IMPLEMENTASI DELEGATED COMPUTATION PADA PUBLIC CLOUD MENGGUNAKAN ALGORITMA FULLY HOMOMORPHIC ENCRYPTION

ANNISA MUZAYANA
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201106347@mhs.dinus.ac.id

ABSTRAK

Saat ini penggunaan cloud computing telah menjadi trend dikalangan organisasi dan masyarakat luas. Hal ini dikarenakan kemudahan dalam berbagi dan hemat dari segi ekonomis. Namun kemudahan dalam berbagi inilah yang dapat membuat cloud computing ini mempunyai masalah keamanan. Kemungkinan data dicuri atau dibobol dapat terjadi. Selain itu masalah keamanan juga muncul dari sisi provider. Fully Homomorphic Encryption menjadi salah satu solusi dimana kemudahan berbagi data dan keamanan data akan dapat dipertahankan tanpa harus mengorbankan apapun. Masalah tersebut menjadi dasar penelitian ini. Dengan menggunakan skema Delegation Computation (pendelegasian perhitungan) hal ini bisa sangat dimungkinkan terjadi. Penelitian ini menerapkan skema delegated computation untuk dapat mendelegasikan pemrosesan data ke pihak kedua yang telah diberikan akses dan memliki kunci publik tanpa mengetahui data aslinya. Serta menggunakan algoritma Fully Homomorphic Encryption untuk memungkin skema dapat digunakan untuk memproses data ciphertext oleh pihak kedua yang diberi akses dan memiliki kunci publik. Sehingga keamanan dan kenyamanan berbagi data tercapai, dan dapat diaplikasikan ke kehidupan sehari â€“ hari. Namun, diperlukan operasi yang cakupannya lebih banyak seperti pengurangan dan pembagian agar pemrosesan data dapat lebih efektif.

Kata Kunci : kriptografi, homomorfisme, enkripsi, fully homomorphic encryption, delegation computation

IMPLEMENTATION OF DELEGATED COMPUTATION ON PUBLIC CLOUD USING FULLY HOMOMORPHIC ENCRYPTION ALGORITHM

ANNISA MUZAYANA
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201106347@mhs.dinus.ac.id

ABSTRACT

Today the use of cloud computing has become a trend among organizations and the wider community. it is because of the easiness way of sharing and saving economically. But the easiness of sharing is can cause a security problem on cloud computing. The possibility of data stolen or compromised may occur. In addition, security issues also arise from the provider side. Fully Homomorphic Encryption become one of the solutions where easiness way of data sharing and data security will be maintained without having to sacrifice anything. The issue became the basis of this research. By using the Delegation scheme Computation (delegating calculation) it can be very possible to happen. This research applies the scheme for the computation delegated may delegate the processing of data to a second party who has been granted access and possess the public key without knowing the original data. And Fully Homomorphic Encryption algorithm to enable the scheme can be used to process data by the second ciphertext given access and has a public key. So that the safety and comfort of data sharing is reached, and can be applied to daily life - today. However, the coverage required operating more like subtraction and division in order to be more effective data processing.

Keyword : cryptography, homomorphisme, encryption, fully homomorphic encryption, delegation computation