

## ABSTRAK

Perkembangan *malware* yang pesat menimbulkan tantangan baru dalam menjaga keamanan sistem informasi. Data yang dipublikasikan oleh *G Data Security Labs*, tahun 2022 tercatat lebih dari 50 juta *malware* baru. Dalam menghadapi ancaman ini, penelitian ini mengimplementasikan tiga algoritma machine learning, yaitu *Logistic Regression*, *XGBoost*, dan *Convolutional Neural Network (CNN)* untuk klasifikasi *malware* berdasarkan analisis data statis. Dataset berjumlah 130.046 sampel *malware* dan benign diperoleh dari Kaggle dan VirusShare. Tahapan penelitian meliputi pra-pemrosesan data, pembagian dataset dengan rincian 80% data latih dan 20% data uji, pelatihan model, dan evaluasi performa dengan metrik akurasi, presisi, *recall*, dan *F1-score*. Hasil evaluasi menunjukkan bahwa *XGBoost* dengan akurasi 98,89%, *precision* 98,91%, *recall* 98,88%, dan *F1-score* 98,89%. Selanjutnya, algoritma CNN memiliki performa terbaik kedua dengan akurasi 99,31%, *precision* 99,30%, *recall* 99,33%, dan *F1-score* 99,31%. Terakhir, algoritma *Logistic Regression* mencatat akurasi 96,11%, *precision* 96,07%, *recall* 96,15%, dan *F1-score* 96,11%. Dengan demikian, CNN terbukti menjadi model paling efektif untuk klasifikasi *malware* dalam konteks data dan metode yang digunakan, berkontribusi pada pengembangan sistem deteksi *malware* yang lebih akurat dan efisien.

**Kata Kunci:** *Machine Learning, Logistic Regression, XGBoost, Convolutional Neural Network, Malware*