ABSTRAK

Penelitian ini menguraikan pengembangan pendekatan yang jarang digunakan dalam mendeteksi obfuscated malware, seperti Trojan, Spyware, dan Ransomware, yang mengubah kode sumber mereka untuk mengelabui deteksi tradisional. Contohnya, Trojan menyamar sebagai aplikasi benign, Spyware menyusup dalam aplikasi bersih untuk mencuri informasi, dan Ransomware membatasi akses ke data penting dengan tuntutan tebusan. Ketiga jenis malware ini saling terhubung, membentuk serangan yang kompleks dan berbahaya bagi keamanan sistem. Penelitian ini mengeksplorasi implementasi metode Deep Neural Decision Forest (DNDF) untuk mendeteksi obfuscated malware, mengoptimalkan model decision forest dan deep neural network. Evaluasi menggunakan 10-fold cross-validation menunjukkan ketangguhan model terhadap variasi data dan keseimbangan. Penggunaan Extra Trees dalam pelatihan mendukung identifikasi fitur relevan, meningkatkan ketepatan deteksi, terutama dalam kasus dataset tidak seimbang. Penelitian ini memberikan kontribusi pada pengembangan solusi deteksi obfuscated malware dengan pendekatan DNDF dan strategi evaluasi yang matang. Hasil penelitian ini diharapkan dapat memberikan kontribusi yang berarti dalam meningkatkan keamanan sistem terhadap ancaman malware yang semakin kompleks.

Kata Kunci: deteksi malware, Obfuscated malware, Neural Decision Forest, Feature Selection, keamanan sistem, Extra Trees Classifier.