BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berikut merupakan kesimpulan dari penelitian Sistem Monitoring Kontrak Kerjasama dengan Protokol *Two Central Facilities* menggunakan Algoritma AES dan Whitespace Manipulation:

1. Diterapkannya protokol *two central facilities* dalam sistem monitoring kontrak kerjasama memenuhi aspek otentikasi dan nir-penyangkalan. Melalui aturan pada protokol ini sistem dapat melakukan otentikasi terhadap *user* yang memiliki hak akses terhadap sistem. Sedangkan aspek nir-penyangkalan, sistem mencatat aktivitas user dalam *log file.* Kedua fasilitas utama yaitu CLA dan CTF dapat saling berkomunikasi dalam menentukan user yang terotentikasi maupun tidak, dibuktikan dengan hasil analisis terhadap proses otentikasi. Dalam penerapan protokol ini terdapat hal yang harus diperhatikan, yaitu adanya aturan yang disepakati oleh CLA, CTF, dan client dalam melakukan otentikasi dan melayani request dari *user*. Hal lain yang tidak kalah penting adalah aturan dalam membangkitkan serta menyimpan validation ID pada proses otentikasi.
2. Algoritma AES dan *whitespace manipulation* dalam sistem monitoring kontrak kerjasama memenuhi empat tujuan kriptografi, yaitu kerahasiaan, integritas data, dan otentikasi. Algoritma AES mampu untuk menjaga kerahasiaan data dalam proses transmisi dengan merubahnya ke dalam bentuk terenkripsi, dibuktikan dengan membandingkan paket data yang dikirimkan antara client dan CTF dengan dan tanpa algoritma AES. Penyisipan digital watermark pada data kontrak dalam bentuk berkas PDF dapat menjaga integritas data dan otentikasi. Proses penyisipan tanda air dilakukan di client sebelum mengirimkan berkas lampiran ke CTF, hal ini dapat menjaga integritas data dari berkas lampiran yang diunggah. Pada aspek otentikasi, tanda air yang disisipkan mampu digunakan sebagai alat

untuk melakukan pembuktian atau klaim terhadap keotentikan suatu berkas kontrak yang telah diunggah ke sistem. Dalam penggunaan algoritma AES, kerahasiaan kunci yang digunakan harus diperhatikan. Sedangkan dalam penggunaan algoritma whitespace manipulation, penyisipan tanda air diharuskan tidak menyebabkan kerusakan pada berkas PDF.

5.2 Saran

Berikut merupakan beberapa saran guna pengembangan lebih lanjut:

1. Gunakan bahasa pemrograman lain selain php mengingat proses enkripsi dan dekripsi adalah suatu rangkaian transformasi matematis. Hal ini didasari oleh hasil pengujian *turn around time* terhadap berkas PDF. Proses dekripsi pada berkas PDF dengan ukuran awal sebesar 1 MB memakan waktu sekitar 633 detik. Bahasa pemrograman python dan java dinilai baik dalam memproses data dalam ukuran besar.
2. Dilihat dari fungsinya, CTF merupakan pusat tabulasi data sehingga dapat disimpan beberapa aplikasi. Penelitian lebih lanjut dapat memberikan gambaran bagaimana pengaruh yang diberikan jika CTF melayani lebih dari satu aplikasi.
3. Algoritma *whitespace manipulation* akan lebih baik jika tanda air disisipkan dengan cara disebarkan menggunakan suatu aturan tertentu.