PERANCANGAN SISTEM *LOGIN WEBSITE* BERBASIS ISO/IEC 27001 DENGAN DETEKSI AKTIVITAS MENCURIGAKAN MENGGUNAKAN KNN

ABSTRAK

Keamanan sistem *login* merupakan komponen penting dalam sistem berbasis web karena berfungsi sebagai pintu masuk utama bagi pengguna untuk mengakses informasi dan layanan. Meningkatnya jumlah pelanggaran data yang disebabkan oleh pencurian kredensial, kata sandi yang lemah, dan aktivitas *login* yang mencurigakan menyoroti perlunya mekanisme keamanan yang lebih adaptif. Penelitian ini bertujuan untuk merancang sistem *login* situs web berdasarkan kontrol keamanan ISO/IEC 27001 dan menerapkan algoritma *K-Nearest Neighbors* (KNN) untuk mendeteksi aktivitas *login* mencurigakan dengan menggunakan metode *Rapid Application Development* (RAD). Beberapa kontrol keamanan yang diambil dari ISO/IEC 27001 telah diterapkan, termasuk kebijakan kata sandi, penguncian akun, batas waktu sesi, pencatatan aktivitas pengguna, pemblokiran IP, dan autentikasi Google OAuth. Algoritma KNN diterapkan pada kumpulan data aktivitas *login* yang disimulasikan. Hasil pengujian menunjukkan bahwa sistem yang dibangun mampu beroperasi dengan baik, sebagaimana dikonfirmasi oleh *Black Box Testing*. Model KNN mencapai kinerja terbaiknya pada K=7, dengan akurasi sebesar 90,67 persen, presisi sebesar 90,41 persen, dan *recall* sebesar 90,41 persen. Selain itu, evaluasi *User Acceptance Testing* (UAT) menghasilkan skor rata-rata sebesar 91,3 persen.
Kata Kunci: ISO/IEC 27001, *K-Nearest Neighbors*, keamanan sistem *login*, *machine learning*, deteksi aktivitas mencurigakan

PERANCANGAN SISTEM *LOGIN WEBSITE* BERBASIS ISO/IEC 27001 DENGAN DETEKSI AKTIVITAS MENCURIGAKAN MENGGUNAKAN KNN

ABSTRACT

Login system security is a crucial component of web-based systems as it serves as the primary gateway for users to access information and services. The rising number of data breaches caused by credential theft, weak passwords and suspicious login activity highlights the need for more adaptive security mechanisms. This research aims to design a website login system based on ISO/IEC 27001 security controls and to implement the K-Nearest Neighbours (KNN) algorithm to detect suspicious login activity using the Rapid Application Development (RAD) method. Several security controls derived from ISO/IEC 27001 have been implemented, including password policies, account locking, session timeouts, user activity logging, IP blocking, and Google OAuth authentication. The KNN algorithm was applied to a dataset of simulated login activity. Test results show that the system developed is capable of operating effectively, as confirmed by Black Box Testing. The KNN model achieved its best performance at K=7, with an accuracy of 90.67 per cent, a precision of 90.41 percent, and a recall of 90.41 percent. Furthermore, the User Acceptance Testing (UAT) evaluation yielded an average score of 91.3 percent.
Keywords: *ISO/IEC 27001, K-Nearest Neighbors, login system security, machine learning, suspicious activity detection*