

ABSTRAK

Keamanan pada sistem pemungutan suara elektronik berbasis blockchain menjadi perhatian utama dalam era digital. Penelitian ini bertujuan untuk membangun model prediksi terhadap transaksi tidak valid pada sistem e-voting berbasis blockchain menggunakan pendekatan data science. Dua algoritma yang digunakan adalah Random Forest dan Support Vector Machine (SVM). Dataset yang digunakan berisi lebih dari 500.000 entri transaksi blockchain, dengan proses *resampling* menggunakan SMOTE untuk mengatasi ketidakseimbangan kelas antara transaksi valid dan tidak valid.

Model awal menunjukkan bahwa baik Random Forest maupun SVM gagal mengenali transaksi tidak valid, dengan nilai recall sebesar 0.00. Setelah dilakukan tuning parameter dan penerapan SMOTE, performa model meningkat secara signifikan. Model SVM menghasilkan recall tertinggi pada kelas minoritas sebesar 57%, meskipun akurasi total menurun. Sebaliknya, Random Forest menunjukkan recall sebesar 42%, dengan akurasi yang lebih tinggi.

Hasil ini menunjukkan bahwa pendekatan machine learning mampu meningkatkan sensitivitas deteksi terhadap transaksi anomali dalam sistem e-voting, meskipun masih terdapat trade-off terhadap precision dan akurasi umum. Penelitian ini memberikan dasar awal untuk pengembangan sistem pendukung keamanan pada voting elektronik dengan bantuan prediksi berbasis data.

.

Kata Kunci: e-voting, blockchain, Random Forest, SVM, data mining, ketidakseimbangan data, keamanan sistem.