Implementasi dan analisa pengiriman data menggunakan algoritma kriptografi RSA pada sistem eucalyptus private cloud IaaS = Implementation and analysis data transfer using RSA cryptography algorithm on eucalyptus private cloud IaaS system

Dyani Mustikarini, author

Abstrak

Skripsi ini berisi mengenai konsep dasar, perancangan dan implementasi enkripsi data dengan RSA yang diterapkan pada private cloud Infrastucture as a Service (IaaS). Tujuan dari skripsi ini menganalisa keamanan pengiriman data dan waktu dari implementasi kriptografi RSA pada sistem Eucalyptus private cloud. Pengiriman data pada sistem virtualisasi private cloud membutuhkan enkripsi untuk mengantisipasi serangan dari man-in-the-middle sehingga penyerang tidak mengetahui isi data dengan mudah.
Hasil penelitian menunjukkan bahwa waktu eksekusi program RSA dipengaruhi oleh ukuran data dan nilai kunci RSA yang dibangkitkan. Peningkatan ukuran data akan mempengaruhi peningkatan waktu eksekusi program RSA. Peningkatan waktu eksekusi untuk format .txt sebesar 31,44%, untuk format .doc sebesar 24,83% dan untuk format .pdf sebesar 24,85%. Nilai d untuk kunci privat RSA yang besar akan sangat mempengaruhi waktu eksekusi karena membutuhkan waktu dekripsi yang lebih lama.
Sedangkan nilai e yang besar untuk kunci publik RSA tidak terlalu signifikan mempengaruhi waktu enkripsi menjadi lebih lama namun tetap berkontribusi terhadap waktu eksekusi RSA. Keamanan pengiriman data pada sistem private cloud dibutuhkan terutama dengan RSA 2048 bit dan sistem padding, namun pada skripsi ini hanya digunakan enkripsi plain RSA.
<hr>This thesis contains about fundamental concept, the design and the implementation of data encryption using RSA which is applied on private cloud Infrastucture as a Service (IaaS). The purposes of this thesis are to analyze the the data transfer security and the time of RSA cryptography appliance on Eucalyptus private cloud system. Secret data transfer on private cloud virtualization requires encryption in order to anticipated the attack from man-in-the-middle so that the attacker won?t know the contents of data easily.
The result of this research prove that RSA execution time influented by the size of data and the value of the generated RSA keys. Data size increment will influence the execution times of RSA. The increment time for .txt is 31,44%, increment time for .doc is 24,83%, and increment time for .pdf is 24,85%. Large values of d for RSA private key greatly affect the execution time because need a longer decryption time.
However, the large value of e for public keys isn?t influence the encryption time significantly but still contributes the execution time. The security of data transfer on private cloud system is needed especially using RSA 2048 bit and padding system appliance,however this thesis only implement plain RSA encryption.