Penerapan Algoritma Ensemble Learning Berdasarkan Decision Tree Based Model untuk Mendeteksi Serangan Video Injection

Muhammad Naufal Abdillah[1], Vera Suryani[2],

[1,2]Fakultas Informatika, Universitas Telkom, Bandung
[1]@students.telkomuniversity.ac.id, [2]@telkomuniversity.ac.id

Abstrak

Dalam beberapa dekade terakhir, teknologi deteksi biometrik dengan cepat mendapatkan popularitas dalam memperkuat keamanan tanpa memberikan beban tambahan pada seseorang untuk mengingat kata sandi atau membawa perangkat lain, dan di antara sistem yang sering diterapkan, penggunaan sistem pengenalan wajah memiliki peran penting, karena penggunaannya yang luas mulai dari sistem ponsel cerdas hingga imigrasi. Namun karena penggunaannya yang luas, terdapat peningkatan kekhawatiran terhadap ancaman keamanan yang mencoba melewati sistem, dan salah satu ancaman tersebut adalah serangan *video injection*, yaitu suatu bentuk serangan yang mencoba menipu sensor-sensor sistem, dengan menggunakan video atau gambar yang dimasukkan langsung ke aliran data, atau dengan masker fisik. Untuk mencegah terjadinya kerusakan maka diperlukan deteksi dini terhadap serangan-serangan tersebut, dan salah satu cara untuk mendeteksinya adalah melalui pembelajaran mesin, khususnya dengan menggunakan algoritma *ensemble learning*. Penelitian ini menggunakan algoritma *ensemble learning stacking* dengan menggabungkan algoritma XGBoost, dan LightGBM. Model *ensemble* menghasilkan nilai f1-score sebesar 0.9217 dengan akurasi 92.5%, sedangkan estimator dasar menghasilkan kinerja yang lebih rendah.