

] Poduval, A., Doke, A., Nemade, H., & Nikam, R. (2019). Secure file storage on cloud 1[using hybrid cryptography. International Journal of Computer Science and Engineering, 7(01), 587-591.

] Srivalli, B. S. S., & SwarupMedikonda, B. (2019). Development of a Cloud-based 2[Secure Text File Application using Hybrid Cryptography and Steganography. International Journal of Recent Technology and Engineering (IJRTE), 8(1), 3267-3271.

] Kanatt, S., Jadhav, A., & Talwar, P. (2020). Review of secure file storage on cloud using 3[hybrid cryptography. International Journal of Engineering Research & Technology (IJERT), 9(2), 16-20.

] Poduval, V., Koul, A., Rebello, D., Bhat, K., & Wahul, R. M. (2020). Cloud based 4[secure storage of files using hybrid cryptography and image steganography. International Journal of Recent Technology and Engineering (IJRTE), 8(6), 665-667.

جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تعزيز أمن التخزين السحابي باستخدام التشفير وإخفاء المعلومات

Enhancing Cloud Storage Security using Cryptography and Steganography

م.مريم عمار يوسف
د.وسيم موسى السمارة

الملخص

يهدف البحث إلى تعزيز أمن التخزين السحابي 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.

القسم النظري

تزايد استخدام الحوسبة السحابية مؤخراً، حيث توجهت كبرى شركات تكنولوجيا المعلومات إلى تبني وتطبيق فكرة الحوسبة السحابية، فأصبحت تؤجر موارد الحوسبة وموارد التخزين الموجودة في مراكز البيانات الخاصة بها، وكانت أولى هذه الشركات شركة أمازون Amazon ذات سحابة EC2 تلتها شركة مايكروسوفت Microsoft التي زودت مستخدميها بمنصة سحابية عرفت بـ Windows Azure، بعدها جاءت شركة Apple بخدمة الحوسبة السحابية iCloud ثم حذوهم شركة أوراكل Oracle و شركة غوغل Google وغيرهم من الشركات الأخرى.

القسم العملي

تم بناء نظام للاستخدام الشّخصي حيث تم استخدام الرقم التسلسلي الخاص بالهاتف من أجل توليد مفاتيح التشفير بحيث يتم استدعاء توابع محدّدة بناء على خيار المستخدم وذلك باستخدام لغة البرمجة python، حيث أنّ الخيارات المتاحة عبر واجهة المستخدم هي التّشفير Encrypt، فك التّشفير Decrypt، رفع ملف إلى الحساب السّحابي Upload file بالإضافة إلى تحميل ملف من الحساب السّحابي Download file.

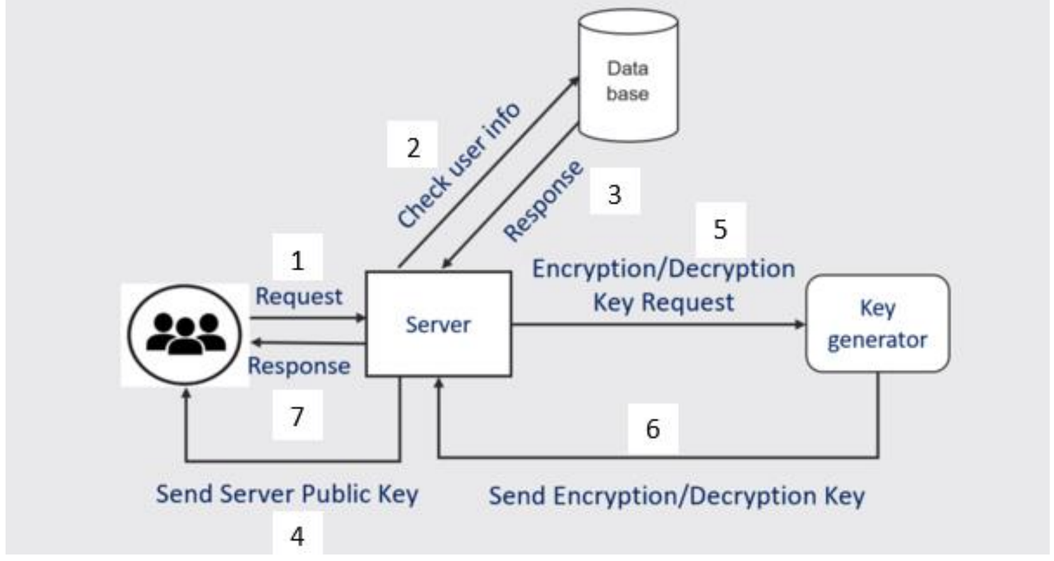
تم بناء نموذج يتيح تشفير الملفات والتّحقّق منها وتوقيعها وفك تشفيرها ضمن الصّلاحيات المُتاحة دون الرّجوع لمالك الملف الأصلي بالإضافة إلى التّحقّق من الملفات باستخدام توقيع محفوظ وتحديث الملفات لأي شخص ضمن مجموعة العمل المحدّدة فقط مع بيان صاحب آخر تعديل على الملف ولا يتيح لأي شخص خارج مجموعة العمل بالوصول إلى الملفات الخاصة بمجموعة العمل أو إجراء أي تعديل، بالإضافة إلى إمكانيّة إضافة مستخدم جديد وتحميل أو رفع الملفات من وإلى السّحابة علماً أنّه تم استخدام قناة إتصال مشفّرة آمنة بين المخدّم والعميل.

النتائج والمناقشة

النتائج المستخلصة في هذه المرحلة من البحث تبيّن أنّ: استخدام الخوارزميات AES,DES في نظام هجين Hybrid لن يؤدّي إلى تغير زمن التشفير وفك التشفير وهذه النتائج متوافقة مع الدراستين البحثيتين [(Padmavathi. B, Ranjitha. S, 2013) ، (Maitri. P, Verma.A, 2016)

تم اقتراح وتنجيز نظامين مختلفين لتعزيز أمن تخزين الملفات على السّحابة حيث تم بناء نظام مخدّم وعميل يستخدمون التشفير والتوقيع الرقمي لتبادل الملفات بينهما.

تم 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 يتم إظهار صاحب أخر تعديل على الملفات ممّا يضمن عدم تعديل أي ملف وتشفيره دون معرفة صاحب أخر تعديل والمالك الأصلي.



المراجع

Poduval, A., Doke, A., Nemade, H., & Nikam, R. (2019). Secure file storage on cloud using hybrid cryptography. International Journal of Computer Science and Engineering, 7(01), 587-591.

] Srivalli, B. S. S., & SwarupMedikonda, B. (2019). 2[Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography. International Journal of Recent Technology and Engineering (IJRTE), 8(1), 3267-3271.

] Kanatt, S., Jadhav, A., & Talwar, P. (2020). Review of 3[secure file storage on cloud using hybrid cryptography. International Journal of Engineering Research & Technology (IJERT), 9(2), 16-20.

] Poduval, V., Koul, A., Rebello, D., Bhat, K., & Wahul, 4[R. M. (2020). Cloud based secure storage of files using hybrid cryptography and image steganography. International Journal of Recent Technology and Engineering (IJRTE), 8(6), 665-667.

جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تعزيز أمن التخزين السحابي باستخدام التشفير وإخفاء المعلومات

Enhancing Cloud Storage Security using Cryptography and Steganography

م.مريم عمار يوسف
د.وسيم موسى السمارة

الملخص

يهدف البحث إلى تعزيز أمن التخزين السحابي 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.

القسم النظري

تزايد إستخدام الحوسبة السحابية مؤخراً، حيث توجهت كبرى شركات تكنولوجيا المعلومات إلى تبني وتطبيق فكرة الحوسبة السحابية، فأصبحت تؤجر موارد الحوسبة وموارد التخزين الموجودة في مراكز البيانات الخاصة بها، وكانت أولى هذه الشركات شركة أمازون Amazonذات سحابة 2 ECتلتها شركة مايكروسوفت Microsoftالتي زودت مستخدميها بمنصة سحابية عرفت بـ Windows Azure، بعدها جاءت شركة Apple بخدمة الحوسبة السحابية iCloud ثم حذا حذوهم شركة أوراكل gOracle شركة غوغل Googleوغيرهم من الشركات الأخرى.

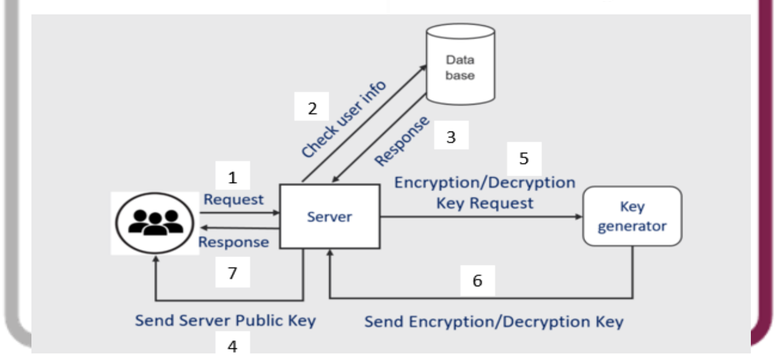
القسم العملي

تم بناء نظام للاستخدام الشّخصي حيث تم استخدام الرقم التسلسلي الخاص بالهاتف من أجل توليد مفاتيح التشفير بحيث يتم استدعاء توابع محدّدة بناء على خيار المستخدم وذلك باستخدام لغة البرمجة python، حيث أنّ الخيارات المتاحة عبر واجهة المستخدم هي التّشفير Encrypt، فك التّشفير Decrypt، رفع ملف إلى الحساب السّحابي Upload file بالإضافة إلى تحميل ملف من الحساب السّحابي Download file.

تم بناء نموذج يتيح تشفير الملفات والتّحقّق منها وتوقيعها وفك تشفيرها ضمن الصّلاحيات المُتاحة دون الرّجوع لمالك الملف الأصلي بالإضافة إلى التّحقّق من الملفات باستخدام توقيع محفوظ وتحديث الملفات لأي شخص ضمن مجموعة العمل المحدّدة فقط مع بيان صاحب آخر تعديل على الملف ولا يتيح لأي شخص خارج مجموعة العمل بالوصول إلى الملفات الخاصة بمجموعة العمل أو إجراء أي تعديل، بالإضافة إلى إمكانيّة إضافة مستخدم جديد وتحميل أو رفع الملفات من وإلى السّحابة علماً أنّه تم استخدام قناة إتصال مشفّرة آمنة بين المخدّم والعميل.

القسم العملي

يوضّح الشّكلمخطّطاً لعمل النّظام المنجز بشكل عام حيث يقوم العميل بتسجيل الدّخول وإرسال طلب إلى المخدّم بناء على الخيارات المتاحة فيقوم المخدّم بالتّحقّق من معلومات العميل من خلال قاعدة البيانات الموجودة لديه، فإذا نجحت عمليّة التّحقّق من معلومات العميل يقوم المخدّم بإرسال مفتاح التّشفير العام الخاص بالمخدّم للعميل ومن ثم توليد مفاتيح التّشفير أو فك التّشفير وفقاً لطلب العميل من خلال مولّد المفاتيح وإرسال المفاتيح للمخدّم والذي يقوم بإرسال مفاتيح التّشفير للعميل لاستكمال عمليّة التّشفير أو فك التّشفير.



النتائج والمناقشة

النتائج المستخلصة في هذه المرحلة من البحث تبيّن أنّ: استخدام الخوارزميات AES,DES في نظام هجين Hybrid لن يؤدّي إلى تغير زمن التشفير وفك التشفير وهذه النتائج متوافقة مع الدراستين البحثيتين](Padmavathi. B, Ranjitha. S, 2013)، (Maitri. P, Verma.A, 2016)

تم اقتراح وتنجيز نظامين مختلفين لتعزيز أمن تخزين الملفات على السّحابة حيث تم بناء نظام مخدّم وعميل يستخدمون التشفير والتوقيع الرقمي لتبادل الملفات بينهما.

تم 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 يتم إظهار صاحب أخر تعديل على الملفات ممّا يضمن عدم تعديل أي ملف وتشفيره دون معرفة صاحب أخر تعديل والمالك الأصلي.

المراجع

Poduval, A., Doke, A., Nemade, H., & Nikam, R. (2019). Secure file storage on cloud using hybrid cryptography. International Journal of Computer Science and Engineering, 7(01), 587-591.

[2] Srivalli, B. S. S., & SwarupMedikonda, B. (2019). Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography. International Journal of Recent Technology and Engineering (IJRTE), 8(1), 3267-3271.

[3] Kanatt, S., Jadhav, A., & Talwar, P. (2020). Review of secure file storage on cloud using hybrid cryptography. International Journal of Engineering Research & Technology (IJERT), 9(2), 16-20.

جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تعزيز أمن التخزين السحابي باستخدام التشفير وإخفاء المعلومات

Enhancing Cloud Storage Security using Cryptography and Steganography

م.مريم عمار يوسف
د.وسيم موسى السمارة

الملخص

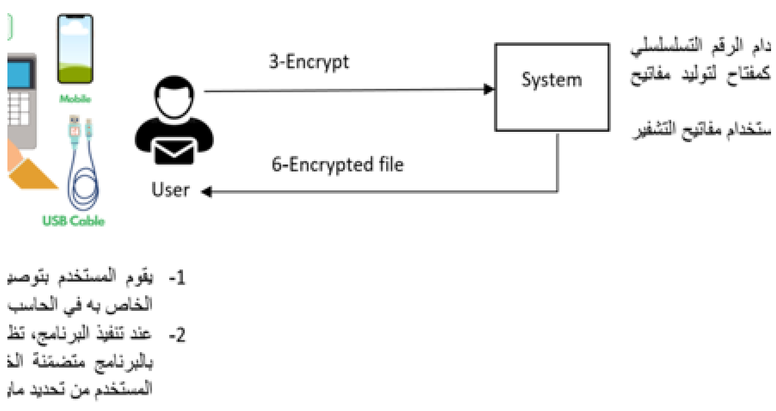
يهدف البحث إلى تعزيز أمن التخزين السحابي التّشفير وإخفاء المعلومات و يتناول البحث دراسة أداء خوارزميات التّشفير AES,DES,RSA ودرجة الأمان الناتجة عن استخدام هذه الخوارزميات في تشفير الملفات حيث تمّ اقتراح وتنجيز نظامين مختلفين لتعزيز أمن تخزين الملفات على السّحابة، الأوّل من أجل إدارة الملفات الخاصة بالمستخدم 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.

القسم النظري

تزايد استخدام الحوسبة السحابية مؤخراً، حيث توجهت كبرى شركات تكنولوجيا المعلومات إلى تبني وتطبيق فكرة الحوسبة السحابية، فأصبحت تؤجر موارد الحوسبة وموارد التخزين الموجودة في مراكز البيانات الخاصة بها، وكانت أولى هذه الشركات شركة أمازون Amazon ذات سحابة EC 2 تلتها شركة مايكروسوفت Microsoft التي زودت مستخدميها بمنصة سحابية عرفت بـ Windows Azure، بعدها جاءت شركة Apple بخدمة الحوسبة السحابية iCloud ثم حذا حذوهم شركة أوراكل Oracle و شركة غوغل Google وغيرهم من الشركات الأخرى.

القسم العملي

يوضّح الشّكلمخطّطاً لعمل النّظام المنجز بشكل عام حيث يقوم العميل بتسجيل الدّخول وإرسال طلب إلى المخدّم بناء على الخيارات المتاحة فيقوم المخدّم بالتّحقّق من معلومات العميل من خلال قاعدة البيانات الموجودة لديه، فإذا نجحت عمليّة التّحقّق من معلومات العميل يقوم المخدّم بإرسال مفتاح التّشفير العام الخاص بالمخدّم للعميل ومن ثم توليد مفاتيح التّشفير أو فك التّشفير وفقاً لطلب العميل من خلال مولّد المفاتيح وإرسال المفاتيح للمخدّم والذي يقوم بإرسال مفاتيح التّشفير للعميل لاستكمال عمليّة التّشفير أو فك التّشفير.

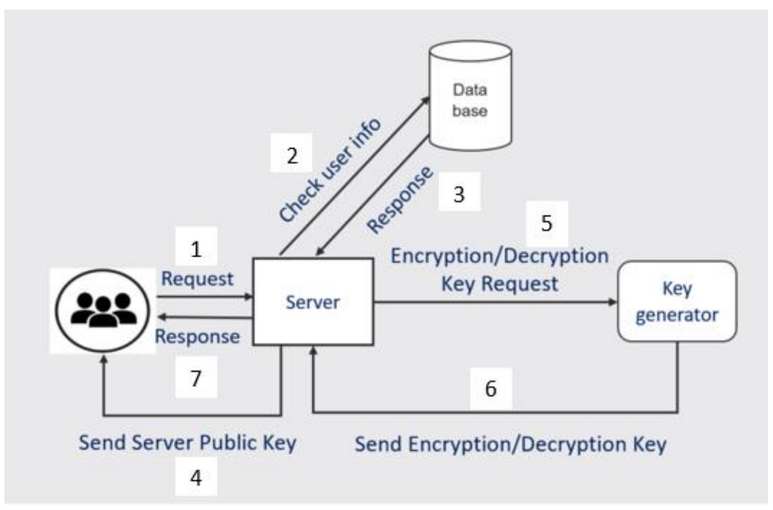


النتائج والمناقشة

النتائج المستخلصة في هذه المرحلة من البحث تبيّن أنّ: استخدام الخوارزميات AES,DES في نظام هجين Hybrid لن يؤدّي إلى تغير زمن التشفير وفك التشفير وهذه النتائج متوافقة مع الدراستين البحثيتين [(Maitri. P, Verma.A, 2016)، (Padmavathi. B, Ranjitha. S, 2013)

تم اقتراح وتنجيز نظامين مختلفين لتعزيز أمن تخزين الملفات على السّحابة حيث تم بناء نظام مخدّم وعميل يستخدمون التشفير والتوقيع الرقمي لتبادل الملفات بينهما.

تم 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 يتم إظهار صاحب أخر تعديل على الملفات ممّا يضمن عدم تعديل أي ملف وتشفيره دون معرفة صاحب أخر تعديل والمالك الأصلي.



المراجع

Poduval, A., Doke, A., Nemade, H., & Nikam, R. (2019). Secure file storage on cloud using hybrid cryptography. International Journal of Computer Science and Engineering, 7(01), 587-591.

[2] Srivalli, B. S. S., & SwarupMedikonda, B. (2019). Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography. International Journal of Recent Technology and Engineering (IJRTE), 8(1), 3267-3271.