

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Penggunaan algoritma Argon2 terbukti mampu meningkatkan keamanan dalam proses penyimpanan password. Argon2 merupakan algoritma yang telah diakui secara luas memiliki ketahanan terhadap serangan seperti brute-force dan rainbow table attack, karena bersifat memory-hard dan menghasilkan output hash yang unik untuk setiap input berbeda (berkat penggunaan salt). Penerapan Multi-Factor Authentication (MFA) melalui pengiriman kode OTP ke email pengguna memberikan lapisan keamanan tambahan dalam sistem login. Dengan metode ini, hanya pengguna yang dapat mengakses email terdaftar yang dapat menyelesaikan proses registrasi.
2. Integrasi antara Argon2 dan MFA menghasilkan sistem login yang lebih kuat dan tahan terhadap serangan siber seperti credential stuffing dan phishing. Kombinasi ini menurunkan risiko akses tidak sah secara signifikan.
3. Pengujian pada sistem menunjukkan bahwa konfigurasi parameter hashing (terutama time cost) mempengaruhi waktu eksekusi hashing secara signifikan. Semakin tinggi nilai time cost, maka semakin lama waktu hashing, namun semakin tinggi pula tingkat keamanannya.

4. Hasil pengujian parameter Argon2 menunjukkan pengaruh signifikan terhadap waktu hashing: Time Cost = 1 menghasilkan waktu 2,028 ms, Time Cost = 2 menghasilkan waktu 48,623 ms dan Time Cost = 3 menghasilkan waktu 71,219 ms. Artinya, semakin tinggi nilai time cost, semakin tinggi pula keamanan hashing, namun harus tetap memperhatikan performa sistem.
5. Firebase Authentication dan Firestore terbukti efektif untuk menyimpan data autentikasi dan informasi pengguna secara realtime dan aman, serta mendukung sistem login modern yang terintegrasi dengan layanan cloud.

5.2 Saran

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Integrasi OTP dengan server produksi atau layanan pihak ketiga (seperti Twilio, SendGrid, atau Firebase Cloud Functions) agar pengiriman OTP dapat dilakukan secara realtime ke email atau nomor telepon pengguna tanpa bergantung pada sistem lokal.
2. Penyesuaian parameter Argon2 seperti memory cost dan time cost harus mempertimbangkan perangkat target dan pengalaman pengguna (UX), agar sistem tetap aman namun tetap responsif saat login.
3. Pengujian pada penelitian ini masih bersifat fungsi internal (black-box). Untuk penelitian lanjutan, dapat dilakukan simulasi serangan brute-force dan analisis performa lebih mendalam pada berbagai perangkat.