

ABSTRAK

Di era globalisasi, perkembangan internet dalam teknologi informasi menyebabkan tingkat kejahatan yang merugikan banyak pihak. Hal ini disebabkan adanya gangguan ancaman (*threat*) dan kerentanan (*vulnerability*) terhadap keamanan sistem. *Threat* dan *vulnerability* ini bisa ditemukan pada Twitter karena banyaknya pengguna memposting kejahatan sistem secara bebas pada Twitter.

Pada penelitian Tugas Akhir ini, dilakukanlah pendeteksian pada teks *threat* dan *vulnerability* pada Twitter menggunakan algoritma *Support Vector Machine* (SVM). Proses pada penelitian ini yaitu teks akan dikumpulkan ke dalam *dataset*, dilabeli, dilakukan *text pre-processing*, selanjutnya diberikan pembobotan yaitu dengan metode POS Tagging dan *Term Frequency – Inverse Document Frequency* (TF-IDF), dan data akan di *training* agar algoritma SVM dapat mengklasifikasikan data tersebut untuk didapatkan nilai *accuracy*, *precision*, *recall* dan *F1-Score*.

Hasil dari penelitian Tugas Akhir ini mengambil data Twitter dengan total 4270 data, dengan 2135 data positif dan 2135 data negatif. Sistem klasifikasi ini bekerja dengan menggunakan algoritma *Support Vector Machine*. Pada penelitian ini digunakan *dataset* 90% untuk data pelatihan (*training data*) dan 10% untuk data pengujian (*testing data*). Pengujian parameter Gamma dan C dengan nilai terbaik adalah 30000 dan 1. Dari hasil pengujian tersebut, didapatkan nilai *accuracy* sebesar 89%, *precision* sebesar 89%, *recall* sebesar 89% dan *F1-Score* 89%.

Kata Kunci: *Vulnerability, Support Vector Machine, Text Pre-processing, TF-IDF, Threat, Twitter*