الكلمات المفتاحية للبحث عن البيانات المشفره في الحوسبة السحابية

إعداد

راكان نواف احمد الهوادي

إشراف

الاستاذ الدكتور خالد عبدالحافظ الكعابنة

الملخص

أدى النمو السريع لخدمات الإنترنت السحابية المستندة إلى السحابة إلى العديد من الهجمات الأمنية الخطيرة التي تثير قلق المستخدمين. يواجه المستهلكون والشركات الذين يستخدمون السحابة لتخزين بياناتهم مقايضة صعبة للأمان والموثوقية ومنع مخاطر الخصوصية ، فضلاً عن تقليل تكاليف التخزين السحابي الأكثر أمانًا.

الهدف الرئيسي من هذه الرسالة هو حل مشكلة أمن البيانات وكذلك تقليل معدل التصادم أثناء فهرسة البيانات. وسيوفر إطارًا لحل مشكلة أمان البيانات باستخدام خوارزميات التجزئة الآمنة وتشفير العسل معًا. بالإضافة إلى ذلك ، يعد البحث عن بعد أفضل لأنه يعطينا نتائج الكلمات التي نريد العثور عليها ، حيث يتم البحث عن قيمة الكلمة التي نريد الوصول إليها.

ومن احد المشاكل التي واجهناها هي مشكلة تصادم البيانات التي واجهتها بعض الخوارزميات. لقد اخترنا الخوارزمية التي لا تحتوي على تصادم للبيانات وكل قيمها فريدة وعدد الخطوات فيها أقل وذلك للمساعدة في عملية فهرسة البيانات لتسهيل البحث عنها.

يتم تنفيذ تشفير البيانات وفك التشفير محليًا قبل إرسال البيانات إلى السحابة، نقوم بتشفير الكلمة الأصلية في كلمة مفهومة بإستخدام تشفير العسل الذي يساعد على ايقاع المتسللين في الفخ، معتقدين أنهم حصلوا على البيانات الأصلية. وفي عملية فك التشفير نعتمد على جدول التجزئة لتحويل هذه القيم إلى الكلمات الأصلية.

ومع ذلك، تتطلب هذه العملية مساحة تخزين أكبر بسبب استخدام وظائف الهاش، مما يزيد من حجم كل كلمة إلى 32 بت. تهدف هذه الرسالة إلى حل المشكلة عن طريق تقليل المخاطر التي تهدد البيانات والقضاء عليها مع الحفاظ على فوائد استخدام سعة التخزين السحابية وتعزيزها.

Keyword Search On Encrypted Data In I-Cloud Computing

Prepared by:
Rakan Nawaf Alhawadi

Supervised by:
Prof. Khalid A.Kaabneh

Abstract

The rapid growth of cloud-based Internet and cloud-based services has led to many serious security attacks that cause concern to users. Consumers and companies who are using the cloud to store their data face a difficult trade-off for security, reliability and privacy risk prevention, as well as reducing costs for safer cloud storage.

The main purpose of this thesis is to provide a solution to data security as well as reducing the collision rate during data indexing. It will provide a framework for solving the problem of data security using secure hash algorithms and honey encryption together. In addition, a remote search is better because it gives us the results of the words we want to find it, where the value of the word which we want to access it is searched.

One of the problems which we faced is data collision that is suffering from them some algorithms. We chose the algorithm that does not contain

a data collision and all its values are unique and the number of steps is less to help in the process.

Data encryption and decryption are done locally before sending the data to the I- cloud, we encrypt the original word into an understandable word by using honey encryption that helps to trap the hackers, they believe that they get the original data during the decryption process; we depend on the hash table to convert these values to the original words.

However, this process requires more storage space because we used the hash functions which it increases the size of each word is 32 bits. The aims of this thesis to solve the problem by eliminating and reducing the risks which threatening data while maintaining the benefits of using and enhancing cloud storage.