Evaluasi *User-Adaptive* Fitur dalam *Keystroke Biometric* menggunakan Beragam Metode *Distance Similarity*

Irsyad Muhamad Al Anshori[1], Prasti Eko Yunanto[2], Farah Afianti[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]irsyadlibra@student.telkomuniversity.ac.id, [2]gppras@telkomuniversity.ac.id, [3]farahafi@telkomuniversity.ac.id,

Abstrak

Pertumbuhan pengguna *smartphone* global diperkirakan mencapai 5,25 miliar pada tahun 2023. Hal tersebut meningkatkan kebutuhan akan sistem *authentication* yang aman. Meskipun metode konvensional seperti PIN dan kata sandi mudah diimplementasikan, pengguna dikenali berdasarkan teks, sehingga menimbulkan risiko keamanan. Sebagai solusi, kombinasi sistem *authentication biometric* diperkenalkan. *Keystroke biometric* sebagai *biometric* dengan karakteristik *behavioral* telah banyak diteliti dan menjadi fokus penelitian. Penelitian ini mengevaluasi *user-adaptive feature* dalam *keystroke biometric* menggunakan beragam metode *distance similarity*. Model *keystroke* dibangun dengan *digraph* yang merepresentasikan informasi *keys* dan waktu pengetikan, seperti DD, UD, UU, DU, dan *Duration*. Model ini disimpan dan dibandingkan dengan model pengguna *legitimate* untuk mendapatkan nilai *similarity score*. Performansi dievaluasi dengan *Equal Error Rate* (EER), *False Acceptance Rate* (FAR), dan *False Rejection Rate* (FRR). Hasil menunjukkan metode *Euclidean* memberikan keseimbangan performa terbaik dengan EER terendah sebesar 0,4588 pada skenario I dan 0,4598 pada skenario II. Metode lain, seperti *Soergel*, *Canberra*, *Matusita*, dan *Manhattan*, lebih baik dalam mencegah penerimaan *impostor*, namun meningkatkan risiko penolakan pengguna *legitimate*. Pemilihan metode harus disesuaikan dengan prioritas antara keamanan dan kenyamanan pengguna dalam sistem *keystroke biometric*.

Kata Kunci*: biometric, biometric behavioral, keystroke biometric, user-adaptive feature, distance similarity.*