BAB 6

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas kesimpulan dan saran dari hasil implementasi metode *searchable encryption* dengan kriptografi kunci asimetri.

6.1 Kesimpulan

Kesimpulan dari penulisan tugas akhir ini, ialah cara kerja dari metode *searchable encryption* dengan kriptografi kunci asimetri berhasil dipelajari. Pencarian data terenkripsi dengan menggunakan metode *searchable encryption* dengan kriptografi kunci asimetri berhasil diterapkan, hal tersebut dibuktikan dengan berhasil dibangunnya perangkat lunak yang memanfaatkan penerapan metode *searchable encryption* dengan kriptografi kunci asimetri. Analisa mengenai efisiensi metode *searchable encryption* dengan kriptografi kunci asimetri dilakukan dengan membandingkan metode tersebut dengan metode pencarian secara *brute force* berdasarkan durasi pencarian dan durasi dekripsi data.

Berikut hasil perbandingan dari metode *searchable encryption* dengan metode *brute force* yang dilakukan menggunakan perangkat lunak yang sudah dibangun:

1. Metode *searchable encryption* memiliki nilai waktu proses dekripsi lebih rendah daripada metode *brute force*.

2. Metode *searchable encryption* memiliki nilai waktu pencarian lebih besar daripada metode *brute force*. Perbedaan nilai tersebut tidak terlalu signifikan.

Dari hasil perbandingan tersebut, dapat disimpulkan bahwa metode *searchable encryption* dengan kriptografi kunci asimetri lebih efisien secara waktu daripada metode *brute force*.

Berdasarkan pengujian keamanan metode *searchable encryption*, nama kata kunci yang digunakan pada *e-mail* dan tersimpan pada basis data tidak sepenuhnya aman. Meskipun kata kunci telah menjadi *searchable encryption*, pihak lain yang memiliki hak akses pada basis data masih dapat mengetahui nama kata kunci yang digunakan. Pihak tersebut cukup mengirimkan beberapa *e-mail* dengan kata kunci yang sama kepada pihak yang ingin diserang. Jika nilai *searchable encryption* yang dihasilkan pada basis data sama dengan nilai *searchable encryption* yang lain, maka nilai tersebut merupakan kata kunci terenkripsi untuk kata kunci yang digunakan penyerang.

6.2 Saran

Adapun saran untuk pengembangan dari perangkat lunak yang dibangun, seperti:

1. Tidak menyimpan *string* biner acak yang merepresentasikan kata kunci pada kamus kata kunci. *String* biner dibangun setiap sebuah kata kunci akan dijadikan *searchable encryption*. *String* biner yang telah dibangun disimpan pada basis data dibagian tabel "kata_kunci" agar nilai *searchable encryption* dapat diuji *trapdoor*. *Trapdoor* hanya berisikan kunci privat dan nilai modulus dari kata kunci yang ingin dicari. Hal-hal tersebut dilakukan agar nilai

searchable encyrption yang disimpan pada basis data selalu berbeda meskipun menggunakan kata kunci dan ditujukan pada penerima yang sama.

2. Menambahkan metode pencarian data terenkripsi lain yang dapat menyembunyikan pola pencarian pada basis data, sehingga keamanan data lebih terjamin karena berdasarkan pengujian fungsional pada bagian 5.2.1.3, *server* dapat mengetahui pola pencarian dari metode *searchable encryption* yang telah diimplemnetasikan.

DAFTAR REFERENSI

[1] Curtmola, R., Garay, J., Kamara, S., dan Ostrovsky, R. (2006) Searchable symmetric encryption: improved definitions and efficient constructions. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, 30 October-3 November, pp. 79–88. ACM, New York.

[2] Diffie, W. dan Hellman, M. (2006) New directions in cryptography. *IEEE Trans. Inf. Theor.*, **22**, 644–654.

[3] Forouzan, B. A. dan Fegan, S. C. (2006) Cryptography. Bagian dari Olson, R. (ed.), *Data Communications And Networking*. McGraw-Hill, New York, USA.

[4] Forouzan, B. A. (2008) Introduction. Bagian dari Olson, R. (ed.), *Cryptography & Network Security*. McGraw-Hill, New York, USA.

[5] Boneh, D., Crescenzo, G. D., Ostrovsky, R., dan Persiano, G. (2004) Public key encryption with keyword search. *Advances in Cryptology - EUROCRYPT 2004*, Interlaken, Switzerland, 2-6 May, pp. 506–522. Springer, Berlin, Heidelberg.