ABSTRAK

Keamanan *data* dalam proses *transfer file* dan informasi sensitif merupakan aspek penting untuk melindungi dari ancaman penyalahgunaan *data*, termasuk aktivitas pencurian *data* seperti *sniffing, phishing*, dan *brute force*, yang dapat menyebabkan kerugian signifikan bagi pengguna. Penerapan skema autentikasi dan enkripsi yang dapat meningkatkan perlindungan *data* dalam sistem transfer *file* berbasis *Client-Server* menjadi salah satu solusi untuk *data* yang dikirimkan menjadi lebih aman. Metodologi yang digunakan yaitu implementasi algoritma *Advanced Encryption Standard* (AES) 256, pengiriman *One Time Password* (OTP) melalui *e-mail* untuk autentikasi pengguna, serta pengujian ketahanan sistem terhadap serangan *brute force* menggunakan 8 jenis *file* (.txt, .docx, .rar, .pdf, .png, .jpg, mp4, dan .mp3) dengan dua kelompok ukuran untuk mengetahui sistem dapat bekerja pada berbagai jenis *file*. Parameter pengujian adalah ketahanan enkripsi diukur dari ukuran enkripsi, waktu enkripsi, kecepatan pengiriman, serta waktu kirim. Dari hasil pengujian, sistem dengan baik mencegah upaya *brute force* dan memastikan hanya pengguna sah yang dapat mengakses. Algorita AES 256 bekerja dengan baik dalam mengenkripsi *file* dimana Kecepatan pengiriman di sisi *client* umumnya lebih tinggi dibandingkan *server*, dengan .txt memiliki kecepatan tertinggi (3,62 KB/s *client*, 2,77 KB/s *server*) .mp4 terendah (1,81 KB/s *client*, 1,71 KB/s *server*). Waktu pengiriman menunjukkan bahwa *file* kecil dapat dikirim dalam 0 sampai 2 detik, sedangkan *file* besar seperti MP4 membutuhkan waktu hingga 1268 detik di sisi *server* dan 1197 detik di sisi *client*. Perbedaan waktu pengiriman antara *server* dan *client* terlihat pada beberapa *file*, seperti .pdf (14 detik *client*, 15 detik *server*) dan .doc (3 detik *client*, 5 detik *server*. Disamping itu pengujian *brute force* yang dilakukan menggunakan aplikasi *cryptools* menghasilkan perkiraan waktu yang sangat lama untuk menebaknya yaitu selama 5.5e+063 tahun.

Kata Kunci: Autentikasi, *File transfer*, AES 256, *socket programming*