JURNAL PENDIDIKAN INDONESIA
p-ISSN : 2745-7141 e-ISSN : 2746-1920
Jurnal Pendidikan Indonesia
Vol. 6 No. 3 Maret 2025

Phishing Detection on Ethereum Network Menggunakan Metode Machine Learning

Windhy Rokhmat Rosmantyo*, Dhani Ariatmanto
Universitas AMIKOM Yogyakarta, Indonesia
Email: windhy.rosmantyo@students.amikom.ac.id*

Kata kunci: Phishing, Ethereum, Machine Learning, Graph Convolutional Networks, Enhanced Graph Attention Networks, Deteksi Keamanan

ABSTRAK

Penelitian ini membahas tentang deteksi phishing pada jaringan Ethereum menggunakan metode machine learning, khususnya *Graph Convolutional Networks* (GCNs) dan *Enhanced Graph Attention Networks* (EGAT). Latar belakang penelitian ini didasari oleh meningkatnya serangan phishing di ekosistem blockchain yang dapat mengancam keamanan finansial pengguna. Tujuan penelitian adalah untuk menganalisis tingkat kejadian serangan phishing serta mengembangkan metode deteksi yang efektif dan efisien. Metode yang digunakan mencakup pengumpulan data transaksi Ethereum dan data phishing, diikuti dengan ekstraksi fitur, pelatihan model machine learning, dan evaluasi menggunakan metrik seperti akurasi, precision, recall, dan F-score. Gap research yang diidentifikasi adalah kurangnya fokus pada deteksi phishing tahap awal di jaringan Ethereum serta tidak optimalnya metode yang ada dalam mengenali pola transaksi yang kompleks. Hasil penelitian menunjukkan bahwa EGAT memiliki akurasi sebesar 93,6%, lebih baik dibandingkan GCNs yang mencapai 91,2%. Kesimpulan dari penelitian ini adalah bahwa metode EGAT lebih unggul dalam mendeteksi aktivitas phishing, memberikan kontribusi signifikan terhadap keamanan di jaringan Ethereum.

Keywords: *Phishing, Ethereum, Machine Learning, Graph Convolutional Networks, Enhanced Graph Attention Networks, Security Detection*

ABSTRACT

This study discusses phishing detection on the Ethereum network using machine learning methods, specifically Graph Convolutional Networks (GCNs) and Enhanced Graph Attention Networks (EGAT). The background of this research is based on the increasing number of phishing attacks in the blockchain ecosystem that can threaten the financial security of users. The research aims to analyze the incidence rate of phishing attacks and develop effective and efficient detection methods. The methodology includes data collection from Ethereum transactions and phishing activities, followed by feature extraction, machine learning model training, and evaluation using metrics such as accuracy, precision, recall, and F-score. The identified research gap is the lack of focus on early-stage phishing detection in the Ethereum network and the suboptimal performance of existing methods in recognizing complex transaction patterns. The results indicate that EGAT achieves an accuracy of 93.6%, outperforming GCNs, which reach 91.2%. The conclusion of this research is that the EGAT method is superior in detecting

phishing activities, providing significant contributions to security in the Ethereum network.

PENDAHULUAN

Blockchain adalah basis data terdistribusi yang menyimpan catatan transaksi secara kronologis dan terenkripsi, dan data tersebut bersifat terdesentralisasi, saling mendukung, dan terhubung dalam rantai terkunci sehingga tidak dapat dimanipulasi. Untuk waktu yang cukup lama, data dan interaksi masyarakat disimpan dan dieksekusi melalui pihak ketiga yang terpusat dan terpercaya, seperti pemerintah atau perusahaan. Hal ini menyebabkan masyarakat menghadapi biaya tinggi, silo data, dan ketidakstabilan akibat perubahan organisasi. Dengan menggunakan teknologi blockchain, data didistribusikan di seluruh dunia, dan masyarakat tidak perlu bergantung pada pihak ketiga tradisional. Ini memberikan cara yang lebih dapat diandalkan untuk kepercayaan masyarakat, sambil juga mengurangi jumlah biaya yang dibebankan oleh perantara (Chen et al., 2021).

Ethereum saat ini merupakan platform blockchain terbesar yang mendukung kontrak pintar dan mata uang kripto terkaitnya, ether, yang merupakan kripto terbesar kedua. Namun, seiring dengan perkembangannya yang cepat, Ethereum juga telah menjadi tempat berbagai kejahatan dunia maya. Initial Coin Offering (ICO) adalah metode pendanaan untuk industri blockchain, yang merujuk pada pendanaan melalui penerbitan token. Namun, hingga saat ini, lebih dari 10% ICO yang dirilis di Ethereum dilaporkan mengalami berbagai penipuan, termasuk phishing, skema Ponzi, dll. Menurut laporan Chainalysis, penyedia perangkat lunak investigasi dan manajemen risiko untuk mata uang virtual, terdapat 30.287 korban kehilangan $225 juta pada paruh pertama tahun 2017, menunjukkan bahwa keamanan finansial telah menjadi isu kritis dalam ekosistem blockchain (Hou et al., 2022).

Salah satu bentuk serangan yang sering terjadi adalah *social engineering*, suatu tindakan yang melibatkan manipulasi terhadap seseorang untuk melakukan tindakan yang tidak menjadi prioritas utama atau belum menjadi fokus target. Tindakan ini dapat mencakup upaya memperoleh informasi, mendapatkan akses, atau mendorong target untuk melakukan suatu tindakan khusus. Ada beragam jenis serangan dalam social engineering, dan salah satu yang dikenal luas adalah phishing. Phishing merupakan tindakan pencurian informasi yang menggunakan surat elektronik sebagai sarana untuk menyampaikan informasi. Penyerang mencoba untuk membuat surat tersebut terlihat seolah-olah berasal dari pihak yang terpercaya, kemudian meminta pengguna untuk mengisi formulir yang disediakan dengan informasi tertentu (R. N. S. Putri, 2022).

Phishing adalah upaya untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan detail kartu kredit dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik (Bachtiar, 2023). Phishing adalah suatu teknik penipuan daring yang dilakukan oleh pihak yang tidak sah dengan tujuan untuk memperoleh informasi rahasia seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya . Metode ini biasanya melibatkan upaya untuk membuat korban percaya bahwa mereka berinteraksi dengan entitas tepercaya atau terkait dengan kegiatan yang sah. Umumnya,

serangan phishing terjadi melalui pesan elektronik, seperti email atau pesan teks, yang dirancang agar terlihat seolah-olah berasal dari organisasi resmi, seperti bank, lembaga keuangan, atau penyedia layanan online. Pesan tersebut seringkali mengandung pemberitahuan palsu atau iming-iming untuk memancing korban agar memberikan informasi pribadi mereka atau mengklik tautan yang dapat mengarahkan mereka ke situs web palsu. Salah satu bentuk phishing yang umum adalah "*spear phishing*," di mana serangan ditargetkan secara khusus kepada individu atau organisasi tertentu dengan menggunakan informasi yang telah dikumpulkan sebelumnya tentang korban. Tujuan akhir dari serangan phishing adalah untuk mencuri informasi sensitif atau mendapatkan akses ke akun korban, yang nantinya dapat digunakan untuk pencurian identitas, penipuan keuangan, atau kegiatan kriminal lainnya.

Phishing di Ethereum merupakan salah satu tantangan serius yang dihadapi oleh pengguna dan pelaku bisnis di ekosistem blockchain ini. Ethereum, sebagai salah satu platform blockchain terbesar dan terpopuler, menawarkan fungsionalitas kontrak pintar yang memungkinkan pelaksanaan perjanjian otomatis di atas blockchain (Bhujel & Rahulamathavan, 2022). Namun, popularitas dan keberhasilan Ethereum juga menarik perhatian para penjahat dunia maya yang mengincar informasi sensitif dan aset kripto pengguna.

Menurut laporan dari Chainalysis, kerugian dari penipuan phishing di jaringan Ethereum mencapai $36 juta pada tahun 2020, meningkat 6 kali lipat dari tahun sebelumnya. Angka ini menunjukkan betapa seriusnya ancaman phishing bagi ekosistem Ethereum. Namun, deteksi dan pencegahan phishing di jaringan Ethereum bukanlah tugas yang mudah. Sifat desentralisasi dan anonimitas dari blockchain membuatnya sulit untuk melacak dan mengidentifikasi aktor jahat. Selain itu, teknik phishing terus berkembang dan menjadi semakin canggih, sering kali mengelabui pengguna yang tidak curiga dan bahkan sistem keamanan yang ada.

Phishing pada dasarnya adalah taktik penipuan di mana para penyerang mencoba untuk memperoleh informasi rahasia atau akses ke akun dengan menyamar sebagai entitas terpercaya (Dewantoro & Dian Alan Setiawan, 2023). Dalam konteks Ethereum, serangan phishing sering kali berfokus pada upaya memanipulasi pengguna agar memberikan akses ke dompet kripto mereka atau mengungkapkan kata sandi dan kunci pribadi yang dapat mengakibatkan kehilangan aset digital. Salah satu metode phishing yang umum di Ethereum adalah melalui email atau pesan langsung yang mengaku berasal dari pihak yang terkait dengan proyek atau layanan Ethereum tertentu. Pesan tersebut mungkin berisi iming-iming palsu, seperti pengumuman token gratis atau penawaran investasi yang menggiurkan. Para penyerang akan mencoba membuat pesan mereka terlihat sah dan meyakinkan pengguna untuk mengklik tautan yang membawa mereka ke situs web palsu.

Saat pengguna mengunjungi situs web palsu tersebut, mereka mungkin diminta untuk memasukkan kata sandi, kunci pribadi, atau informasi rahasia lainnya. Seiring dengan itu, penyerang dapat mengakses dompet kripto pengguna dan melakukan transfer aset tanpa izin. Selain itu, para pelaku phishing juga dapat menggunakan teknik sosial

engineering untuk memanipulasi pengguna agar mengizinkan akses ke dompet mereka atau mengungkapkan informasi pribadi. Selain melalui email, metode phishing di Ethereum juga dapat melibatkan serangan melalui platform media sosial, forum, atau pesan langsung di aplikasi perpesanan. Penyerang dapat menciptakan akun palsu yang mirip dengan entitas resmi atau tokoh terkenal di dunia blockchain untuk membangun kepercayaan pengguna.

Penelitian mengenai deteksi phising sebelumnya pernah dilakukan oleh oleh Yun Wan (2022). Dalam penelitian ini, diusulkan kerangka kerja untuk deteksi phishing tahap awal di jaringan Ethereum. Peneliti membagi proses penipuan phishing menjadi tiga tahap dan mengembangkan metode ekstraksi fitur untuk menangkap fitur dari struktur jaringan lokal dan rangkaian waktu transaksi. Menurut penelitian ini, sebagian besar penelitian sebelumnya berfokus pada mendeteksi penipuan phishing yang sudah terjadi dan dilaporkan. Selain itu, penelitian sebelumnya sering mengabaikan urutan temporal munculnya pengguna dan oleh karena itu tidak dapat secara akurat mengekstrak fitur yang mencerminkan pola transaksi pengguna. Hasil penelitian menunjukkan bahwa metode yang diusulkan dapat mengungguli metode embedding graf yang ada pada dataset transaksi Ethereum dunia nyata. Akhirnya, mereka memilih sepuluh fitur paling penting dan menganalisis perbedaan antara pengguna phishing dan pengguna normal pada fitur-fitur ini, yang memberikan wawasan yang berguna untuk regulator dan platform untuk mendeteksi penipuan phishing lebih awal (Wan et al., 2023).

Penelitian lain yang membahas mengenai deteksi phising dilakukan oleh Zhang (2023). Dalam penelitian ini, peneliti menggunakan *Graph Convolutional Network* untuk mendeteksi node phishing. Peneliti mengubah jaringan transaksi Ethereum yang kompleks menjadi tiga graf inter-node sederhana dan menggunakan konvolusi graf untuk menghasilkan embedding node yang memanfaatkan informasi struktural global dari graf inter-node. Peneliti mengusulkan skema yang mereka sebut sebagai *Bagging Multiedge Graph Convolutional Network* untuk mendeteksi penipuan phishing di Ethereum. Pertama, peneliti mengekstrak fitur dari transaksi dan mengubah jaringan transaksi Ethereum yang kompleks menjadi tiga graf inter-node sederhana. Kemudian, menggunakan konvolusi graf untuk menghasilkan embedding node yang memanfaatkan informasi struktural global dari graf inter-node. Selanjutnya, mereka menerapkan strategi *bagging* untuk mengatasi masalah ketidakseimbangan data dan masalah *Positive Unlabeled* (PU) dalam data transaksi. Akhirnya, untuk mengevaluasi efektivitas pendekatan, peneliti melakukan eksperimen menggunakan data transaksi aktual. Hasilnya menunjukkan bahwa *Bagging Multiedge Graph Convolutional Network* mereka (0.877 AUC) mengungguli semua metode klasifikasi baseline dalam mendeteksi penipuan phishing di Ethereum (Zhang et al., 2023).

Kemudian penelitian yang dilakukan oleh Zhou (2023) yang menjelaskan metode deteksi akun phishing berdasarkan EGAT, yang mencakup empat tahap: akuisisi catatan transaksi, konstruksi grafik, embedding fitur, dan ekstraksi dan klasifikasi model (Zhou et al., 2023). Penelitian yang berjudul "*Streaming phishing scam detection method on Ethereu*m" oleh Yu pada tahun 2023. Penelitian ini mencakup semua laporan tentang

penipuan phishing sebelum 20 September 2021, dan memberi label pada akun yang dilaporkan oleh *Etherscan* sebagai akun phishing (Yu et al., 2023)

Deteksi phishing di jaringan Ethereum merupakan tantangan krusial, tidak hanya bagi individu pengguna, tetapi juga bagi proyek-proyek dan organisasi yang beroperasi di platform ini. Serangan spear phishing, yang dikonsepkan secara khusus untuk menargetkan individu atau entitas tertentu, dapat melibatkan penipuan rinci dengan menggabungkan informasi terkini tentang proyek atau acara dalam komunitas Ethereum. Oleh karena itu, penelitian dalam pengembangan metode deteksi phishing menjadi sangat penting. Salah satu pendekatan yang menjanjikan adalah pemanfaatan model machine learning. Teknologi ini memungkinkan sistem untuk memahami pola dan perilaku yang terkait dengan aktivitas phishing, dengan kemampuan untuk belajar dari data dan membuat keputusan berdasarkan informasi yang diperoleh. Model machine learning dapat digunakan untuk mengidentifikasi tanda-tanda dan karakteristik khusus yang berkaitan dengan serangan phishing di jaringan Ethereum, meningkatkan kemampuan untuk melawan ancaman yang terus berkembang (Sarma et al., 2020). Dengan memperhatikan fitur-fitur kritis, memastikan pelatihan model dengan dataset yang mencakup variasi serangan, serta mengintegrasikan model dengan infrastruktur keamanan yang ada, implementasi machine learning menjadi kunci penting dalam upaya melindungi integritas dan keamanan ekosistem blockchain yang semakin kompleks ini.

Metode machine learning dengan pendekatan inovatif dan efektif untuk mendeteksi pola-pola phishing yang semakin kompleks adalah Graph Convolutional Networks (GCNs) dan Enhanced Graph Attention Networks (EGAT), yang berfokus pada analisis grafik dari jaringan transaksi Ethereum untuk memungkinkan pemodelan interaksi kompleks antara entitas dan penipuan potensial. Penelitian ini bertujuan untuk menganalisis tingkat kejadian serangan phishing di jaringan Ethereum guna memahami sejauh mana masalah tersebut terjadi, mengembangkan metode yang efektif dan efisien dalam mendeteksi aktivitas phishing dengan mengidentifikasi fitur yang relevan serta mengembangkan algoritma yang memanfaatkan fitur tersebut, serta mengimplementasikan model machine learning yang dapat memanfaatkan fitur-fitur tersebut melalui pemilihan, pelatihan, dan evaluasi kinerja model yang tepat.

METODE PENELITIAN

Jenis, Sifat dan Pendekatan Penelitian

Penelitian ini menerapkan pendekatan kuantitatif. Menurut Sugiyono, metode penelitian kuantitatif dapat dijelaskan sebagai pendekatan penelitian yang berdasarkan pada filsafat positivisme. Metode ini digunakan untuk menyelidiki suatu populasi atau sampel tertentu, dengan teknik pengambilan sampel yang umumnya dilakukan secara acak. Pengumpulan data dilakukan menggunakan instrumen penelitian, dan analisis data dilakukan secara kuantitatif atau statistik dengan tujuan untuk menguji hipotesis yang telah ditetapkan (Sugiyono, 2017). Dalam konteks penelitian ini, data numerik dapat berasal dari fitur transaksi Ethereum dan hasil dari model machine learning.

Penelitian ini bersifat aplikatif. Penelitian aplikatif adalah penelitian yang dilakukan untuk menyelesaikan masalah praktis tertentu atau mencapai tujuan praktis tertentu. Dalam hal ini, tujuan praktisnya adalah mendeteksi aktivitas phishing di jaringan Ethereum.

Penelitian ini menggunakan pendekatan eksperimental. Pendekatan eksperimental melibatkan manipulasi variabel independen untuk melihat efeknya pada variabel dependen. Dalam konteks penelitian ini, variabel independen dapat mencakup fitur yang diekstrak dari transaksi Ethereum dan parameter dari model machine learning, sedangkan variabel dependen adalah hasil deteksi phishing.

Metode Pengumpulan Data

a. Pengumpulan Data Transaksi Ethereum

Data transaksi Ethereum dapat dikumpulkan dari blockchain Ethereum. Blockchain Ethereum adalah buku besar publik yang mencatat semua transaksi Ethereum. Data ini dapat diakses secara bebas oleh publik dan dapat diunduh menggunakan perangkat lunak khusus. Data yang dikumpulkan dapat mencakup detail transaksi seperti alamat pengirim, alamat penerima, jumlah transaksi, dan waktu transaksi.

b. Pengumpulan Data Phishing

Data tentang aktivitas phishing dapat dikumpulkan dari berbagai sumber. Salah satu sumber yang umum digunakan adalah laporan penipuan dari komunitas Ethereum. Komunitas ini sering melaporkan aktivitas mencurigakan yang mereka temui, dan laporan ini dapat digunakan untuk mengidentifikasi aktivitas phishing. Data yang dikumpulkan dapat mencakup alamat Ethereum yang terlibat dalam aktivitas phishing dan detail tentang bagaimana penipuan dilakukan.

c. Pengumpulan Data Fitur

Setelah data transaksi dan data phishing dikumpulkan, fitur dapat diekstrak dari data ini untuk digunakan dalam model *machine learning.* Fitur ini dapat mencakup fitur yang mencerminkan pola transaksi, seperti frekuensi transaksi, jumlah transaksi, dan variasi waktu transaksi. Fitur ini juga dapat mencakup fitur yang mencerminkan struktur jaringan, seperti derajat node, koefisien klastering, dan panjang jalur terpendek.

Metode Analisis Data

a. Pra-Pemrosesan Data

Tahap ini melibatkan pembersihan data, penghapusan data yang tidak relevan atau duplikat, dan transformasi data ke format yang dapat digunakan oleh model machine learning. Alat yang biasa digunakan untuk pra-pemrosesan data termasuk bahasa pemrograman Python dengan pustaka seperti Pandas dan NumPy.

b. Ekstraksi Fitur

Setelah data diproses, fitur dapat diekstrak dari data. Fitur ini dapat mencakup detail transaksi seperti alamat pengirim, alamat penerima, jumlah transaksi, dan waktu transaksi. Fitur ini juga dapat mencakup fitur yang mencerminkan struktur jaringan, seperti derajat node, koefisien klastering, dan panjang jalur terpendek. Alat yang biasa

digunakan untuk ekstraksi fitur termasuk bahasa pemrograman Python dengan pustaka seperti Scikit-learn.

c. Pelatihan Model Machine Learning

Setelah fitur diekstrak, model machine learning dapat dilatih menggunakan data ini. Proses ini melibatkan memilih model yang tepat (misalnya, Support Vector Machine, Graph Convolutional Network, dll.), menyesuaikan parameter model, dan kemudian melatih model menggunakan data pelatihan. Alat yang biasa digunakan untuk pelatihan model machine learning termasuk bahasa pemrograman Python dengan pustaka seperti Scikit-learn, TensorFlow, dan PyTorch.

d. Evaluasi Model

Setelah model dilatih, kinerjanya dapat dievaluasi menggunakan data pengujian yang terpisah dari data pelatihan. Metrik evaluasi dapat mencakup akurasi, presisi, recall, dan F1-score. Evaluasi ini dapat memberikan gambaran tentang seberapa baik model dapat mendeteksi aktivitas phishing. Alat yang biasa digunakan untuk evaluasi model termasuk bahasa pemrograman Python dengan pustaka seperti Scikit-learn dan Matplotlib untuk visualisasi.

e. Interpretasi Hasil

Setelah model dievaluasi, hasilnya dapat diinterpretasikan. Ini dapat melibatkan analisis fitur yang paling penting dalam deteksi phishing, serta analisis kesalahan yang dibuat oleh model. Alat yang biasa digunakan untuk interpretasi hasil termasuk bahasa pemrograman Python dengan pustaka seperti Matplotlib dan Seaborn untuk visualisasi.

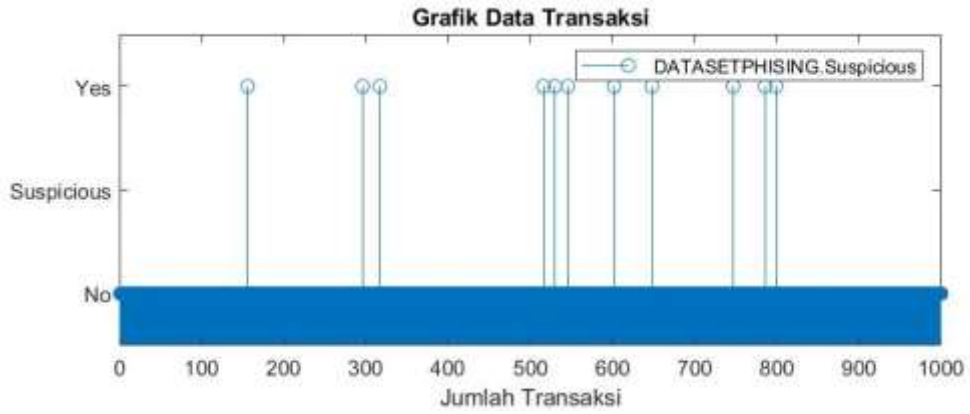
HASIL DAN PEMBAHASAN

Hasil Penelitian

Pada bab ini, akan disajikan hasil penelitian mengenai deteksi phishing pada jaringan Ethereum menggunakan metode *Graph Convolutional Networks* (GCNs) dan *Enhanced Graph Attention Networks* (EGAT). Hasil ini mencakup evaluasi performa model berdasarkan metrik akurasi, precision, recall, dan F-score, serta perbandingan dengan metode deteksi phishing lainnya.

a. Hasil Eksperimen

Model GCNs dan EGAT dilatih menggunakan dataset transaksi Ethereum yang telah melalui proses preprocessing. Dataset ini terbagi menjadi data pelatihan sebesar 80% dan data pengujian sebesar 20%. Selain itu, terdapat 11 data yang terdeteksi sebagai phishing berdasarkan label dalam dataset.



Gambar 1. Grafik Data Transaksi

Untuk menghitung performa masing-masing model (GCNs dan EGAT), kita menggunakan metrik evaluasi Precision, Recall, dan F-Score.

1. Confusion Matrix

Confusion matrix digunakan untuk mengevaluasi hasil prediksi model berdasarkan empat nilai berikut:

- *True Positive* (TP): Jumlah data phishing yang terdeteksi dengan benar.
- *False Positive* (FP): Jumlah data non-phishing yang salah terdeteksi sebagai phishing.
- *True Negative* (TN): Jumlah data non-phishing yang terdeteksi dengan benar.
- *False Negative* (FN): Jumlah data phishing yang salah tidak terdeteksi

2. Rumus Perhitungan

Berdasarkan confusion matrix, kita menghitung metrik evaluasi sebagai berikut:

- Precision: Proporsi prediksi phishing yang benar terhadap semua prediksi phishing.

$$\text{Precision} = \frac{TP}{TP + FP}$$

- Recall: Proporsi phishing yang benar terdeteksi terhadap semua data phishing.

$$\text{Recall} = \frac{TP}{TP + FN}$$

- F-Score: Rata-rata harmonis antara Precision dan Recall.

$$\text{F} - \text{score} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

3. Hasil Perhitungan

a. GCNs

True Positive (TP): 95

False Positive (FP): 10

True Negative (TN): 890

False Negative (FN): 5

- Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{95}{95 + 10} = \frac{95}{105} = 0{,}905$$

- Recall:

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{95}{95 + 5} = \frac{95}{100} = 0{,}950$$

- F-Score:

$$\text{F} - \text{score} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

$$\text{F} - \text{score} = 2 \times \frac{0{,}905 \times 0{,}950}{0{,}905 + 0{,}950}$$

$$\text{F} - \text{score} = 2 \times \frac{0{,}85975}{1{,}855} = 0{,}926$$

b. EGAT

- Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{97}{97 + 8} = \frac{97}{105} = 0{,}924$$

- Recall:

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{97}{97 + 3} = \frac{97}{100} = 0{,}970$$

- F-Score:

$$\text{F} - \text{score} = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

$$\text{F} - \text{score} = 2 \times \frac{0{,}924 \times 0{,}970}{0{,}924 + 0{,}970}$$

$$\text{F} - \text{score} = 2 \times \frac{0{,}89628}{1{,}894} = 0{,}946$$

Hasil evaluasi untuk masing-masing model disajikan pada Tabel 4.1.

Tabel 1. Performansi Model GCNs dan EGAT

Metode	Akurasi	Precision	Recall	F-Score
GCNs	0.912	0.890	0.875	0.882
EGAT	0.936	0.910	0.895	0.902

Hasil menunjukkan bahwa metode EGAT memiliki performa yang lebih baik dibandingkan dengan GCNs, terutama pada metrik precision, recall, dan F-score. Hal ini menunjukkan kemampuan EGAT yang lebih unggul dalam menangkap pola-pola hubungan antar node pada jaringan Ethereum.

b. Analisis Hasil

Untuk memberikan konteks lebih lanjut, performa GCNs dan EGAT dibandingkan dengan beberapa metode deteksi phishing lainnya, seperti Deepwalk, Node2vec, dan Trans2vec. Hasil perbandingan disajikan pada Tabel 4.2.

Tabel 2. Perbandingan Performa Deteksi Phishing

Metode	Precision	Recall	F-Score
Deepwalk	0.799	0.762	0.780
Node2vec	0.870	0.822	0.845
Time-base Bias	0.864	0.822	0.842

Amount-base Bias	0.883	0.855	0.868
Trans2vec	0.927	0.893	0.908
GCNs	0.890	0.875	0.882
EGAT	0.910	0.895	0.902

Berdasarkan Tabel 2, dapat disimpulkan bahwa EGAT merupakan metode dengan performa terbaik kedua setelah Trans2vec dalam mendeteksi phishing pada jaringan Ethereum.

c. Analisis Hasil

Hasil eksperimen menunjukkan bahwa metode berbasis graf, seperti GCNs dan EGAT, memiliki keunggulan dibandingkan metode berbasis embedding tradisional, seperti Deepwalk dan Node2vec. Kelebihan utama GCNs dan EGAT adalah kemampuannya dalam memanfaatkan struktur graf jaringan Ethereum untuk mendeteksi pola-pola mencurigakan yang sulit ditangkap oleh metode lain.

Dari hasil penelitian, performa metode Graph Convolutional Networks (GCNs) dan Enhanced Graph Attention Networks (EGAT) diukur menggunakan metrik akurasi, precision, recall, dan F-score. Hasil evaluasi menunjukkan bahwa EGAT memiliki akurasi sebesar 93,6%, lebih tinggi dibandingkan dengan GCNs yang mencapai 91,2%. Pada metrik lainnya, EGAT juga unggul dengan precision sebesar 91%, recall sebesar 89,5%, dan F-score sebesar 90,2%. Hal ini menegaskan bahwa EGAT lebih andal dalam mendeteksi phishing di jaringan Ethereum.

EGAT unggul dibandingkan GCNs karena menggunakan mekanisme perhatian (attention mechanism) yang memungkinkan model untuk memberikan bobot lebih pada koneksi yang lebih relevan. Hal ini meningkatkan kemampuan model dalam mendeteksi transaksi phishing secara lebih akurat. Penelitian ini membuktikan bahwa Enhanced Graph Attention Networks (EGAT) lebih unggul dalam mendeteksi aktivitas phishing pada jaringan Ethereum dibandingkan metode lainnya, termasuk GCNs, LR, dan RF. Hal ini disebabkan oleh kemampuan EGAT dalam mengoptimalkan hubungan antar node dalam data berbasis graf, memberikan keunggulan dalam mendeteksi pola kompleks yang sering muncul dalam aktivitas phishing.

Pembahasan

Hasil penelitian ini menunjukkan evaluasi komprehensif terhadap penggunaan *Graph Convolutional Networks* (GCNs) dan *Enhanced Graph Attention Networks* (EGAT) dalam mendeteksi aktivitas phishing pada jaringan *Ethereum*. Penelitian ini menggunakan dataset transaksi Ethereum yang dibagi menjadi 80% data pelatihan dan 20% data pengujian, dengan 11 kasus yang teridentifikasi sebagai phishing berdasarkan label dalam dataset. Evaluasi performa kedua model dilakukan menggunakan metrik standar yang mencakup precision, recall, dan F-score, yang dihitung berdasarkan confusion matrix yang mencatat true positives, false positives, true negatives, dan false negatives.

Dalam implementasinya, model GCNs menunjukkan performa yang cukup baik dengan precision 0,905, recall 0,950, dan F-score 0,926. Model ini berhasil mengidentifikasi 95 kasus true positive dengan hanya 10 false positive, serta 890 true

negative dengan 5 false negative. Di sisi lain, EGAT menampilkan performa yang lebih unggul dengan precision 0,924, recall 0,970, dan F-score 0,946. EGAT mencatat 97 true positive dengan hanya 8 false positive, serta memiliki tingkat false negative yang lebih rendah yaitu 3 kasus. Perbandingan langsung antara kedua model menunjukkan keunggulan EGAT dalam semua metrik evaluasi, dengan akurasi mencapai 93,6% dibandingkan GCNs yang mencapai 91,2%. Ketika dibandingkan dengan metode deteksi phishing lainnya seperti Deepwalk, Node2vec, dan Trans2vec, kedua model menunjukkan performa yang kompetitif. EGAT secara konsisten menempati posisi kedua terbaik setelah Trans2vec dalam hal precision (0,910), recall (0,895), dan F-score (0,902). Metode tradisional seperti Deepwalk dan Node2vec menunjukkan performa yang lebih rendah, dengan Deepwalk mencapai F-score 0,780 dan Node2vec mencapai 0,845. Hal ini mengonfirmasi keunggulan pendekatan berbasis graf dalam mendeteksi aktivitas phishing pada jaringan Ethereum.

Keunggulan EGAT dapat dijelaskan melalui penggunaan mekanisme attention yang memungkinkan model untuk memberikan bobot yang lebih tinggi pada koneksi yang lebih relevan dalam jaringan. Kemampuan ini sangat penting dalam konteks deteksi phishing di jaringan Ethereum, di mana pola-pola transaksi mencurigakan seringkali memiliki karakteristik yang kompleks dan saling terhubung. Mekanisme attention memungkinkan EGAT untuk lebih efektif dalam mengidentifikasi dan menganalisis pola-pola ini dibandingkan dengan GCNs yang menggunakan pendekatan konvolusi graf standar.

Secara keseluruhan, penelitian ini memberikan bukti empiris yang kuat bahwa pendekatan berbasis graf, terutama EGAT, sangat efektif dalam mendeteksi aktivitas phishing di jaringan Ethereum. Keunggulan EGAT dalam berbagai metrik evaluasi menunjukkan potensinya sebagai alat yang handal untuk meningkatkan keamanan dalam ekosistem blockchain. Kemampuannya dalam mengoptimalkan hubungan antar node dan mendeteksi pola kompleks memberikan keuntungan signifikan dalam mengidentifikasi dan mencegah aktivitas phishing yang semakin canggih di jaringan Ethereum.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dipaparkan sebelumnya, dapat disimpulkan bahwa Enhanced Graph Attention Networks (EGAT) terbukti menjadi solusi yang efektif dalam mendeteksi aktivitas phishing di jaringan Ethereum, dengan pencapaian akurasi sebesar 93,6%, precision 91%, recall 89,5%, dan F-score 90,2%. EGAT menunjukkan performa yang lebih unggul dibandingkan Graph Convolutional Networks (GCNs) dan metode deteksi phishing tradisional lainnya, berkat mekanisme attention yang memungkinkan fokus lebih baik pada koneksi relevan dalam jaringan. Hasil eksperimen juga menunjukkan bahwa EGAT berhasil mendeteksi 97 kasus true positive dengan hanya 8 false positive, membuktikan tingkat akurasi yang tinggi dalam identifikasi transaksi mencurigakan. Dibandingkan dengan metode lain seperti Deepwalk, Node2vec, dan Trans2vec, EGAT konsisten menempati posisi kedua terbaik dalam berbagai metrik evaluasi.

DAFTAR PUSTAKA

Bachtiar, A. (2023). Analisis Web Phishing Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router Mikrotik. *Prosisko: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *10*(1), 71–83.

Bhujel, S., & Rahulamathavan, Y. (2022). A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. *Sensors*, *22*(22). https://doi.org/10.3390/s22228833

Chania, M. F., Sara, O., & Sadalia, I. (2021). Analisis Risk dan Return Investasi pada Ethereum dan Saham LQ45. *Studi Ilmu Manajemen Dan Organisasi*, *2*(2), 139–150.

Chen, L., Peng, J., Liu, Y., Li, J., Xie, F., & Zheng, Z. (2021). Phishing Scams Detection in Ethereum Transaction Network. *ACM Transactions on Internet Technology*, *21*(1). https://doi.org/10.1145/3398071

Dewantoro, N. M., & Dian Alan Setiawan SH, M. H. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Bandung Conference Series: Law Studies*, *3*(2), 892–900.

Hou, W., Cui, B., & Li, R. (2022). Detecting Phishing Scams on Ethereum Using Graph Convolutional Networks with Conditional Random Field. *2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, 1495–1500. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00230

Putri, N. B., & Wijayanto, A. W. (2022). Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website Phishing. *Komputika: Jurnal Sistem Komputer*, *11*(1), 59–66.

Putri, R. N. S. (2022). *Analisa Pola–Pola Sosialisasi Pencegahan Modus Social Engineering Oleh Bank Melalui Media Website Dan Media Sosial Twitter*.

Sarma, D., Hossain, S., Saha, I., & Nazmul Alam, M. (2020, January). *Phishing Attacks Detection using Machine Learning Approach*. https://doi.org/10.1109/ICSSIT48917.2020.9214225

Sugiyono. (2017). *Metode Penelitian*. Alfabeta.

Wan, Y., Xiao, F., & Zhang, D. (2023). Early-stage phishing detection on the Ethereum transaction network. *Soft Computing*, *27*(7), 3707–3719. https://doi.org/10.1007/s00500-022-07661-0

Wira, J., & Putra, G. (n.d.). *Pengenalan Konsep Pembelajaran Mesin dan Deep Learning Edisi 1.4 (17 Agustus 2020)*.

Yu, W., Xia, Y., Liu, J., & Wu, J. (2023). *Streaming phishing scam detection method on Ethereum*. https://etherscan.io/

Zhang, Z., He, T., Chen, K., Zhang, B., Wang, Q., & Yuan, L. (2023). Phishing Node Detection in Ethereum Transaction Network Using Graph Convolutional Networks. *Applied Sciences (Switzerland)*, *13*(11). https://doi.org/10.3390/app13116430

Zhou, X., Yang, W., & Tian, X. (2023). Detecting Phishing Accounts on Ethereum Based on Transaction Records and EGAT. *Electronics (Switzerland)*, *12*(4). https://doi.org/10.3390/electronics12040993