BAB VI
PENUTUP

Seluruh proses dari penelitian yang telah dikerjakan dan semua data yang telah diperoleh dari penelitian ditujukan untuk membuat suatu kesimpulan dan saran dalam hal ini maka merupakan tahap akhir dari kegiatan-kegiatan penelitian.

6.1. Kesimpulan

Pada sub bab ini, maka penarikan kesimpulan diambil dari seluruh kegiatan penelitian yang telah dilakukan oleh penulis. Lebih rinci mengenai pengambilan kesimpulan adalah sebagai berikut ini.

1. Mekanisme pengamanan data peserta pelatihan dan sertifikasi dilakukan dengan cara menerapkan algoritma *AES* dan algoritma *Base64*, di mana terdapat 4 proses dalam pengamanan data yang dilakukan.
    a. Proses pertama, enkripsi data berupa *plaintext* menjadi *ciphertext*.
    b. Proses kedua, *encoding* data berupa ciphertext menjadi *index base64*.
    c. Proses ketiga, decoding data berupa *index base64* menjadi *ciphertext*.
    d. Proses keempat, dekripsi data berupa *ciphertext* menjadi *plaintext*.
2. Hasil dari enkripsi (*encipher*) menggunakan algoritma *AES* 256 *bit* memiliki tingkat kerumitan dan sensitivitas yang tinggi, di mana hasil dari enkripsi yang terjadi adalah berupa *ciphertext*, yang mana dalam hal ini proses enkripsi dan dekripsi membutuhkan *cipher key* yang sama (*match*) apabila *cipher key* yang dipakai pada proses enkripsi berbeda (*mismatch*) dengan yang dipakai ketika dilakukan proses dekripsi maka sistem tidak akan dapat mendekripsi pesan tersebut.
3. Pada proses *encoding* pesan menggunakan algoritma *base64* dalam kasus ini penerapannya untuk *mengencode ciphertext* ke dalam bentuk karakter *index base64*, dengan demikian maka data mudah untuk diolah dan disimpan dalam database.
4. Dari proses enkripsi (*encipher*) yang terjadi didapatkan bahwa hasil enkripsi memiliki tingkat sesitivitas yang tinggi terhadap perubahan kalimat yang

terjadi, apabila suatu kalimat dari hasil enkripsi ada yang dihapus maupun diubah, maka proses dekripsi pesan tidak dapat dilakukan dengan kata lain gagal dengan keterangan "*authentication failed*".

5. Pada hasil enkripsi pesan walaupun kalimat teks (*plaintext*) yang dipakai sama namun apabila dienkripsi kembali maka akan memberikan hasil enkripsi yang berbeda dari sebelumnya, sehingga hasil enkripsi dari algoritma *AES* ini tidak *passive*, berbeda dengan algoritma *base64* di mana apabila kalimat teks yang sama akan dilakukan *encoding* maka akan menghasilkan output yang sama persis alias *passive*. Oleh karena itu, dengan penggabungan algoritma *AES* 256 *bit* dan algoritma *base64 encoding* maka hasil enkripsi akan memberikan output yang berbeda-beda walaupun kalimat yang akan dienkripsi sama dengan sebelumnya.

6.2. Saran

Saran yang dapat diberikan terhadap keberlanjutan penelitian di masa yang akan datang adalah sebagai berikut ini.

1. Tambahkan algoritma *token bucket* untuk membatasi jumlah upaya yang dapat dilakukan oleh pengguna terhadap *online form*, sehingga penggunaan algoritma ini dapat untuk mencegah *brute force attacks*, dan untuk membantu mengontrol limit maksimum dari setiap aksi yang diberikan oleh pengguna.
2. Tambahkan fitur notifikasi untuk setiap pesan yang masuk ke dalam *inbox* akun pengguna aplikasi. Apabila *administrator* mengirimkan sertifikat maupun pesan singkat kepada akun pengguna, maka pengguna yang dituju mendapatkan sebuah notifikasi dari aplikasi.

UNIVERSITAS PEMBANGUNAN JAYA