

Abstrak

Di era digital seperti sekarang, menggunakan mata uang digital atau *cryptocurrency* dalam berbagai transaksi virtual menjadi sesuatu yang lazim karena dianggap memudahkan dalam hal bertransaksi. *Cryptocurrency* adalah mata uang digital yang digunakan untuk bertransaksi virtual dalam jaringan internet. Jenis-jenis *cryptocurrency* yang sering digunakan antara lain *Litecoin*, *Ethereum*, *Monero*, *Ripple*, dan *Bitcoin*. Meskipun *cryptocurrency* memiliki sandi-sandi rahasia yang cukup rumit dan kompleks yang berfungsi untuk melindungi dan menjaga keamanan mata uang digital, tidak menutup kemungkinan dapat diretas oleh peretas yang lihai. Peretasan terkait *cryptocurrency* merupakan salah satu jenis kejahatan digital yang sangat merugikan dan berbahaya. Contohnya beberapa tahun terakhir, kasus peretasan pada transaksi *bitcoin* menggunakan *ransomware* semakin marak. *Ransomware* merupakan perangkat lunak berbahaya yang diam-diam menginfeksi perangkat korban, dan tiba-tiba meminta pembayaran tebusan untuk mendekripsi data yang telah dienkripsi. Sesuai namanya, *ransom* yang berarti tebusan, jenis *malware* ini bertujuan untuk memeras korban yang komputernya terinfeksi *ransomware* dengan meminta sejumlah uang sebagai tebusan. Oleh karena itu, dibangun sebuah rancangan berupa sistem deteksi *ransomware* berdasarkan data pencurian *bitcoin* yang tersedia sehingga dapat meminimalisir serangan peretasan terhadap *cryptocurrency* dikemudian hari. Sistem deteksi *ransomware* dibangun menggunakan metode jaringan saraf tiruan *backpropagation* dengan menggunakan perangkat lunak WEKA. Hasil terbaik pada pengujian data yaitu dengan menggunakan parameter jumlah 9 *neuron hidden layer*; *learning rate* 0,1; dan jumlah iterasi 5000 menghasilkan tingkat akurasi sebesar 97%.

Kata kunci : *cryptocurrency*, *bitcoin*, deteksi *ransomware*, jaringan saraf tiruan, *backpropagation*, *weka*.