ANALISIS ALGORITMA DAN KINERJA PADA COUNTER DENGAN CBC-MAC (CCM) SEBAGAI FUNGSI ENKRIPSI TERONTETIKASI

Shelvie Nidya Neyman, Sugi Guritman, Ratna Purnama Sari

ABSTRAK

Algoritma CCM merupakan suatu modus enkripsi terotentikasi yang mengkombinasikan modus enkripsi Counter dengan modus otentikasi CBC-MAC. CCM didasarkan pada algoritma blok kunci simetrik dengan panjang blok 128 bit, seperti algoritma AES. CCM melindungi tiga elemen data, yaitu: nonce, payload, dan associated data.

Berdasar analisis, CCM didesain untuk mendapatkan kerahasiaan dan otentikasi pesan secara simultan menggunakan sebuah kunci rahasia. Kebutuhan akan hanya fungsi forward cipher dari algoritma blok yang mendasari CCM menjadikan ukuran kode implementasi CCM yang lebih kecil. Meskipun demikian, beberapa timbal balik kinerja pada proses-proses dalam CCM harus dipikirkan terlebih dahulu sebelum mengaplikasikan algoritma ini. Semakin besar nonce, maka akan semakin kecil panjang maksimum dari payload yang bisa diproteksi CCM.

Semakin kecil nonce, maka akan semakin kecil jumlah maksimum nonce yang berbeda. Semakin besar nilai MAC akan memberikan jaminan otentisitas yang semakin besar pula. Namun, dengan semakin besar nilai MAC maka semakin besar pula ruang penyimpanan yang harus disediakan bagi ciphertext. Dengan analisis algoritma, didapatkan CCM memiliki kompleksitas pada lingkup O(n) baik bagi proses generation-encryption maupun decryption-verification. Melalui analisis uji implementasi menggunakan Matlab 6.5 dan analisis uji statistik (Independent-Samples T-Test), dapat disimpulkan bahwa running time proses CCM generation-encryption tidak berbeda nyata dengan running time proses CCM decryption-verification dengan selang kepercayaan 95%. Melalui analisis regresi, dapat disimpulkan bahwa untuk payload berukuran besar dan tanpa associated data, nilai running time proses generation-encryption dan decryption-verification pada AES-CCM adalah 1.8 sampai dengan 2.0 kali running time proses enkripsi pada AES-ECB.