BAB 6

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Pada bagian ini akan diberikan kesimpulan atas penelitian yang telah dilakukan. Berikut adalah beberapa kesimpulan tersebut:

1. Pada penelitian ini, telah dipelajari dasar-dasar dalam penambangan data serta 3 teknik enkripsi yang dapat digunakan untuk melakukan enkripsi data. Sehingga telah dimengerti beberapa fungsi dasar dalam penambangan data serta cara kerja masing-masing skema enkripsi.

2. Pada penelitian ini, telah diimplementasikan skema enkripsi *simple XOR*, *ElGamal* dan *order preserving encryption*. Ketiga skema tersebut juga telah digunakan untuk melakukan enkripsi data nilai dan data singkatan.

3. Pada penelitian ini, telah dilakukan juga uji coba operasi fungsi-fungsi dasar dalam penambangan data terhadap data terenkripsi masing-masing skema.

4. Berdasarkan pengujian yang telah dilakukan, penambangan data terhadap data terenkripsi tanpa memerlukan dekripsi terlebih dahulu, dapat dilakukan. Masing-masing skema yang telah diimplementasikan menghasilkan data terenkripsi yang memungkinkannya dilakukan penambangan data secara langsung. Tetapi, skema *order preserving encryption* menghasilkan cipherteks yang memiliki kemungkinan tertinggi untuk ditambang secara langsung.

5. Kemungkinan penambangan data dapat dilakukan terhadap data terenkripsi sepenuhnya bergantung pada skema enkripsi itu sendiri. Oleh karena itu, penyiapan data terenkripsi yang siap ditambang dilakukan dengan mengimplementasikan skema enkripsi yang akan digunakan, dan melakukan enkripsi seluruh data.

6. Pada pengujian yang telah dilakukan, fungsi penambangan data terhadap data terenkripsi dilakukan begitu saja. Atau dengan kata lain, data terenkripsi yang akan ditambang dianggap sebagai data asli. Tetapi, bergantung pada skema enkripsi yang digunakan, terdapat kemungkinan diperlukannya adaptasi. Contohnya, pada *ElGamal additively homomorphic*, fungsi *sum* dilakukan bukan dengan menjumlahkan seluruh cipherteks tetapi justru mengkalikan seluruhnya.

7. Penelitian ini telah menghasilkan perangkat lunak yang mampu melakukan enkripsi data numerik menggunakan ketiga skema yang telah disebutkan sebelumnya, serta mampu melakukan operasi penambangan data terhadap data asli maupun data terenkripsi.

6.2 Saran

Terdapat beberapa saran dari penulis mengenai kelanjutan dari penelitian ini. Berikut adalah saran-saran tersebut:

1. Seperti yang telah disebutkan pada bab-bab sebelumnya, skema *order preserving encryption* yang diimplementasikan dalam penelitian ini, menghilangkan 1 tahap, yaitu tahap *transform*. Oleh karena itu, jika skema ini akan diteliti lebih lanjut, maka lebih baik bila dilengkapi dengan tahap *transform* tersebut.

2. Seperti yang dapat dilihat pada lampiran, data-data yang digunakan pada penelitian ini relatif berukuran kecil. Ada baiknya, penelitian ini dilanjutkan menggunakan data yang berukuran sangat besar.

3. Seperti yang telah disebutkan sebelumnya, skema yang paling mampu menyelesaikan masalah dari penelitian ini secara teori seharusnya adalah *homomorphic encryption*, yaitu lebih spesifik *fully homomorphic encryption*. Oleh karena itu, dirasa akan lebih baik jika skema-skema yang diuji coba selanjutnya mengarah ke *fully homomorphic encryption*.

DAFTAR REFERENSI

[1] van Tilborg, H. C. (1999) *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial*, 1st edition. Kluwer Academic Publishers, Boston/Dordrecht/London.

[2] dan Micheline Kamber dan Jian Pei, J. H. (2012) *Data Mining: Concepts and Techniques*, 3rd edition. Morgan Kaufmann Publishers, Waltham, Mass.

[3] Getting Started with MATLAB Version 7 (2005) *MATLAB : The Language of Technical Computing*. The MathWorks, Inc. Singapore.

[4] Sirajudeen, Y. M. dan Anitha, R. (2018) Survey on homomorphic encryption. *Advances in Engineering Research (AER)*, **142**, 70–74.

[5] Agrawal, R., Keirnan, J., Srikant, R., dan Xu, Y. (2004) Order preserving encryption for numeric data. Technical Report ACM 1-58113-859-8/04/06. IBM Almaden Research Center, 650 Harry Road, San Jose, CA 95120.