

ABSTRAK

Melihat beragamnya ancaman yang ada di dalam sistem komputer, seluruh lingkup dan persyaratan keamanan sistem komputer harus direncanakan dan diperhitungkan secara terinci pada saat desain berdasarkan kebutuhan yang diinginkan untuk mencegah terjadinya permasalahan pada sistem komputer. Oleh karena itu sistem penyimpanan data pada jaringan komputer membutuhkan keamanan khusus terhadap datanya. Ketika kita membicarakan tentang strategi keamanan dan kerahasiaan data dalam jaringan computer, maka solusi yang terpikir adalah teknik enkripsi, dekripsi, dan kriptografi.

Sistem pada tugas akhir ini menerapkan algoritma simetrik AES, algoritma asimetrik RSA, algoritma fungsi hash satu arah SHA-1, *digital signature*, dan HMAC. Algoritma–algoritma tersebut ditawarkan sebagai solusi keamanan data pada sistem penyimpanan data jaringan komputer NAS dengan teknik penyimpanan data SNAD. Semua algoritma diimplementasikan dan diadaptasikan dengan bahasa pemrograman *Delphi* sebagai *software interface*. Desain sistem dilakukan dengan menggunakan metoda analisis terstruktur yang dituangkan dalam prosedur simulasi.

Keamanan data pada sistem penyimpanan data jaringan komputer NAS dengan teknik penyimpanan data SNAD ini dapat dianalisa performansinya dengan parameter performansi kecepatan waktu dan performansi tingkat kegagalan sistem dalam menyimpan dan membuka kembali file private dan file share, serta ketangguhan sistem akan kemampuan dalam memelihara keamanan datanya.

Dari hasil analisa parameter-parameter di atas, maka diambil kesimpulan bahwa teknik penyimpanan data SNAD pada jaringan komputer NAS cukup tangguh dalam menjaga keamanan data di server penyimpanan data, namun cukup rentan pada proses pengiriman filenya. Selain itu Kecepatan dan kegagalan sistem dipengaruhi oleh kecepatan prosessor komputer yang digunakan sebagai server dan client, traffic jaringan dan algoritma kriptografi yang digunakan.

Kata kunci :SNAD, NAS, AES, RSA, SHA-1, HMAC