حماية البيانات الخاصة من قبل مزود الخدمة السحابية

مريم عبيد مسلم الرشيدي

المستخلص

تشكك معظم الشركات في إجراءات الأمن التي يوفرها مقدمي الخدمات السحابية وبالتالي يرفضون تخزين البيانات السرية، مثل سجلات الموظفين، في مثل هذه الخدمات السحابية. اقترح هذه البحث خوارزمية تشفير تدعى "الخوارزمية العشوائية" لأنها مبنية على فكرة الأختيار عشوائي لتشفير الملفات التي يتم رفعها بواسطة المستخدم بواسطة خمسة خوارزميات تشفير. ساعدت تقنية التجزئة المقترحة في إضافة الأمان والخصوصية إلى تطبيقات التخزين السحابية. استنادًا إلى الدراسات السابقة في الفصل الثالث، أنشأنا تقنية تجزئة على مستوى الملف والتي لا تعمل على مستوى قاعدة البيانات، على عكس الأساليب الشائعة الاستخدام في حالة تقنيات التجزئة مثل التجزئة الأفقية والتجزئة الرأسية والتجزئة الهجينة، والتي تعمل على مستوى قاعدة البيانات . عملت خوارزمية التشفير وتقنية التجزئة المقترحة ضمن إطار أمان متكامل يتضمن بوابة مصادقة المستخدم و التي تقوم بتشفير بيانات تسجيل المستخدم من خلال خوارزمية تشفير تسمى Rivest-Shamir-Adleman (RSA). كانت نتائج الإطار الأمني المقترح إيجابية، حيث ساهمت في تقليل وقت التشفير وفك التشفير بنسبة ٩٩ ٪ تقريبًا، مقارنة بالدراسات السابقة بالأضافة إلى رفع مستوى أمن الملفات.

الكلمات الرئيسية - أمن البيانات؛ الحوسبة السحابية؛ التجزئة؛ خصوصية المستخدم؛ خوارزميات التشفير.

Protecting Sensitive Data on Cloud Service Provider

Mariam Obid Muslim Alrashidy

Prof. Dr. Maher Ali Khemakhem

ABSTRACT

Most companies are skeptical about the security and insurance measures offered by cloud services and are reluctant to store sensitive data, such as employee records, in the cloud. Thus, more effort is needed to support the security of information in cloud computing. In this thesis, we conduct a theoretical study of security issues related to data security in cloud computing. This is followed by a survey of the techniques and algorithms used to support data security, integrity and confidentiality. Then, we propose a cryptography algorithm called the "random algorithm" which is built on the idea of randomizing the encryption of uploaded files among five encryption algorithms. The proposed fragmentation technique adds security and privacy to cloud storage applications. Based on earlier studies, we have created a file-level fragmentation technique that does not work at the database level, in contrast to commonly employed fragmentation techniques, such as horizontal fragmentation, vertical fragmentation, and hybrid fragmentation, which work at the database level. The proposed encryption algorithm and fragmentation technique work within an integrated security framework that includes a user authentication gateway that encrypts user registration data through a cryptography algorithm called the Rivest-Shamir-Adleman algorithm (RSA). The results of the proposed security framework were positive, as it contributed to reducing the encryption time and decoding time by approximately 99%, compared to earlier studies.

Index Terms - Data security; cloud computing; fragmentation; user privacy; encryption algorithms.