

ABSTRAK

Malicious URL (Uniform Resource Locator), atau biasa disebut dengan situs web jahat adalah ancaman yang umum dan serius bagi keamanan siber. URL berbahaya menampung konten yang tidak diminta (*spam, phishing, unduhan drive-by, dll.*) dan memikat pengguna yang tidak menaruh curiga untuk menjadi korban penipuan (kehilangan uang, pencurian informasi pribadi, dan instalasi *malware*), dan menyebabkan kerugian miliaran dolar setiap tahun. Salah satu cara untuk mendeteksi *Malicious Website* yaitu dengan mendeteksi dini lewat URL nya. Dalam penelitian ini, dilakukan pendeteksian *Malicious URL* dengan menggunakan Leksikal Fitur untuk ekstraksi fiturnya dan *Random Forest* untuk pengklasifikasiannya. Dalam pengeksraksiannya, metode yang digunakan adalah berdasarkan karakteristik dan atribut dari URL itu sendiri.

Pada penelitian ini, dataset yang diperoleh memiliki tingkat ketidakseimbangan data yang tinggi. Maka dari itu dilakukan *Random Oversampling* untuk proses penyeimbangan datanya. Lalu pengujian model pada penelitian ini difokuskan pada pengoptimasian fitur leksikal yang digunakan dalam mengklasifikasi jenis *malicious url* yaitu *benign, defacement, malware, dan phishing* menggunakan 10 fitur, 15 fitur, 19 fitur, dan 23 fitur untuk mencari hasil akurasi klasifikasi terbaik dengan *8-fold cross validation* untuk pengujiannya.

Penelitian ini mencapai kesimpulan bahwa penambahan fitur leksikal yang optimal dapat meningkatkan akurasi deteksi URL berbahaya. Melalui eksperimen dengan variasi fitur, hasil terbaik diperoleh dengan 23 fitur leksikal, mencapai akurasi 97,6%. Namun, ditemukan bahwa pendeteksian URL statis tanpa tanda "/" diakhirnya secara konsisten terdeteksi sebagai *phishing*, menunjukkan tantangan dalam membedakan URL berbahaya dan aman secara akurat. Dengan demikian, penelitian ini memberikan wawasan penting untuk mengoptimalkan algoritma Random Forest dalam mendeteksi URL berbahaya, mengingat kompleksitas ancaman siber saat ini.

Kata Kunci: *Lexical Features, Random Forest, Confusion Matrix, K-Fold Cross Validation, Random Oversampling, Malicious, URL.*