BAB IV
PENUTUP

4.1 Kesimpulan

Berdasarkan hasil implementasi yang telah dilakukan mengenai *JSON Web Token (JWT)* untuk keamanan *RESTful API*, kesimpulan yang diperoleh dari seluruh proses dan hasil pembahasan pada implementasi yang telah dilakukan sebagai berikut :

a. Dengan menerapkan *JSON Web Token* pada *RESTful API* ketika melakukan permintaan *user* harus melakukan proses login terlebih dahulu untuk mendapatkan token. Token ini nantinya akan digunakan untuk melakukan permintaan ke *server*.
b. *JSON Web Token (JWT)* menggunakan kunci rahasia *(secret key)* untuk memastikan integritas data yang dikirim serta mencegah manipulasi informasi dalam token.
c. Penggunaan *JSON Web Token (JWT)* pada *RESTful API* dapat digunakan untuk otentikasi/otorisasi dua aplikasi yang berbeda.

4.2 Saran

Pada implementasi yang telah dilakukan ini semua proses sudah berjalan sesuai dengan semestinya namun berdasarkan implementasi yang dilakukan, saran dibutuhkan dari pengembangan sistem ketika melakukan pengamanan *RESTful API JSON Web Token (JWT)* menggunakan model enkripsi terhadap pesan yang digunakan yaitu enkripsi asimetris dan simetris, menggunakan kombinasi *private key* dan *public key*, dengan standar sebagai berikut:

1. Standard Asymmetric Encryption Signature:

   SHA256withRSA dengan *Private Key (Kpriv)* dan *Public Key (Kpub) (256 bits).*
2. Standard Symmetric Encryption Signature

   HMAC_SHA512 (512 bits)
3. Standard Symmetric Encryption

   AES-256 dengan *client secret* sebagai *encryption key*.