BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan mengenai implementasi sistem autentikasi berbasis *JSON Web Token* (JWT) dengan mekanisme *refresh token* dalam aplikasi *mobile*, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Implementasi sistem autentikasi berbasis JWT dengan mekanisme *refresh token* pada aplikasi *mobile* telah berhasil dilakukan dengan memperhatikan aspek-aspek penting:
   - Validitas masa berlaku *token* yang berbeda (*access token* dengan waktu singkat dan *refresh token* dengan waktu lebih panjang) meningkatkan keamanan dengan membatasi jendela waktu potensial serangan.
   - Integritas tanda tangan *token* menggunakan algoritma kriptografi HMAC SHA-256 yang kuat untuk mencegah manipulasi dan pemalsuan *token*.
   - Peningkatan pengalaman pengguna melalui pembaruan *access token* otomatis tanpa perlu *login* ulang, menjaga sesi tetap aktif selama *refresh token* valid
   - Perbandingan algoritma HS256 dan HS512, berdasarkan pengujian dengan 50 kali percobaan untuk setiap algoritma dalam lingkungan lokal, menunjukkan bahwa HS256 memiliki waktu respons rata-rata untuk proses *refresh token* yang lebih cepat, yaitu sekitar 259.66 ms, dibandingkan dengan HS512 yang mencatatkan rata-rata sekitar 309.66 ms. Selisih waktu respons rata-rata sekitar 50 ms ini mengindikasikan bahwa HS256 lebih efisien untuk kebutuhan aplikasi *mobile* yang mengutamakan respons cepat dan penggunaan sumber daya yang minimal, sehingga mendukung pengalaman pengguna yang lebih *seamless* dan potensi beban kerja yang lebih ringan

2. Sistem otorisasi berbasis JWT telah berhasil diimplementasikan untuk mengamankan operasi CRUD (*Create, Read, Update, Delete*) pada fitur portofolio digital. Implementasi ini memastikan bahwa hanya pengguna yang terautentikasi dan memiliki izin yang sesuai yang dapat melakukan operasi pada data portofolio. Selain itu, integrasi konversi portofolio menjadi CV berbasis *Applicant Tracking System* (ATS) telah berhasil diimplementasikan sebagai studi kasus penerapan pada mahasiswa Fakultas Ilmu Komputer UPNVJ.
3. Berdasarkan hasil pengujian keamanan akses operasi CRUD pada empat simulasi yakni dengan kondisi token valid, tanpa token, token milik orang lain, dan token kadaluwarsa berhasil masuk ke kondisi aktual sesuai yang diharapkan. Kemudian, pengujian simulasi keamanan sesi ganda sudah sesuai dengan yang diharapkan yakni ketika ada ponsel terbaru *login* dengan akun yang sama, akun sebelumnya akan otomatis keluar jika akses *protected resource* atau accessToken sudah lebih dari 1 menit.

5.2 Saran

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, berikut beberapa saran untuk pengembangan dan penelitian lebih lanjut:

1. Eksplorasi Mekanisme Autentikasi Lanjutan: Mengingat penelitian ini berfokus pada implementasi dasar JWT dan *refresh token*, penelitian selanjutnya disarankan untuk mengeksplorasi mekanisme yang lebih canggih seperti penggunaan *biometric authentication* (sidik jari atau wajah) yang terintegrasi dengan JWT untuk lapisan keamanan tambahan.
2. Perluasan Cakupan Operasi yang Diamankan: Disarankan untuk memperluas penerapan keamanan JWT tidak hanya pada operasi CRUD portofolio, tetapi juga pada fitur-fitur lain yang mungkin dikembangkan di masa depan, seperti modul pesan atau kolaborasi antar pengguna.
3. Integrasi dengan Sistem Akademik Kampus: Untuk meningkatkan nilai aplikasi, disarankan untuk melakukan penelitian mengenai integrasi aplikasi portofolio ini dengan sistem informasi akademik yang sudah ada

di UPNVJ, seperti PRESMA, untuk sinkronisasi data prestasi dan kegiatan mahasiswa.

4. Validasi Kompatibilitas CV ATS secara Mendalam: Penelitian selanjutnya dapat berfokus untuk melakukan pengujian kompatibilitas format CV yang dihasilkan terhadap berbagai perangkat lunak *Applicant Tracking System* (ATS) yang populer digunakan industri, untuk memvalidasi efektivitasnya secara teknis.
5. Pengembangan Lintas Platform dan Distribusi Resmi: Disarankan untuk mengembangkan aplikasi ini untuk platform iOS dan melakukan distribusi resmi melalui Google Play Store dan Apple App Store guna mempermudah akses, instalasi, dan proses pembaruan bagi pengguna.
6. Audit Keamanan Formal: Mengingat keamanan hanya dibatasi pada implementasi JWT, penelitian selanjutnya sebaiknya melibatkan audit keamanan formal, termasuk melakukan penetration testing untuk mengidentifikasi dan menambal potensi kerentanan sistem.
7. Perluasan Target Pengguna: Disarankan untuk memperluas jangkauan pengguna aplikasi tidak hanya untuk mahasiswa Fakultas Ilmu Komputer, tetapi juga untuk seluruh mahasiswa di lingkungan UPN "Veteran" Jakarta.
8. Analisis Kebutuhan untuk Alumni: Melakukan studi kebutuhan baru yang berfokus pada alumni atau *fresh graduate* untuk mengembangkan fitur-fitur yang relevan dengan kebutuhan mereka dalam mencari pekerjaan, yang mungkin berbeda dari mahasiswa aktif.
9. Pelaksanaan *User Acceptance Test* (UAT) Formal: Sangat disarankan untuk melakukan pengujian penerimaan pengguna (*User Acceptance Testing*/UAT) secara formal dengan melibatkan sampel pengguna yang representatif (mahasiswa, verifikator) untuk mendapatkan umpan balik kuantitatif dan kualitatif terhadap fungsionalitas dan usabilitas aplikasi.
10. Pengujian Beban (*Load Testing*): Untuk melengkapi pengujian yang sudah ada, penelitian selanjutnya perlu melakukan *load testing* pada *backend* untuk mengukur seberapa baik performa sistem dalam menangani permintaan dari banyak pengguna secara bersamaan.

11. Implementasi Fitur Hasil Wawancara: Disarankan untuk mengembangkan fitur-fitur tambahan yang telah diidentifikasi dari hasil wawancara awal namun belum diimplementasikan, seperti fitur interaksi atau diskusi portofolio dan chatbot untuk navigasi.
12. Pengujian Performa di Lingkungan Produksi: Melakukan pengujian ulang perbandingan performa algoritma HS256 dan HS512 di lingkungan *server cloud* (produksi) untuk mendapatkan hasil yang lebih realistis dengan memperhitungkan faktor latensi jaringan.