BAB 6

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas kesimpulan dan saran dari hasil analisis algoritma *Searchable Encryption*

6.1 Kesimpulan

Kesimpulan dari penulisan skripsi ini adalah algoritma *Searchable Encryption* telah berhasil dipelajari. Algoritma *Searchable Encryption* ini juga berhasil diterapkan yang dibuktikan dengan berhasilnya dibangun perangkat lunak yang menerapkan algoritma *Searchable Encryption*. Analisis mengenai algoritma *Searchable Encryption* dilakukan dengan cara membandingkan durasi pencarian data pada basis data menggunakan cara yang disebutkan oleh Dawn Song [1] dengan cara pencarian usulan.

Berdasarkan hasil analisis terhadap algoritma *Searchable Encryption* yang dilakukan terhadap perangkat lunak yang sudah dibangun:

1. Algoritma *Searchable Encryption* sudah dapat melakukan data terenkripsi. Pencarian ini masih belum sempurna karena terbatas harus sesuai dengan kondisi saat data belum dienkripsi (*case sensitive*) dan tidak dapat hanya sebagian kata saja.

2. Secara teori, algoritma *Searchable Encryption* ini dapat digunakan untuk semua jenis tulisan, namun pada skripsi ini dibatasi hanya untuk *encoding* ISO/IEC 8859-1 dikarenakan bahasa pemrograman dan basis data yang digunakan.

3. Cara pencarian data pada basis data menggunakan cara berdasarkan referensi tidak optimal. Durasi pencarian data terlampau lama untuk jumlah data yang besar.

4. Algoritma *Searchable Encryption* dapat diimplementasikan di dunia nyata. Namun implementasi ini masih belum praktis karena *user* masih harus mengingat bagaimana ia menulis *plaintext* yang akan dicari.

6.2 Saran

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

1. Membuat algoritma untuk membuat kunci yang digunakan untuk proses enkripsi untuk menambahkan keamanan. Hal ini dikarenakan dalam pembuatan perangkat lunak untuk skripsi ini kata kunci untuk proses enkripsi disimpan secara *hard code* di dalam kode program. Penyimpanan kata kunci untuk proses enkripsi dengan cara ini sangat tidak disarankan karena sangat rawan untuk bocor bila ada serangan ke dalam kode program.

2. Memilih bahasa pemrograman dan basis data yang dapat memakai *encoding* yang lain (misalkan UTF-16) dan *encoding* yang digunakan sebisa mungkin sama. Perbedaan pada *encoding* yang digunakan membatasi batasan nilai yang dapat dienkripsi, disimpan, dan didekripsi dengan akurat

3. Membuat indeks untuk kata kunci sehingga proses pencarian dapat dipercepat lagi. Pada perangkat lunak yang sudah dibuat, proses pencarian memerlukan waktu yang agak lama untuk jumlah data yang besar karena melihat setiap kata kunci pada setiap data. Dengan dibuatnya indeks kata kunci, proses pencarian akan lebih cepat karena pencarian dilakukan pada indeks, bukan pada seluruh data.

4. Memperbaiki algoritma *Searchable Encryption* agar dapat melakukan pencarian berdasarkan sebagian kata dari *plaintext* atau tidak secara *case sensitive*. Pengembangan ini dibutuhkan didasari pada pencarian pada perangkat lunak ini menjadi lebih sulit karena harus ingat bagaimana kondisi penulisan data yang akan dicari pada saat disimpan.

DAFTAR REFERENSI

[1] Song, D. X., Wagner, D., dan Perrig, A. (2000) Practical techniques for searches on encrypted data. *IEEE Symposium on Security and Privacy*, Berkeley, California, USA, 14 - 17 Mei, pp. 44–55. IEEE, Canada.

[2] van Tilborg, H. C. (2000) *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*, 528th edition. Kluwer Academic Publishers, US.

[3] Mollin, R. A. (2007) *An Introduction to Cryptography*, second edition edition. Chapman & Hall/CRC, Boca Raton.

[4] Forouzan, B. A. (2007) *Cryptography and Network Security*, special indian edition 2007 edition. Tata McGraw-Hill Publishing Company Limited, New York.

[5] Lukman, I. (2016) Perbandingan teknik random-modulation dan algoritma floyd-steinberg dalam dithering pada extended visul cryptography. Skripsi. Universitas Katolik Parahyangan, Indonesia.

[6] Schneier, B. dan Kelsey, J. (1996) Unbalanced feistel networks and block-cipher design. *Fast Software Encryption, 3rd International Workshop Proceedings*, Cambridge, February, pp. 121–144. Springer-Verlag, New York.

[7] Kherad, F. J., Naji, H. R., Malakooti, M. V., dan Haghighat, P. (2010) A new symmetric cryptography algorithm to secure e-commerce transactions. *Financial Theory and Engineering (ICFTE), 2010 International Conference on*, Dubai, United Arab Emirates, 18-20 Juni, pp. 234–237. IEEE, Canada.

[8] Aumasson, J.-P. dan Bernstein, D. J. (2012) Siphash: A fast short-input prf. Bagian dari Galbraith, S. D. dan Nandi, M. (ed.), *INDOCRYPT*, Kolkata, India, 9 - 12 Desember, Lecture Notes in Computer Science, **7668**, pp. 489–508. Springer, New York.