ABSTRAK

URL berbahaya merupakan tantangan serius dalam keamanan siber, mengingat semakin banyaknya ancaman seperti *malware, ransomware, spyware, phishing, defacement, dan trojan*. Deep learning memiliki kemampuan untuk mempelajari pola yang kompleks pada data secara otomatis dan efektif, sehingga dapat digunakan untuk mendeteksi anomali dan pola berbahaya pada URL. Penelitian sebelumnya telah mengusulkan berbagai metode untuk mendeteksi URL berbahaya, termasuk metode berbasis daftar hitam dan fitur URL. Namun, metode-metode ini sering kali kurang efektif dalam menangani pola serangan yang terus berkembang. Dalam mendeteksi URL berbahaya, menurut berbagai penelitian, penerapan deep learning memiliki potensi untuk meningkatkan efisiensi dan akurasi proses, tetapi masih ada peluang untuk lebih mengoptimalkan efisiensi dan akurasi. Makalah ini bertujuan untuk mengembangkan sistem pendeteksi URL berbahaya menggunakan deep learning berbasis ekstraksi fitur. Metode ini akan meningkatkan representasi data melalui analisis teks dan transformasi data tersebut, serta pemilihan fitur-fitur penting dari dataset. Penelitian ini menggunakan dataset multiclass yang mencakup kategori seperti benign, defacement, phishing, dan malware. Di antara ukuran evaluasi yang akan diterapkan dalam proses evaluasi model adalah sebagai berikut: akurasi, presisi, recall, F1-score, dan rata-rata makro. Diyakini bahwa metodologi yang digunakan dalam penelitian ini akan secara signifikan meningkatkan keamanan siber dengan membuat sistem pendeteksian URL berbahaya menjadi lebih terkurasi dan efektif. Di antara desain yang diuji, model GRU mencapai akurasi tertinggi sebesar 92,59%.

Kata kunci: URL Berbahaya, Deep Learning, Ekstraksi Fitur, Keamanan Siber, Deteksi URL