

## ABSTRACT

*In the era of globalization, the development of the internet in information technology causes a crime rate that is detrimental to many parties. This is due to the presence of threats and vulnerability to system security. Threats and vulnerabilities can be found on Twitter because many users post system crimes freely on Twitter.*

*In this final project, the detection of threats and vulnerability on Twitter is carried out using the Support Vector Machine (SVM) algorithm. The process in this research is that the text will be collected into a dataset, labeled, text pre-processing is carried out, then given weighting, namely the POS Tagging and Term Frequency – Inverse Document Frequency (TF-IDF) methods, and the data will be trained so that the SVM algorithm can classify the data to obtain accuracy, precision, recall and F1-Score values.*

*The results of this final project take twitter data with a total of 4270 data, with 2135 positive data and 2135 negative data. This classification system works by using the Support Vector Machine algorithm. In this research, 90% dataset is used for training data and 10% for testing data. The best Gamma and C parameter tests are 30000 and 1. From the performance test results, the accuracy value is 89%, precision is 89%, recall is 89% and F1-Score is 89%.*

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