

ABSTRAK

Perkembangan teknologi digital membawa dampak positif sekaligus ancaman dalam bentuk kejahatan siber, salah satunya adalah *malware*. *Malware* menyebar melalui *email*, situs *web*, dan perangkat USB dengan berbagai tipe seperti *trojan* dan *ransomware*. Metode analisis berbasis *cloud* yang umum digunakan dinilai memiliki keterbatasan seperti ketergantungan *internet*, risiko penyebaran, serta biaya tinggi. Penelitian ini mengangkat permasalahan tingginya risiko dan biaya dalam penggunaan sistem analisis *malware* berbasis *cloud*, khususnya pada lingkungan *airgap* yang membutuhkan isolasi penuh.

Sebagai solusi, dikembangkan sistem analisis *malware* berbasis *machine learning* dengan algoritma *Bidirectional Long Short-Term Memory* (Bi-LSTM) yang dijalankan secara lokal pada perangkat *mini-PC*. Sistem ini dirancang tanpa koneksi *internet* dengan fitur antarmuka pengguna menggunakan PyQt5 dan laporan otomatis melalui ReportLab. Pendekatan yang digunakan berbasis analisis dinamis untuk mengamati perilaku *malware* secara langsung.

Hasil pengujian menunjukkan sistem mampu mengklasifikasikan *malware* dengan akurasi sebesar 93% dan klasifikasi multikelas sebesar 80% menggunakan Bi-LSTM. Sistem juga terbukti aman dan stabil dalam lingkungan terisolasi, serta memberikan waktu analisis lebih cepat dibanding metode konvensional. Kesimpulannya, sistem ini merupakan solusi efektif dan efisien untuk kebutuhan analisis *malware* di lingkungan terbatas seperti *airgap*.

Kata kunci: *malware*, Bi-LSTM, *airgap*, *machine learning*, *sandbox*