

Intisari

Penelitian ini pada dasarnya dilakukan dengan tujuan untuk memperbaiki kinerja *server web* hotel dalam menangani keamanan data reservasi kamar hotel secara *on-line*. Reservasi secara *on-line* biasanya ditangani hanya dengan menerapkan teknik penyandian data saja. Tentunya langkah ini akan membebani *server web* hotel karena memerlukan waktu komputasi yang cukup tinggi.

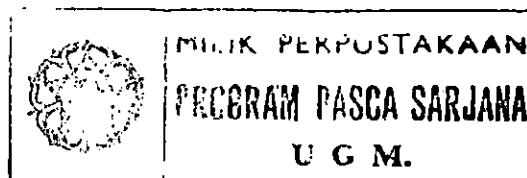
Penanganan lebih lanjut terhadap permasalahan ini akan diatasi dengan mengembangkan model penanganan keamanan reservasi *on-line* dengan memadukan teknik pemampatan dan penyandian data. Model keamanan data ini akan dibangun dengan melakukan proses pemampatan data terlebih dahulu dari pada penyandian datanya. Model ini dikembangkan dengan maksud untuk mengurangi jumlah blok data yang akan disandikan.

Dalam implementasinya akan dibangun 2 model keamanan data reservasi secara *on-line* yaitu :

- a. Model keamanan data reservasi dengan hanya menerapkan teknik penyandian data.
- b. Model keamanan data reservasi dengan memadukan teknik pemampatan dan penyandian data.

Kedua model tersebut akan dibangun dengan metoda penyandian data yang sama yaitu dengan penyandian *public key* (kunci umum) RSA 512 *bit*, sedangkan metoda pemampatan datanya menggunakan metoda pengkodean data Huffman. Kedua model itu akan dikembangkan dengan menggunakan teknologi *java bean* sehingga dapat digunakan untuk mendukung pemrograman *server side*. Pengujian kedua model di atas diujikan pada sistem reservasi kamar hotel secara *on-line* pada jaringan intranet. Hasil pengujian menunjukkan bahwa penanganan keamanan reservasi secara *on-line* dengan pemaduan teknik pemampatan dan penyandian data ternyata dapat mereduksi waktu komputasi *server* rata-rata hingga 22,66% pada sisi pengirim dan 23,83% pada sisi penerima data, dari waktu komputasi *server* yang menerapkan model penanganan keamanan reservasi dengan hanya menggunakan metoda penyandian RSA.

Kata kunci : pemampatan, penyandian, keamanan data.



Abstract

The present study aims to increase the performance of a online-reservation hotel web server which is protected by cryptographic techniques only. Cryptographic protection of data decreases the server performance, because the running time of the encryption/decryption process is quite large.

Therefore the problem of securing online-reservation will be solved with developing a model of protection with integrated compression. The model uses compression before any cryptographic technique is applied. The purpose of this model is to reduce the number of data blocks encrypted during the cryptographic process. In our implementation we develop 2 protection models for on-line reservation, that is :

1. Protection model of reservation data with integrated cryptographic technique,
2. Protection model of reservation data with integrated compression and cryptographic techniques.

Both protection models use the RSA public key cryptosystem, whereas the compression process uses the Huffman coding method. The implementation was done with Java Bean technology. The result of this research shows that the model with integrated compression can reduce the running time up to 22,66% in the transmitter and 23,83% in the receiver, compared to the running time of the encryption-only process.

Key words : cryptography, compression, data protection.

