BAB 5. PENUTUP

5.1. Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem *login website* berbasis ISO/IEC 27001 dengan deteksi aktivitas mencurigakan menggunakan algoritma *K-Nearest Neighbors* (KNN), maka dapat diperoleh kesimpulan sebagai berikut:

1. Sistem *login* berbasis web yang dikembangkan telah berhasil memenuhi prinsip-prinsip keamanan sesuai standar ISO/IEC 27001 melalui penerapan berbagai kontrol keamanan, meliputi kebijakan kata sandi yang kuat, *account lockout*, *session timeout*, *logging*, pemblokiran alamat IP yang mencurigakan, serta autentikasi dua faktor menggunakan Google OAuth. Pengembangan sistem menggunakan metode *Rapid Application Development* (RAD) sehingga proses implementasi dapat dilakukan secara cepat dan terstruktur. Hasil *Black Box Testing* menunjukkan bahwa seluruh fungsi sistem berjalan dengan baik, sedangkan *User Acceptance Testing* (UAT) memperoleh tingkat kepuasan pengguna sebesar 91,3%, yang menunjukkan bahwa sistem telah memenuhi kebutuhan pengguna dari aspek fungsionalitas dan kemudahan penggunaan.
2. Algoritma *K-Nearest Neighbors* (KNN) berhasil diterapkan untuk mendeteksi aktivitas *login* yang mencurigakan menggunakan data simulasi aktivitas *login*. Berdasarkan hasil pengujian, model memberikan performa terbaik pada nilai K = 7 dengan akurasi sebesar 90,67%, presisi 90,41%, dan *recall* 90,41%. Hasil tersebut menunjukkan bahwa algoritma KNN mampu mengidentifikasi pola aktivitas *login* yang mencurigakan dengan tingkat kinerja yang baik. Selain itu, berdasarkan perbandingan sistem *login* berjalan dengan sistem *login* usulan, penerapan KNN dapat meningkatkan kemampuan sistem dari yang sebelumnya hanya melakukan validasi kredensial menjadi sistem yang dapat melakukan analisis pola perilaku *login* secara *real-time*. Integrasi KNN dengan kontrol keamanan ISO/IEC 27001 memungkinkan sistem tidak hanya menerapkan pencegahan seperti kebijakan *password, account lock,* dan *logging*, tetapi juga mampu mendeteksi indikasi aktivitas mencurigakan serta memberikan respons keamanan berdasarkan pola perilaku pengguna.

5.2. Saran

Berdasarkan hasil penelitian yang telah dilakukan, berikut beberapa saran untuk pengembangan penelitian selanjutnya:

1. Penelitian selanjutnya disarankan menggunakan data set *login* yang lebih besar, lebih beragam, dan berasal dari kondisi nyata agar model deteksi aktivitas mencurigakan dapat merepresentasikan pola serangan secara lebih akurat.
2. Penelitian selanjutnya disarankan melakukan pengujian pada lingkungan operasional yang lebih mendekati kondisi industri agar efektivitas penerapan ISO/IEC 27001 dan model KNN dapat dievaluasi secara lebih menyeluruh.
3. Sistem pada penelitian selanjutnya disarankan agar tidak hanya memberikan *alert* ketika *login* terdeteksi mencurigakan, tetapi juga dilengkapi dengan mekanisme mitigasi otomatis, misalnya pembatasan akses sementara, penguncian menu atau fitur yang penting dan tidak boleh sembarang akses, serta step verifikasi tambahan sebelum *user* dapat melanjutkan aktivitas.