PENERAPAN *HYBRID CRYPTOSYSTEM* ALGORITMA *TWOFISH* DAN RSA UNTUK KEAMANAN PENYIMPANAN DATA PADA *CLOUD COMPUTING*

Oleh
Moni Dwi Septi — monidwisepti@student.upi.edu
1404643

ABSTRAK

Pada penelitian sebelumnya tentang analisis perangkat lunak klien *cloud computing* Dropbox serta protokol transmisinya menunjukkan kelemahan dan menjelaskan kemungkinan vektor serangan terhadap klien, melakukan tiga serangan terhadap Dropbox dan berhasil menembus sistem keamanan Dropbox. Penelitian ini bertujuan untuk mengamanankan data yang akan disimpan di *cloud computing*. Pada penelitian ini pengamanan dilakukan dengan mengenkripsi *file* sebelum dikirim ke penyimpanan *online*. Algoritma kriptografi yang digunakan adalah *hybrid cryptosystem Twofish* dan RSA. Hasil penelitian ini menyimpulkan bahwa penerapan *hybrid cryptrosystem* ini dapat diimplementasikan pada penyimpanan *online cloud computing* dan memenuhi tujuan kriptografi yaitu kerahasiaan data. Kedua algoritma baik *Twofish* maupun RSA memiliki nilai *avalanche effect* yang baik yaitu berada disekitar 50%. Selain itu dilakukan pengujian lama waktu dan perubahan ukuran *file* dalam proses enkripsi dan dekripsi *file*. Ukuran *file* yang telah dienkripsi lebih besar dari pada *file* asli. Algoritma *Twofish* memiliki kecepatan rata-rata proses enkripsi sebesar 672473.87 byte/detik dan rata-rata proses dekripsi 693823.88 byte/detik. Sedangkan algoritma RSA memiliki rata-rata kecepatan proses enkripsi 143.20 byte/detik dan proses dekripsi 79.61 byte/detik.

Kata Kunci: *Cloud Computing, Hybrid Cryptosystem, Twofish, RSA*

THE APLICATION HYBRID CRYPTOSYSTEM TWOFISH AND RSA ALGORITHM FOR DATA STORAGE SECURITY ON CLOUD COMPUTING

Arranged by
Moni Dwi Septi — monidwisepti@student.upi.edu
1404643

ABSTRACT

The previous research on analysis of Dropbox client software and transmission protocols showed weaknesses which explained the possibility of attack vectors on clients where it was obtained that there were three attacks on Dropbox and successfully penetrated the Dropbox security system. This study aims to secure data that will be stored in cloud computing. In this research, security was done by encrypting files before they were sent to online storage. The cryptographic algorithm used was the Twofish and RSA hybrid cryptosystem. From the results of this study, it can be concluded that the application of hybrid cryptrosystems can be implemented in online cloud computing storage and meet cryptographic objectives, namely data confidentiality. The test results showed that both the Twofish and RSA algorithms had a good avalanche effect which was around 50%. In addition, testing the length of time and changes in file size were carried out in the process of encrypting and decrypting files. The size of the encrypted file was greater than the original file. The Twofish algorithm had an average speed of the encryption process of 672473.87 bytes / second and the average decryption process was 693823.88 bytes / second. While the RSA algorithm had an average encryption process speed of 143.20 bytes / second and the decryption process was 79.61 bytes/second.

***Keywords**: Cloud Computing, Hybrid Cryptosystem, Twofish, RSA*