BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pendahuluan, landasan teori, pembahasan hingga pembuatan sistem keamanan ini yang telah di uraikan pada bab-bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut :

1. Peneliti dapat merancang sebuah sistem keamanan yang bisa meminimalisir serangan brute force attack, rainbow table dan CSRF(Cross Site Forgery).

2. Peneliti dapat mengimplementasikan algoritma RSA-OAEP 2048 bit dan HMAC-SHA256 pada password dan token untuk meningkatkan Confidently dan Data Integrity.

3. Berdasarkan sistem keamanan yang di buat, dapat di simpulkan bahwa hasil dari enkripsi ini menjadi sebuah kata-kata yang acak tidak bisa di mengerti oleh manusia.

5.2 Saran

Berdasarkan implementasi dan hasil pada sistem keamanan ini, masih dapat di kembangkan lagi. Saran-saran yang berguna untuk pengembangan sistem ini sebagai berikut :

1. Kriptografi yang di gunakan bisa di kombinkasikan lagi dengan teknik algoritma yang lain seiring mengikutinya zaman.
2. Dalam pembuatan kunci, semoga kedepannya bisa lebih besar lagi dari sistem ini agar level keamanannya dapat bertambah atau perhitungan matematikanya lebih rumit dan lama dalam proses brute force-nya.
3. Mungkin kedepannya untuk proses kriptografi pada web ini, bisa di kombinasikan dengan bahasa pemrograman lain, yang bisa melakukan proses perhitungan lebih efisien.
4. Untuk login, kedepannya mungkin bisa di tambahkan dengan multi factor authentication.