Implementasi protokol oblivious transfer untuk pemilihan berkas dalam lingkungan klien-server

Simatupang, Obeth Mangara, author

Abstrak

Perkembangan teknologi yang semakin pesat mendorong terbentuknya sebuah cara transfer data diantara dua pihak yaitu pengirim dan penerima, dimana pengirim yang mempunyai data sebanyak N tidak dapat mengetahui data-data mana saja yang telah dipilih oleh penerima dan penerima hanya dapat mempelajari data-data yang telah dipilihnya tersebut. Data-data yang dapat dipilih adalah sebanyak k dimana 1 k N, dan pengirim dapat memilih satu demi satu data yang dia inginkan. Cara transfer data yang demikian dapat dilakukan dengan protokol Oblivious Transfer yang disebut dengan OTN k×1. Fokus pada tugas akhir ini adalah menelaah dan mengimplementasikan protokol OTN k×1 yang diajukan oleh Moni Naor dan Benny Pinkas pada tahun 1999. Implementasi dilakukan pada platform Java 2 Standard Edition. Implementasi ini menerapkan protokol OTN k×1 untuk pemilihan k berkas secara oblivious. Hasil dari pengujian menguatkan teori bahwa protokol OTN k×1 memang menjalankan transfer data secara oblivious dan keamanannya tergantung pada jumlah data yang dimiliki oleh pengirim. Pengujian dilakukan dengan menggunakan sebuah notebook Pentium M 1,6GHz dengan memori 512 MB dan sebuah komputer Pentium III 1GHz dengan memori 128 MB. Semakin banyak data yang dimiliki oleh pengirim semakin aman protokol ini, namun biaya yang dibutuhkan untuk komputasi persiapan protokol, pengiriman dan penyimpanan menjadi semakin besar. Implementasi protokol...