BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan yang telah dipaparkan pada bab-bab sebelumnya, maka ditarik kesimpulan sebagai berikut.

1. Rancangan sistem 2FA menggabungkan algoritma ECDSA untuk menjamin keaslian identitas pengguna serta SHA 256 untuk memastikan integritas. Pada rancangan ini terdapat dua faktor autentikasi, yaitu: pertama autentikasi berupa *username* dan *password* yang dikombinasikan dengan SHA 256; kedua autentikasi berupa tanda tangan digital dengan kombinasi ECDSA dan SHA 256. SHA 256 digunakan untuk melakukan *hashing* terhadap *username*, *password*, kunci privat, dan pesan acak, sedangkan ECDSA digunakan sebagai faktor autentikasi kedua untuk melakukan tanda tangan digital dengan *file* kunci privat milik *client*.
2. Konstruksi program aplikasi login akun dilakukan dengan menggunakan bahasa pemrograman Python dengan bantuan *library* tkinter, hashlib, os, dan random. *Library-library* tersebut digunakan sebagai *library* utama untuk tampilan antarmuka yang memudahkan *client* mengakses program, melakukan kalkulasi terhadap fungsi *hash*, dan memeriksa suatu *file* pada perangkatnya. Terdapat 3 halaman pada program aplikasi login akun, yaitu halaman menu utama, halaman registrasi akun, dan halaman login akun.
3. Validasi dilakukan dengan menguji berbagai skenario login, seperti penggunaan *username* dan *password* yang salah, file kunci privat yang tidak sesuai, dan tanda tangan digital yang tidak valid. Hasil pengujian menunjukkan bahwa sistem mampu secara akurat menolak upaya login yang tidak sah dan hanya memberikan akses kepada pengguna yang berhasil melewati kedua tahap verifikasi. Hal ini membuktikan bahwa kombinasi algoritma ECDSA dan SHA 256 dapat diimplementasikan secara efektif dalam sistem 2FA untuk meningkatkan keamanan autentikasi dan menjaga integritas serta keaslian data pengguna.

5.2 Saran

Berdasarkan kesimpulan dalam penerapan program aplikasi login akun dengan sistem 2FA berbasis ECDSA dan SHA 256, saran dari penulis untuk penelitian selanjutnya adalah sebagai berikut.

1. Pada penelitian ini, program aplikasi login akun masih berupa prototipe yang menggunakan bahasa pemrograman Python, sehingga tidak dapat dengan mudah dipakai secara langsung pada perangkat lain. Untuk penelitian selanjutnya, disarankan untuk membuat dengan Bahasa pemrograman yang lebih umum dalam aplikasi, seperti Java, sehingga dapat memungkinkan sistem ini untuk dikembangkan secara lebih luas.
2. Pada penelitian ini, *database* pada *server* masih berupa *file txt* yang masih dapat dilihat oleh semua orang. Pada penelitian selanjutnya, disarankan untuk membuat ruang aman untuk *database* pada *server*.
3. Penelitian selanjutnya diharapkan untuk membuat program aplikasi login akun yang dapat digunakan pada banyak perangkat secara sekaligus untuk menguji keamanan yang dipakai secara daring.