BAB V
SIMPULAN DAN SARAN

5.1 Simpulan *(Conclusion)*

Berdasarkan hasil penelitian dan implementasi pengamanan Application Programming Interface (API) menggunakan Two-Factor Authentication (2FA) dengan algoritma Time-Based One Time Password (TOTP), dapat disimpulkan sebagai berikut:

1. Penerapan JSON Web Token (JWT) pada API order dilakukan dengan cara menyisipkan token pada header setiap melakukan *request* pada API. JWT memastikan bahwa hanya pengguna yang telah melakukan autentikasi untuk dapat melakukan permintaan transaksi, sehingga mencegah transaksi oleh pengguna yang tidak sah.
2. Implementasi algoritma TOTP berhasil meningkatkan keamanan autentikasi login pada sistem yang sebelumnya hanya menggunakan *Single Factor Authentication* (SFA). Dengan adanya autentikasi tambahan ini, sistem menjadi lebih baik dalam mencegah akses tidak sah akibat kebocoran kredensial pengguna.
3. Penggunaan TOTP efektif dalam mencegah terjadinya duplikat *request* pada API order. Autentikasi tambahan berbasis waktu memastikan bahwa setiap transaksi unik dan hanya valid untuk durasi tertentu, sehingga saldo pengguna akan selalu berkurang sesuai dengan nominal transaksi tanpa manipulasi.

5.2 Saran *(Suggestion)*

Berdasarkan hasil penelitian dan implementasi, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan lebih lanjut:

1. Pengembangan sistem monitoring dan pelaporan real-time yang lebih detail untuk mendeteksi aktivitas mencurigakan dan potensi pelanggaran keamanan secara lebih cepat.

2. Melakukan edukasi bagi pengguna mengenai pentingnya menjaga keamanan autentikasi, seperti tidak membagikan kredensial login serta menjaga kerahasiaan token TOTP.
3. Mempertimbangkan integrasi sistem dengan platform notifikasi lain seperti SMS atau push notification untuk memperluas opsi autentikasi tambahan yang nyaman dan aman bagi pengguna.