# BAB V
# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan mekanisme *Two-Factor Authentication (2FA)* pada sistem autentikasi mampu memberikan peningkatan yang signifikan terhadap aspek keamanan dibandingkan dengan metode autentikasi konvensional yang hanya menggunakan satu faktor. Dengan mengombinasikan faktor pengetahuan berupas *password* dan faktor kepemilikan berupa *One-Time Password (OTP)*,sistem mampu menciptakan lapisan perlindungan tambahan yang efektif dalam mencegah akses tidak sah. Hasil implementasi menunjukkan bahwa sistem autentikasi yang dikembangkan telah berhasil menerapkan proses verifikasi berlapis, di mana pengguna diwajibkan untuk melewati dua tahapan autentikasi sebelum memperoleh akses ke sistem. Pendekatan ini terbukti mampu mengurangi risiko yang timbul akibat kebocoran kredensial, karena penyerang tidak hanya membutuhkan *password*, tetapi juga harus menguasai faktor kedua yang bersifat dinamis dan terbatas waktunya.

Berdasarkan evaluasi keamanan yang dilakukan menggunakan kerangka kerja Authenticator Assurance Level (AAL) dari NIST SP 800-63B, sistem yang dikembangkan dalam penelitian ini dapat dikategorikan pada tingkat AAL2. Hal ini menunjukkan bahwa sistem telah memenuhi kriteria sebagai sistem autentikasi *multi-factor* yang mampu memebrikan tingkat jaminan keamanan yang lebih tinggi dibandingkan dengan *single-factor authentication*. Namun demikian, sistem ini belum mencapai tingkat AAL3 karena belum menggunakan autentikator yang memiliki ketahanan tinggi terhadap serangan tingkat lanjut, seperti *phishing-resistant authentication*. Selain itu, penelitian ini juga menunjukkan bahwa meskipun implementasi 2FA mampu meningkatkan keamanan, masih terdapat beberapa potensi kelemahan, terutama yang berkaitan dengan ketergantungan pada media pengiriman OTP serta memungkinkan serangan berbasis rekayasa sosial seperti phishing. Oleh karena itu, keamanan sistem tidak hanya bergantung

pada teknologi yang digunakan, tetapi juga pada kesadaran dan perilaku pengguna dalam menjaga kerahasiaan kredensial mereka.

Secara keseluruhan, penelitian ini berhasil menunjukkan bahwa penerapan 2FA merupakan langkah yang efektif dalam meningkatkan keamanan sistem autentikasi. Selain itu, penggunaan metode evaluasi berbasis NIST AAL memebrikan kerangka analisis yang sistematis, objektif, dan dapat dipertanggungjawabkan secara ilmiah dalam menilai tingkat keamanan sistem.

## 5.2 Saran

Berdasarkan hasil penelitian dan evaluasi yang telah dilakukan, terdapat beberapa saran yang dapat dijadikan sebagai pertimbangan untuk pengembangan sistem di masa mendatang. Pertama, sistem autentikasi dapat ditingkatkan dengan mengadopsi autentikator yang lebih kuat dan modern, seperti penggunaan *hardware security key* atau teknologi bometrik yang berintegrasi dengan perangkat pengguna. Penggunaan autentikator jenis ini dapat meningkatkan ketahanan sistem terhadap berbagai jenis serangan, khususnya *phishing*, sehingga memungkinkan sistem untuk mencapai tingkat AAL3.

Kedua, mekanisme pengiriman OTP perlu ditingkatkan kea rah yang lebih aman, misalnya dengan enggunakan aplikasi autentikator berbasis *time-based* OTP (TOTP) dibandingkan dengan *email* dan SMS. Pendekatan ini dinilai lebih aman karena tidak bergantung pada jaringan komunikasi yang rentan terhadap penyadapan atau pengambilalihan akun. Ketiga, aspek edukasi pengguna juga perlu diperhatikan sebagai bagian dari strategi keamanan secara menyeluruh. Pengguna perlu diberikan pemahaman mengenai pentingnya menjaga kerahasiaan kredensial serta kewaspadaan terhadap berbagai bentuk serangan rekayasa sosial, seperti *phishing*.

Keempat, perlu dilakukan peningkatan pada aspek keamanan tambahan, seperti implementasi deteksi anomaly pada aktivitas login, penggunaan notifikasi keamanan secara *real-time,* serta penerapan enkripsi yang lebih kuat dalam proses transmisi data. Hal ini bertujuan untuk memperkuat sistem dalam menghadapi ancaman yang semakin kompleks. Kelima, untuk penelitian selanjutnya,

disarankan untuk melakukan pengujian keamanan yang lebih mendalam, seperti simulasi serangan (*penetration testing*) atau analisis risiko yang lebih komprehensif. Hal ini dapat memberikan gambaran yang lebih detail mengenai ketahanan sistem terhadap berbagai scenario.

Dengan adanya pengembangan lebih lanjut berdasarkan saran-saran tersebut, diharapkan sistem autentikasi yang dikembangkan dapat mencapai tingkat keamanan yang lebih tinggi, serta mampu memenuhi kebutuhan keamanan pada berbagai konteks penggunaan, termasuk sistem yang menangani data dengan tingkat sensitivitas tinggi.