BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian Penerapan hybrid cryptosystem untuk keamanan penyimpanan data pada *cloud computing* adalah sebagai berikut :

1. Enkripsi dan dekripsi *file* dengan *hybrid cryptosystem* algoritma *Twofish* dan RSA dapat diimplementasikan untuk pengamanan *file* yang akan disimpan dan dibagikan di *cloud computing.* Pada proses enkripsi menghasilkan *cipherfile* yang terdiri dari *ciphertext file* asli dan *cipherkey*. Pada proses enkripsi, *file* asli dienkripsi dengan menggunakan algoritma *Twofish* sedangkan kunci *Twofish* dienkripsi menggunakan RSA yang kemudian hasil dari kedua proses dikirim bersamaan ke penyimpanan cloud. Pada proses dekripsi, *cipherkey* didekripsi terlebih dahulu menggunakan algoritma RSA untuk mendapatkan kunci *Twofish*. Selanjutnya kunci *Twofish* tersebut akan digunakan untuk mendekripsi *ciphertext file* menjadi *file* asli menggunakan algoritma *Twofish*. Dari hasil pengujian *file* berhasil dienkripsi dan dan didekripsi kembali kebentuk semula. *File* hanya bisa didekripsi dengan kunci yang valid.
2. A*valanche effect* dan *randomness* Algoritma *Twofish* dan RSA memberikan hasil yang sangat baik. Pengujian *avalanche effect* kedua algoritma berada disekitar 50% ini bearti kedua algoritma sulit dipecahkan oleh *cryptanalisys.* Rata-rata hasil pengujian algoritma *Twofish* yaitu 50.78% sedangkan rata-rata hasil algoritma RSA yaitu 49.77%, Untuk pengujian *randomness* terhadap *ciphertext* yang dihasilkan menggunakan aplikasi CrypTool 1.4.3, baik algoritma *Twofish* maupun algoritma RSA berhasil melewati pengujian yang diberikan seperti *Frequency test, Poker Test, Run Test, Long Run Test, dan Serial Test*, karena semua hasil pengujian berada dibawah *maximal test value*, hal ini membuktikan bahwa algoritma *Twofish* dan RSA menghasilkan *ciphertext* yang acak.

3. *Hybrid cryptosystem* algoritma *Twofish* dan RSA mampu mengenkripsi dan mendekripsi *file* yang berukuran besar. Ukuran *file* setelah dienkripsi lebih besar dibandingkan ukuran *file* asli, besar ukuran *file* tidak mempengaruhi besar peningkatan ukuran

file karena untuk berbagai ukuran *file* jumlah peningkatan selalu 156 byte. Peningkatan ini dikarenakan kunci *Twofish* yang di enkripsi menggunakan RSA di tuliskan bersamaan dengan *file* asli serta adanya penambahan padding pada algoritma *Twofish.* Berdasarkan pengujian lama waktu proses algoritma *Twofish* memiliki kecepatan enkripsi yang lebih besar dibanding proses dekripsinya. Sedangkan RSA memiliki kecepatan enkripsi yang lebih kecil dibanding dekripsinya. Algoritma *Twofish* memiliki kecepatan rata-rata proses enkripsi sebesar 672473.87 byte/detik dan rata-rata proses dekripsi 693823.88 byte/detik. Sedangkan algoritma RSA memiliki rata-rata kecepatan proses enkripsi 143.20 byte/detik dan proses dekripsi 79.61 byte/detik.

5.2 Saran

Berikut merupakan saran terhadap penelitian ini untuk pengembangan lebih lanjut:

1. Perlu diadakannya pengembangan lebih lanjut terkait sistem yang dibuat dengan masukan seperti gambar, video dan lainnya.
2. Menggunakan bahasa pemrograman selain PHP seperti Matlab, Java atau bahasa pemgrograman lannya.
3. Menambahkan algoritma kompresi untuk memperkecil ukuran file setelah dienkripsi.