

ABSTRAK

Penelitian ini berjudul “Deteksi Email *Phishing* Menggunakan Model *Transformer* BERT dengan integrasi Fitur URL”. Tujuan penelitian ini adalah menganalisis pengaruh penambahan fitur URL terhadap performa model BERT dalam mendeteksi email *phishing*. Penelitian menggunakan metode eksperimen dengan dua skenario pengujian, yaitu model BERT sebagai model dasar (*baseline*) dan model BERT yang diintegrasikan dengan sembilan fitur URL menggunakan metode *feature fusion*. Data penelitian terdiri atas dataset pertama sebanyak 39.154 email dan dataset kedua sebanyak 5.001 email. Tahapan penelitian meliputi *preprocessing* teks email, ekstraksi dan normalisasi fitur URL, implementasi model, serta evaluasi hasil. Evaluasi dilakukan menggunakan *confusion matrix* dan metrik *accuracy*, *precision*, *recall*, serta *F1-score*. Hasil penelitian menunjukkan bahwa kedua model memiliki performa yang baik dalam mendeteksi email *phishing*. Pada dataset pertama, kedua model menunjukkan performa yang relatif setara dengan seluruh metrik berada di atas 99%, meskipun model BERT + URL menghasilkan *recall* yang lebih tinggi. Pada dataset kedua, model BERT + URL memperoleh *accuracy* 98,60%, *precision* 96,82%, *recall* 98,21%, dan *F1-score* 97,51%, lebih tinggi dibandingkan model BERT. Hasil penelitian menunjukkan bahwa integrasi fitur URL dapat meningkatkan kemampuan deteksi *phishing*, terutama dalam mengurangi email *phishing* yang tidak terdeteksi.

Kata kunci: Email *Phishing*, BERT, Fitur URL, Deteksi *Phishing*, *Feature Fusion*

ABSTRACT

This study is entitled "Phishing Email Detection Using the BERT Transformer Model with Integrated URL Features." The objective of this study is to analyze the effect of integrating URL features on the performance of the BERT model in detecting phishing emails. An experimental method was employed using two testing scenarios: the baseline BERT model and a BERT model integrated with nine URL features through a feature fusion approach. The study utilized two datasets consisting of 39,154 emails in the first dataset and 5,001 emails in the second dataset. The research process included email text preprocessing, URL feature extraction and normalization, model implementation, and performance evaluation. The models were evaluated using a confusion matrix along with accuracy, precision, recall, and F1-score metrics. The results show that both models achieved strong performance in phishing email detection. On the first dataset, the two models demonstrated comparable performance, with all evaluation metrics exceeding 99%, although the BERT + URL model achieved a higher recall value. On the second dataset, the BERT + URL model achieved an accuracy of 98.60%, precision of 96.82%, recall of 98.21%, and an F1-score of 97.51%, outperforming the baseline BERT model. These findings indicate that integrating URL features into the BERT model can improve phishing email detection performance, particularly by reducing the number of phishing emails that remain undetected.

Keywords: Email Phishing, BERT, URL Feature, Phishing Detection, Feature Fusion