Pengembangan Aplikasi Cloud Storage dengan Skema Proxy Re-encryption untuk Keamanan Data = Development of a Cloud Storage Application with Proxy Re-encryption Scheme for Data Security

Ahmad Naufan Wicaksonoputra, author

Abstrak

Cloud storage merupakan salah satu layanan terpopuler dalam konteks komputasi awan dengan keunggulan skalabilitas yang tidak terbatas dan aksesbilitas yang mudah. Namun, terdapat kekhawatiran akan keamanan data yang disimpan di luar kendali pengguna. Salah satu solusinya adalah dengan melakukan enkripsi pada data sebelumn penyimpanan. Masalah lain muncul karena jika ingin membagikan data tersebut, maka pengguna harus memberikan kunci miliknya atau melakukan dekripsi-enkripsi dengan kunci baru. Solusi selanjutnya adalah dengan mengimplementasikan algoritma re-enkripsi yang memungkinkan sistem membagikan data yang terenkripsi secara aman tanpa perlu mengungkap data asli atau memerlukan kunci asli. Oleh karena itu, akan dikembangkan aplikasi CloudCipher yang sudah terintegrasi dengan alat kriptografi untuk melakukan enkripsi dan dekripsi data serta memanfaatkan algoritma re-enkripsi dalam proses pembagian datanya. Dari hasil evaluasi, usability fitur cloud storage mendapatkan respon yang baik sementara fitur alat kriptografi mendapatkan respon yang kurang baik dikarenakan banyaknya istilah-istilah kriptografi yang kurang dimengerti oleh pengguna secara umum. Dari sisi performa, masing-masing proses kriptografi yang dilakukan sudah berjalan dengan baik namun masih memerlukan optimisasi lebih lanjut pada bagian komunikasi antar komponen melalui jaringan internet.

.....Cloud storage is one of the most popular services in the context of cloud computing, offering unlimited scalability and easy accessibility advantages. However, there are concerns about the security of data stored outside of the user's control. One solution is to encrypt the data before storing it. This leads to another issue, which is when the users need to share that encrypted data, as they either must provide their personal key or perform a decryption-encryption with a new key. The next solution is to implement a re-encryption algorithm that allows the system to securely share encrypted data without revealing the original data or requiring the original key. Therefore, CloudCipher, an application with integrated cryptographic tools, will be developed to perform data encryption and decryption that also utilize the re-encryption algorithm in its data sharing process. From the evaluation results, the usability of the cloud storage feature received positive feedback, while the cryptographic tool feature received less favourable responses due to the general users' lack of understanding of cryptography terminologies. In terms of performance, the individual cryptographic processes are running well, but further optimization is needed for communication between components over the internet network.