

ABSTRAK

Febriandi. 2025. *Analisis Perbandingan Algoritma Support Vektor Machine (SVM) dan Long Short-Term Memory (LSTM) dalam Deteksi Website Phishing*, Skripsi. Tanjungpinang: Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji. Pembimbing I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Pembimbing II: Novrizal Fattah Fahmitra, S.Kom., M. Kom.

Phishing adalah salah satu metode rekayasa sosial yang sangat ampuh dalam kejahatan siber karena memiliki tingkat kesuksesan yang cukup besar. Metode ini bekerja dengan cara memancing rasa ingin tahu korban atau memanfaatkan kurangnya pengetahuan mereka untuk mendapatkan data pribadi, hak akses, atau menyebarkan *malware*. Website *phishing* merupakan varian *phishing* yang menggunakan situs web sebagai media utamanya. Dalam praktiknya, korban akan diarahkan baik secara langsung maupun tidak langsung menuju situs palsu tersebut. Setelah itu, korban dipancing untuk memberikan informasi sensitif atau memberikan akses yang diminta, baik dengan sengaja maupun tanpa disadari.

Penelitian ini membandingkan dua algoritma *machine learning*, yaitu *Support Vektor Machine* dan *Long Short-Term Memory* dalam mendeteksi website *phishing*. Hasil pengujian menunjukkan bahwa model LSTM memiliki performa lebih tinggi dibandingkan dengan SVM dimana LSTM mencapai *accuracy* sebesar 99,35%, *precision* 99,8% *recall* 98,9% dan *F1-Score* 99,35%. Sementara itu algoritma SVM mencapai akurasi *accuracy* sebesar 97,3%, *precision* 97,11% *recall* 97,5% dan *F1-Score* 97,31%. Temuan ini menunjukkan bahwa kedua model mampu melakukan deteksi *phishing* dengan baik, namun algoritma LSTM lebih unggul dari algoritma SVM.

Kata kunci: Deteksi Website *Phishing*, *Support Vektor Machine* (SVM), *Long Short-Term Memory* (LSTM), *Confusion Matrix*

ABSTRACT

Febriandi. 2025. *Comparative Analysis of Support Vector Machine (SVM) and Long Short-Term Memory (LSTM) Algorithms in Phishing Website Detection*, Thesis. Tanjungpinang: Informatics Engineering Study Program, Department of Electrical Engineering and Informatics, Faculty of Engineering and Maritime Technology, University of Maritim Raja Ali Haji. Advisor I: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. Advisor II: Novrizal Fattah Fahmitra, S.Kom., M. Kom.

Phishing is one of the most powerful social engineering methods in cybercrime as it has a high success rate. It works by piquing a victim's curiosity or capitalizing on their lack of knowledge to obtain personal data, access rights, or spread malware. Website phishing is a variant of phishing that uses websites as its main medium. In practice, the victim will be directed either directly or indirectly to the fake site. After that, the victim is lured into providing sensitive information or granting requested access, either intentionally or unwittingly.

This research compares two machine learning algorithms, namely Support Vector Machine and Long Short-Term Memory in detecting phishing websites. The test results show that the LSTM model has better performance compared to SVM where LSTM achieves accuracy of 99.35%, precision 99.8% recall 98.9% and F1-Score 99.35%. Meanwhile, the SVM algorithm achieved 97.3% accuracy, 97.11% precision 97.5% recall and 97.31% F1-Score. This finding shows that both models are able to perform phishing detection well, but the LSTM algorithm is superior to the SVM algorithm.

Keywords: *Phishing Website Detection, Support Vector Machine (SVM), Long Short-Term Memory (LSTM), Confusion Matrix*