ABSTRAK

Phishing merupakan teknik penipuan dengan meniru situs web resmi untuk mengelabui pengguna agar menyerahkan informasi pribadi atau aset digital, dan ancaman ini semakin serius pada ekosistem Web3 melalui kampanye *airdrop* dan *decentralized application* (*dApp*) palsu yang memanfaatkan *crypto drainer* untuk mencuri aset kripto pengguna. Permasalahan utamanya adalah pendekatan berbasis *blacklist* belum efektif mendeteksi serangan *zero-day Phishing*, sementara analisis tunggal seperti URL saja masih rentan dimanipulasi. Penelitian ini bertujuan untuk mengembangkan sistem deteksi *phishing* yang menggabungkan analisis domain dan analisis konten HTML, yang diimplementasikan ke dalam ekstensi *browser* agar dapat bekerja secara *real-time*. Penelitian ini menggunakan pendekatan *transformer* BERT, yaitu model *pre-trained* DomURLs-BERT yang di-*fine-tune* menggunakan dataset domain, serta algoritma XGBoost yang dilatih menggunakan fitur hasil ekstraksi dari HTML. Hasil dari kedua model tersebut kemudian digunakan dan digabungkan untuk diklasifikasikan ulang menggunakan algoritma XGBoost guna menghasilkan keputusan klasifikasi akhir. Model DomURLs-BERT (Domain) dan XGBoost (HTML) masing-masing mencapai F1-*Macro* sebesar 91,63% dan 98,48% pada *dataset* pengujiannya sendiri. Ketika dievaluasi ulang pada *test set* yang sama dengan model klasifikasi akhir, F1-*Macro* keduanya adalah 93,05% dan 93,47%, sementara model klasifikasi akhir berbasis XGBoost yang menggabungkan kedua model tersebut mencapai F1-*Macro* sebesar 97,61%, meningkat masing-masing 4,56% dan 4,14% dari model domain dan model HTML. Hasil ini menunjukkan bahwa penggabungan analisis domain dan analisis HTML mampu meningkatkan akurasi deteksi *phishing* dibandingkan penggunaan salah satu analisis secara tunggal. Selain itu, sistem ini telah diimplementasikan ke dalam ekstensi *browser* yang mampu memberikan perlindungan secara *real-time* bagi pengguna.

Kata kunci: *Browser Extension, DomURLs-BERT, Phishing Detection, Web3, XGBoost*

ABSTRACT

Phishing is a fraudulent technique that imitates legitimate websites to deceive users into disclosing personal information or digital assets. This threat has become increasingly serious in the *Web3* ecosystem through fake *airdrop* campaigns and malicious *decentralized applications* (*dApps*) that use *crypto drainers* to steal users' cryptocurrency assets. The main challenge is that blacklist-based approaches are ineffective in detecting zero-day *phishing* attacks, while single-source analysis, such as URL-based detection alone, remains vulnerable to manipulation. This study aims to develop a *phishing* detection system that combines domain analysis and HTML content analysis, implemented as a browser extension to operate in real time. The study employs the BERT transformer approach, using the pre-trained DomURLs-BERT model fine-tuned on a domain dataset, and the XGBoost algorithm trained on features extracted from HTML. The outputs of both models are then combined and reclassified using XGBoost to produce the final classification decision. The DomURLs-BERT (Domain) and XGBoost (HTML) models achieved F1-Macro scores of 91.63% and 98.48%, respectively, on their respective test datasets. When reevaluated on the same test set used for the final classification model, their F1-Macro scores were 93.05% and 93.47%, respectively, while the final XGBoost classification model combining both analyses achieved an F1-Macro score of 97.61%, representing improvements of 4.56% and 4.14% over the domain and HTML models, respectively. These results demonstrate that combining domain and HTML analysis can improve *phishing* detection performance compared with using either analysis independently. Furthermore, the system has been implemented as a browser extension capable of providing real-time protection for users.

Keywords: Browser Extension, DomURLs-BERT, Phishing Detection, Web3, XGBoost