INTISARI

PENGHAPUSAN FITUR LEMAH DENGAN PERANGKINGAN FITUR UNTUK MENCEGAH SERANGAN IMPERSONASI PADA SISTEM BIOMETRIK BERBASIS PERILAKU DI PONSEL-PINTAR

Oleh

Afif Izzul Falakh

20/466392/PPA/05958

Ketergantungan kita pada ponsel-pintar dan internet telah membuka banyak peluang bagi pertumbuhan layanan berbasis daring pada ponsel-pintar. Beberapa layanan ini berurusan dengan informasi privat dan sensitive seperti perbankan seluler, dompet digital, dan lain-lain. Karena itu, beberapa langkah pengamanan diimplementasikan untuk membuat sistem menjadi seaman mungkin. Salah satu metode pengamanan yang kian mendapatkan perhatian dari peneliti adalah Sistem Biometric berbasis Perilaku (BBS), khususnya yang berbasis pada perilaku usapan dan genggaman ponsel. Sistem keamanan jenis ini menyediakan otentikasi pengguna secara terus-menerus dan tidak mengganggu sehingga dapat melindungi pengguna di antara sistem keamanan primer. Namun, beberapa riset menunjukkan adanya kemungkinan serangan impersonasi, yang mana si penyerang mencoba menirukan perilaku pengguna untuk mengelabui sistem.

Dengan demikian, riset ini mengusulkan sebuh metode untuk mengidentifikasi keberadaan fitur lemah dalam beberapa cakupan: Fitur Lemah Individu (IWF), Fitur Lemah Umum (CWF), Fitur Lemah Global (GWF). Pertama, simulasi penyerangan dijalankan. Kemudian, efek dari penyerangan ini terhadap model berbasis *Support Vector Machine* (SVM) dibanding dengan model dasar SVM dianalsis untuk menidentifikasi fitur lemah. Beberapa algoritma diimplementasikan untuk mengidentifikasi fitur lemah, yakni *Baseline Feature Rank* (BFR)*, Backward Feature Elimination* (BFE)*, Enhanced Feature Rank* (EFR)*, and Multi Model Recursive Feature Elimination* (MMRFE). Pengujian hipotesis membuktikan bahwa penghapusan IWF, CWF, dan GWF dapat menjaga reliabilitas model dari serangan hingga level tertentu. Dengan hasil terbaik menggunakan BFE diikuti MMRFE, BFR, dan EFR.

Kata kunci: biometrik perilaku, otentikasi, SVM, impersonasi, fitur lemah

ABSTRACT

WEAK FEATURES REMOVAL VIA FEATURE RANKING TO PREVENT IMPERSONATION ATTACK ON SMARTPHONE BEHAVIOR BIOMETRIC SYSTEM

By

Afif Izzul Falakh

20/466392/PPA/05958

Our dependence of smartphone and internet has brought many opportunities for the growth of smartphone based online services. Some of these services are even deal with private and sensitive information such as mobile banking, electronic wallet, and the likes. Since that, multiple security measures are implemented to have the system as secure as possible. One of the security method which is getting more attention from researcher is behavioral biometrics system (BBS), especially the one based on smartphone swipe and handling behavior. This type of security system provide non-intrusive continuous authentication of the user which can protect the user in-between primary authentication system. However, some research shows the existence of impersonation attack, where an attacker is trying to mimic the user behavior to fool the system.

Thus, this research proposed a method to identify the existence of weak features in several scopes: Individual Weak Features (IWF), Common Weak Features (CWF), and General Weak Features (GWF). First, a simulated attack is carried out. Then, the effect on these attack to the augmented Support Vector Machine (SVM) model is compared with the base SVM model is analyzed to identify the weak features. Several algorithm is implemented to identify the weak features namely Baseline Feature Rank (BFR), Backward Feature Elimination (BFE), Enhanced Feature Rank (EFR), and Multi Model Recursive Feature Elimination (MMRFE). By hypothesis testing the IWF, CWF, and GWF is proven to maintain reliability of the model to certain level. With the best one using BFE followed by MMRFE, BFR, and EFR.

Keywords: behavioral biometrics, authentication, SVM, impersonation, weak features