

Perbandingan algoritma AES-128 dan Blowfish-448 yang dikombinasikan dengan algoritma negative database untuk diterapkan pada aplikasi simple-O = Comparison of AES-128 and Blowfish-448 algorithm which combined with negative database to be implemented in simple-o application

Ahmad Shaugi, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20348909&lokasi=lokal>

Abstrak

Database merupakan bagian terpenting dari suatu aplikasi dan perlu untuk diamankan. Pada tesis ini diajukanlah suatu konsep dasar penerapan algoritma negative database (NDB) yang bersamaan dengan algoritma enkripsi. Kemudian dilakukanlah pengujian performansi dari algoritma AES-128 dan Blowfish-448 yang masing-masing dikombinasikan dengan algoritma NDB, untuk kemudian dipilih kombinasi yang terbaik untuk diterapkan pada aplikasi Simple-O. Hasil pengujian algoritma NDB yang dirancang menunjukkan kesesuaian dengan konsep dasar yang diajukan. Setelah dikombinasikan dengan masing-masing algoritma AES-128 dan Blowfish-448, maka didapatkan hasil rata-rata CPU time AES-128 + NDB dan Blowfish-448 + NDB masing-masing sebesar 0.0030 detik dan 0.0037 detik pada proses enkripsi, dan 0.0054 detik dan 0.006 detik pada proses dekripsi. Rata-rata memory usage AES-128 + NDB dan Blowfish-448 + NDB masing-masing sebesar 9.03 kB dan 9 kB pada proses enkripsi, dan 11.67 kB dan 11.61 kB pada proses dekripsi. Rata-rata processing time AES-128 + NDB dan Blowfish-448 + NDB masing-masing sebesar 1.94 ms dan 2.77 ms pada proses enkripsi, dan 4.34 ms dan 5.03 ms pada proses dekripsi. Sedangkan rata-rata throughput AES-128 + NDB dan Blowfish-448 + NDB masing-masing sebesar 385.89 B/ms dan 275.74 B/ms pada proses enkripsi, dan 156.18 B/ms dan 136.55 B/ms pada proses dekripsi.

.....Database is an important part of an application and need to be secured. In this thesis it was proposed a basic concept of the implementation negative database algorithm (NDB) alongside encryption algorithm. Then perform the performance testing of AES-128 and the Blowfish-448 algorithm, which each combined with NDB algorithm, and then selected the best combination to be applied to Simple-O applications. Testing results of NDB algorithms designed show compliance with the basic concepts proposed. After combined with each algorithm AES-128 and Blowfish-448, then obtained an average yield CPU time AES-128 + NDB and Blowfish-448 + NDB respectively 0.0030 seconds and 0.0037 seconds in the encryption process, and 0.0054 seconds and 0.006 seconds in the decryption process. The average memory usage of AES-128 + NDB and Blowfish-448 + NDB respectively 9.03 kB and 9 kB on the encryption process, and 11.67 kB and 11.61 kB in the decryption process. The average processing time of AES-128 + NDB and Blowfish-448 + NDB respectively 1.94 ms and 2.77 ms on the encryption process, and 4.34 ms and 5.03 ms in the decryption process. While the average throughput of AES-128 + NDB and Blowfish-448 + NDB respectively 385.89 B/ms and 275.74 B/ms in the encryption process and 156.18 B/ms and 136.55 B/ms in the decryption process.