Available online at https://ejournal.almaata.ac.id/index.php/IJUBI
Indonesian Journal of Business Intelligence
Volume 9 | Issue 1 | June (2026)
ISSN 2621-3915 (PRINT), ISSN 2621-3923 (ONLINE), Published by **Alma Ata University Press**

IJUBI
Indonesian Journal
---- of ----
Business Intelligence

GRAPH CONVOLUTIONAL NETWORK UNTUK DETEKSI DAN MITIGASI ANCAMAN SIBER: HONEYPOT, BOTNET C2 DAN NSL-KDD

Paulus Harsadi[1], Yovita Kinanti Kumarahadi[2], Hendro Wijayanto[3*]
[1,3]Program Studi Teknologi Informasi, Sekolah Vokasi, Universitas Tiga Serangkai,
[2]Program Studi Sistem Informasi, Sekolah Vokasi, Universitas Tiga Serangkai.
*hendrowijayanto@tsu.ac.id
Jl. KH. Samanhudi No. 84–86 Surakarta, Jawa Tengah, Indonesia.

Article history: *Received: 15 March 2026 ; Revised: 25 May 2026; Accepted: 30 June 2026*

Abstract

Conventional intrusion detection approaches typically evaluate each network record independently, causing relational attack patterns such as lateral movement, command-and-control beaconing, and coordinated botnet flooding to remain undetected, since these patterns only become apparent when the topological relationships among entities are considered. This study proposes and evaluates a Graph Convolutional Network, implemented from first principles, for threat detection and adaptive mitigation recommendation across three data conditions: honeypot network logs represented as an explicit IP-relation graph, botnet command-and-control and distributed denial-of-service traffic exhibiting many-to-few and many-to-one topologies, and the NSL-KDD benchmark, using a k-nearest-neighbor similarity graph since tabular records lack explicit host identity. Node-level features are propagated through a two-layer Graph Convolutional Network following a spectral propagation rule, optimized with Adam, and each predicted threat category is mapped to mitigation actions referencing the NIST Cybersecurity Framework Profile for Artificial Intelligence and ISO/IEC 27001:2022. Testing yielded 99.9% accuracy on the honeypot graph, 100% accuracy on the botnet graph, and 96.3% accuracy (macro F1 = 0.955) on the five-class NSL-KDD condition, with the lowest per-class performance on the Remote-to-Local category (F1 = 0.875). Rather than relying on aggregate accuracy alone, this study reports per-class F1 and precision-recall AUC to avoid misleading conclusions under severe class imbalance. Graph structure analysis revealed that threat nodes exhibit markedly lower connectivity than infrastructure nodes, offering an interpretable structural signature. The complete pipeline executes in under five seconds per condition. The findings indicate that a graph-based representation combined with a standards-mapped mitigation engine offers a viable, interpretable pathway toward adaptive cybersecurity decision support.

Keywords: *Botnet Command-and-Control; Cybersecurity Mitigation; Graph Convolutional Network; Honeypot; Network Intrusion Detection; NSL-KDD.*

Abstrak

Pendekatan deteksi intrusi konvensional umumnya mengevaluasi setiap catatan trafik jaringan secara independen, sehingga pola serangan relasional seperti pergerakan lateral, *beaconing command-and-control*, dan *flooding botnet* cenderung tidak terdeteksi. Karena pola tersebut hanya tampak apabila hubungan topologi antar entitas turut dipertimbangkan. Penelitian ini mengusulkan dan mengevaluasi *Graph Convolutional Network* yang diimplementasikan dari prinsip dasar untuk deteksi ancaman dan rekomendasi mitigasi adaptif pada tiga kondisi data, yaitu *log honeypot* berbentuk graf relasi IP eksplisit, trafik *botnet command-and-control* dan distributed *denial-of-service* dengan topologi *many-to-few* dan *many-to-one*. Serta dataset *benchmark NSL-KDD* yang grafnya dibangun melalui kemiripan *k-nearest-neighbor* karena data tabularnya

IJUBI by https://ejournal.almaata.ac.id/index.php/IJUBI is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

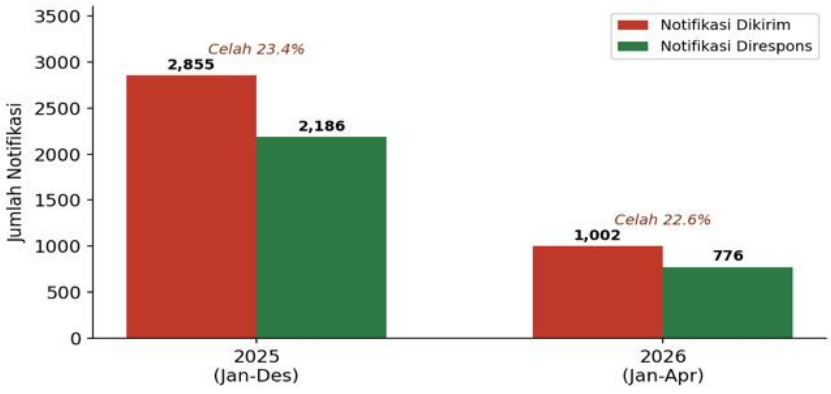
tidak memiliki identitas *host* eksplisit. Fitur tingkat node dipropagasikan melalui *Graph Convolutional Network* dua lapis mengikuti aturan propagasi, dioptimasi dengan *Adam*, dan setiap kategori ancaman terprediksi dipetakan ke dalam tindakan mitigasi yang merujuk pada *NIST Cybersecurity Framework Profile for Artificial Intelligence* dan *ISO/IEC 27001:2022*. Pengujian menghasilkan akurasi 99,9% pada graf *honeypot* dan akurasi 100% pada graf *botnet*. Akurasi 96,3% (macro F1 = 0,955) pada kondisi *NSL-KDD* lima kelas, dengan performa terendah pada kategori *Remote-to-Local* (F1 = 0,875). Penelitian ini melaporkan F1 per kelas dan *precision-recall AUC* untuk menghindari kesimpulan yang kurang tepat akibat ketidakseimbangan kelas. Analisis struktur graf mengungkap bahwa node ancaman memiliki konektivitas yang jauh lebih rendah dibandingkan node infrastruktur, memberikan penanda struktural yang mudah diinterpretasikan. Keseluruhan alur proses berjalan kurang dari lima detik per kondisi data. Temuan menunjukkan representasi berbasis graf yang dipadukan dengan rekomendasi mitigasi terpetakan standar menawarkan jalur yang layak dan mudah digambarkan menuju pengambilan keputusan keamanan siber yang adaptif.

Kata Kunci: *Botnet Command-and-Control; Deteksi Intrusi Jaringan; Graph Convolutional Network; Honeypot; Mitigasi Keamanan Siber; NSL-KDD.*

Pendahuluan

Lanskap ancaman keamanan siber global terus meningkat baik dari sisi volume maupun kompleksitas, dengan serangan yang semakin terindustrialisasi dan sebagian memanfaatkan otomasi berbasis kecerdasan buatan pada sisi penyerang, sebagaimana dilaporkan secara konsisten oleh *FortiGuard Labs*, *CrowdStrike*, dan *Rapid7 Labs* dalam laporan lanskap ancaman tahun 2026 masing-masing lembaga. *World Economic Forum* dalam *Global Cybersecurity Outlook 2026* menegaskan bahwa kesenjangan kapabilitas pertahanan siber organisasi tidak sebanding dengan laju evolusi ancaman. Kesenjangan ini diperparah oleh kurangnya keahlian kritis di banyak organisasi, sebagaimana didokumentasikan oleh ISC2 dalam studi tenaga kerja keamanan siber tahun 2025, meskipun otomasi keamanan yang matang terbukti menghemat biaya dan waktu penahanan insiden menurut laporan tahunan *IBM Security* bersama *Ponemon Institute*.

Urgensi ini tampak lebih fokus pada konteks Indonesia, yang mana Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 5,5 miliar anomali trafik siber sepanjang 2025. Melampaui akumulasi total periode 2020–2024 sekaligus dengan mayoritas mutlak berupa *malware* yang berpotensi menjadi *ransomware*. Sementara kapasitas pemantauan trafik nasional diperkirakan baru mencakup kurang dari 10% keseluruhan trafik. Kesenjangan mitigasi juga tampak pada tindak lanjut, dari 2.855 notifikasi insiden yang dikirimkan BSSN sepanjang 2025, hanya 76,6% yang mendapatkan respons, dengan rasio serupa (77,4%) masih bertahan pada awal 2026. Artinya, hampir satu dari empat organisasi yang telah diinformasikan tetap tidak menindaklanjuti peringatan tersebut, hal ini terlihat pada Gambar 1.



Gambar 1. Kesenjangan Notifikasi dan Respons Insiden Siber Nasional (Data BSSN, 2025–2026)

Di sisi metodologis, sebagian besar sistem deteksi intrusi konvensional berbasis *decision tree*, *ensemble*, maupun *deep learning*, memperlakukan setiap catatan koneksi sebagai entitas independen tanpa mempertimbangkan relasi struktural antarentitas. Tinjauan literatur *Graph Neural Network (GNN)* menegaskan bahwa keterbatasan ini menyebabkan pola serangan relasional, pergerakan lateral, *beaconing command-and-control (C2)*, maupun *flooding* terkoordinasi cenderung lepas dari deteksi konvensional, karena hanya tampak ketika struktur graf turut dianalisis [1][2]. *Graph Convolutional Network (GCN)*, yang mempropagasikan fitur antarnode bertetangga melalui konvolusi spektral sebagaimana dirumuskan pertama kali, menjadi salah satu pendekatan paling banyak diadopsi untuk mengatasi keterbatasan tersebut. Penerapan *GNN/GCN* pada keamanan siber berkembang pesat dan mencakup beragam arsitektur serta domain. Pada deteksi intrusi umum, *AJSAGE* memadukan koneksi jumping-knowledge dengan *GraphSAGE* [3], penataan ulang fitur meningkatkan deteksi multi-kelas [4], dan pendekatan atensi *multi-hop* berbasis fitur *edge* turut terbukti meningkatkan akurasi deteksi intrusi pada graf jaringan [5].

Pada domain *IoT* dan *botnet* secara lebih spesifik, *graph attention network (GAT)* telah diterapkan untuk menangkap bobot relevansi antar-tetangga [6], termasuk pada evaluasi reduksi dimensi berbasis *autoencoder* untuk deteksi botnet, maupun melalui arsitektur konvolusi graf berperhatian termodifikasi [7]. Tinjauan sistematis terbaru turut mengonfirmasi bahwa metode berbasis graf secara konsisten mengungguli pendekatan berbasis fitur datar dalam mendeteksi *botnet IoT* dan serangan *Distributed Denial of Services (DDOS)* [8], sementara pendekatan deteksi node *botnet* berbasis pembelajaran graf melengkapi arah riset ini dengan menangani topologi *command-and-control* yang tersamar [9]. Kerentanan *GNN* terhadap manipulasi turut menjadi perhatian melalui mekanisme deteksi serangan adversarial berbasis graf. Penerapan *GCN* juga meluas ke deteksi kecurangan *Bitcoin* [10] dan infrastruktur pengisian daya kendaraan listrik [11]. Cakupan domain ini turut meluas ke keamanan *cloud computing* melalui kombinasi *GCN* dan *GraphSAGE* [12], deteksi anomali yang mudah diinterpretasikan pada pemantauan infrastruktur teknologi informasi [13], maupun deteksi anomali multi-level berbasis *graph attention network* pada sistem kendali industri [14].

Cakupan riset ini didukung oleh survei komprehensif pada operasi pertahanan siber serta tinjauan sistematis deteksi serangan berbahaya berbasis graf [15]. Kerangka umum penerapan pendekatan berbasis graf dalam keamanan siber turut diulas secara komprehensif, sementara integrasi terkini dengan *large language model* dan *explainable AI* ditegaskan [16], sejalan dengan pendekatan dwi-modalitas yang memadukan graf heterogen dan model bahasa besar untuk deteksi intrusi jaringan [17]. Pada konteks penerapan operasional, arsitektur graf berbasis kesamaan perilaku terbukti meningkatkan performa deteksi sekaligus efisiensi komputasi pada lingkungan *edge computing* [18], sementara pembelajaran mandiri (*self-supervised*) pada representasi aliran jaringan turut terbukti efektif tanpa memerlukan anotasi data berskala besar [19]. Pendekatan berbasis graf pengetahuan turut mendukung deteksi dini yang dapat ditransfer lintas jaringan yang berbeda [20].

Analisis berbasis graf turut diterapkan pada deteksi serangan berurutan di *IoT* [21] dan propagasi virus dalam jaringan [22], menegaskan fleksibilitas representasi graf dalam menangkap ragam pola serangan. Arsitektur graf terfederasi turut diusulkan untuk analisis trafik jaringan skala besar tanpa sentralisasi data [23], sementara pendekatan berbasis graf juga diperluas ke ranah verifikasi intelijen ancaman siber, termasuk deteksi informasi ancaman palsu [24] dan sistem deteksi intrusi *IoT* berbasis graf yang dioptimalkan untuk efisiensi komputasi pada perangkat sumber daya terbatas [25].

Terdapat tiga kesenjangan yang memotivasi penelitian ini. Pertama, mayoritas studi mengevaluasi model pada satu jenis dataset saja, sehingga generalisasi lintas struktur relasional berbeda, seperti antara graf relasi IP eksplisit dan graf kemiripan fitur seperti dataset *NSL-KDD*, belum banyak diuji dalam satu kerangka. Kedua, penelitian *GNN* pada umumnya berhenti pada klasifikasi ancaman tanpa mekanisme tindak lanjut yang selaras dengan tata kelola keamanan siber internasional, seperti profil kecerdasan buatan pada *NIST Cybersecurity Framework* yang baru dirilis oleh *National Institute of Standards and Technology*, maupun *ISO/IEC 27001:2022*. Ketiga, evaluasi pada dataset seperti *NSL-KDD* rentan terhadap kesimpulan yang kurang tepat apabila hanya mengandalkan akurasi agregat, mengingat ketidakseimbangan kelas. Khususnya *R2L* dan *U2R* dapat

mempertahankan akurasi yang tetap tinggi meskipun model gagal mengenali kelas minoritas, sebagaimana turut ditegaskan dalam evaluasi kerangka pembelajaran mesin otomatis pada kondisi data yang tidak seimbang.

Berdasarkan kesenjangan tersebut, penelitian ini mengevaluasi sistem deteksi ancaman dan rekomendasi mitigasi berbasis *GCN* yang diimplementasikan dari prinsip dasar, diuji pada tiga kondisi data, yaitu (1) *log honeypot* yang merepresentasikan pola serangan nyata, dengan skema data mengikuti karakteristik interaksi *Cowrie honeypot* yang telah didokumentasikan pada penelitian terdahulu serta skala mengacu pada dataset *honeypot* multi-regional terkini, (2) *trafik botnet* dan *command-and-control*, serta (3) dataset *benchmark NSL-KDD*. Kontribusi utamanya yaitu (a) implementasi *GCN* dua lapis dari nol tanpa pustaka *deep learning* yang banyak, (b) evaluasi lintas-kondisi pada graf relasi eksplisit maupun graf kemiripan *k-nearest-neighbor*, (c) integrasi deteksi dengan mesin rekomendasi mitigasi yang terpetakan otomatis ke *NIST CSF* dan *ISO/IEC 27001:2022*, dan (d) pelaporan metrik yang sesuai terhadap ketidakseimbangan kelas antara *F1* per kelas dan *precision-recall AUC*, bukan sekadar akurasi keseluruhan.

Dari hasil latar belakang permasalahan yang dikaji, rumusan masalah ini adalah (1) bagaimana performa *GCN* dalam mendeteksi ancaman pada tiga kondisi data yang berbeda struktur relasionalnya; (2) sejauh mana metrik yang mempertimbangkan ketidakseimbangan kelas mengungkap keterbatasan yang tidak tampak pada akurasi keseluruhan; dan (3) bagaimana keluaran deteksi diterjemahkan menjadi rekomendasi mitigasi yang selaras dengan standar keamanan internasional.

Metode

Penelitian ini menggunakan desain penelitian dan pengembangan dengan evaluasi eksperimental pada berbagai kondisi data. Sistem yang dikembangkan dibangun melalui lima tahapan, yaitu : (1) akuisisi dan pra-pemrosesan data, (2) konstruksi representasi graf, (3) pelatihan model *GCN*, (4) evaluasi kinerja dengan metrik yang sesuai untuk data tidak seimbang, dan (5) pemetaan hasil deteksi menjadi rekomendasi mitigasi. Gambar 2 mengilustrasikan alur kelima tahapan tersebut.



Gambar 2. Diagram Alur Metode Penelitian

1. Kondisi dan Sumber Data

Evaluasi dilakukan pada tiga kondisi data dengan struktur relasional berbeda, guna menguji generalisasi pendekatan berbasis graf. Data pertama adalah *log honeypot* yang merepresentasikan interaksi penyerang terhadap layanan umpan (*SSH, Telnet, HTTP*), mencakup pola *port scanning*, *brute-force login*, *DoS flood*, dan serangan web, yang mana skemanya mengikuti karakteristik data yang telah didokumentasikan, dengan skala mengacu pada dataset *honeypot* multi-regional. Data kedua adalah trafik *botnet* dan *command-and-control (C2)*, mencakup *beaconing* periodik *host bot* ke *server C2* serta partisipasi *DDoS* terkoordinasi, merepresentasikan topologi *many-to-few* dan *many-to-one* yang berbeda dari star tunggal pada *honeypot*, merujuk pendekatan deteksi *botnet* berbasis *graph attention network* dan konvolusi graf termodifikasi. Data ketiga adalah *benchmark* akademik dataset *NSL-KDD* (41 atribut fitur, lima kelas: normal, *DoS, Probe, R2L, U2R*). Karena tidak menyertakan identitas *host*, setiap catatan koneksi diperlakukan sebagai *node* tersendiri, dengan ketidakseimbangan kelas pada *Remote-to-Local (R2L)/User-to-Root (U2R)* menjadikannya kasus uji yang tepat untuk mengevaluasi metrik performa.

2. Konstruksi Representasi Graf

Pada data *honeypot* dan *botnet*, graf dibangun dari relasi IP Address. Setiap alamat IP menjadi node, setiap pasangan koneksi sumber-tujuan menjadi *edge*, konsisten dengan prinsip representasi graf pada literatur *GNN* untuk deteksi intrusi. Pada dataset *NSL-KDD*, karena tidak tersedia identitas *host*, graf dibangun melalui pendekatan *k-nearest-neighbor* (**k = 10**, jarak *Euclidean* pada fitur ternormalisasi). Matriks ketetanggaan **A** kemudian dinormalisasi mengikuti formulasi standar *GCN*:

$$\hat{A} = \tilde{D}^{(-1/2)} (A + I) \tilde{D}^{(-1/2)} \quad (1)$$

dengan **I** adalah matriks identitas (*self-loop*) dan **D** adalah matriks derajat dari (**A + I**).

3. Arsitektur *Graph Convolutional Network*

Model inti adalah *Graph Convolutional Network (GCN)* dua lapis yang diimplementasikan dari nol menggunakan operasi matriks murni (tanpa *PyTorch/TensorFlow*) :

$$H^{(l+1)} = \sigma(\hat{A} \cdot H^{(l)} \cdot W^{(l)}) \quad (2)$$

dengan **H^(l)** adalah representasi node pada lapisan **ke-l (H^(0) = X), W^(l)** adalah bobot yang dipelajari, dan **σ** adalah **ReLU** (*Rectified Linear Unit*) pada lapisan tersembunyi serta *softmax* pada lapisan keluaran. Bobot diperbarui lewat *backpropagation* dan dioptimasi dengan *Adam*, regularisasi **L2** diterapkan untuk mengurangi *overfitting*.

4. Prosedur Eksperimen dan Hiperparameter

Setiap kondisi data dibagi menjadi subset latih, validasi, dan uji secara acak terstratifikasi. Tabel 1 merangkum konfigurasi eksperimen.

Tabel 1. Konfigurasi Eksperimen per Kondisi Data

Parameter	Honeypot	Botnet & C2	NSL-KDD
Jumlah node (graf)	7.905	3.350	4.000
Jumlah edge (graf)	9.990	6.254	29.571
Rasio latih : validasi : uji	60% : 20% : 20%	60% : 20% : 20%	70% : 15% : 15%
Jumlah unit tersembunyi	16	16	32
Jumlah epoch	150	150	150
Learning rate	0,02	0,02	0,01
Mode klasifikasi	Biner	Biner & multi-kelas	Multi-kelas (5 kelas)

5. Metrik Evaluasi

Mengingat ketidakseimbangan kelas yang signifikan, khususnya *R2L* dan *U2R* pada *NSL-KDD*, evaluasi tidak hanya mengandalkan akurasi keseluruhan, melainkan turut melaporkan *precision*, *recall*, *F1-score* per kelas, serta *Precision-Recall AUC* untuk kelas positif pada kondisi biner, mengikuti rekomendasi metodologis bahwa akurasi dapat membuat ketidakseimbangan kelas.

6. Model Rekomendasi Mitigasi

Setiap node yang diklasifikasikan sebagai ancaman dipetakan ke salah satu dari sebelas kategori mitigasi (misalnya : *brute-force login, port scanning, DoS/flood*, serangan web, *beaconing C2*, partisipasi *DDoS*). Masing-masing disertai rekomendasi tindakan dan rujukan kontrol standar *NIST Cybersecurity Framework Profile for Artificial Intelligence (NIST, 2025)* yang mencakup enam fungsi inti *Govern, Identify, Protect, Detect, Respond,* dan *Recover*, serta *Annex A* pada *ISO/IEC 27001:2022 (International Organization for Standardization [ISO/IEC], 2022)*. Pemetaan bersifat deterministik (*rule-based*), dengan dirancang agar klasifikasi dapat langsung ditelusuri ke kerangka tata kelola yang diakui secara luas.

Pembahasan

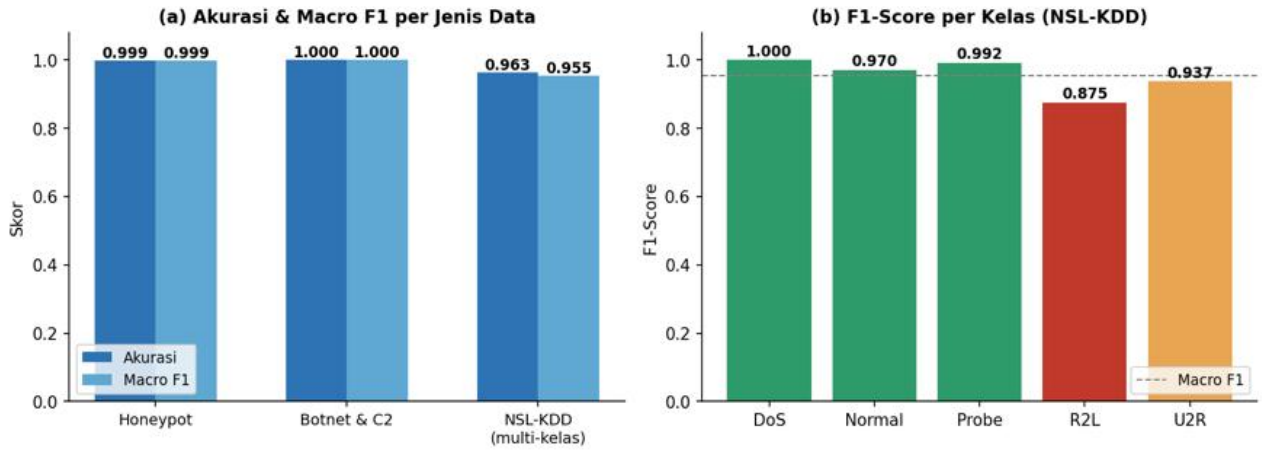
1. Keunggulan Representasi Berbasis Graf

Hasil pada ketiga kondisi data menunjukkan bahwa representasi berbasis graf memungkinkan model mengenali pola yang secara inheren bersifat relasional. Struktur *star-topology* di sekitar *host* target pada *honeypot*, serta topologi *many-to-few (beaconing C2)* dan *many-to-one (DDoS)* pada *botnet*, dimana secara konseptual tidak dapat ditangkap oleh model berbasis tabel yang mengevaluasi setiap baris data secara independen. Temuan ini konsisten dengan argumen utama pada tinjauan literatur *GNN* untuk deteksi intrusi, dimana menegaskan bahwa keunggulan pendekatan graf terletak pada kemampuannya mempelajari representasi dari relasi antarentitas tanpa memerlukan rekayasa fitur domain yang ekstensif. Perbedaan derajat maksimum yang mencolok pada graf *honeypot* dan *botnet* dibandingkan graf *NSL-KDD* berbasis *k-NN* juga menggambarkan bahwa graf relasi secara alami menghasilkan *node hub* yang merepresentasikan target atau infrastruktur kritis. Informasi struktural akan hilang sepenuhnya apabila data diproses sebagai tabel datar.

Visualisasi graf pada yang ditunjukkan pada Gambar 5 memperjelas temuan tersebut secara lebih konkret. *Node* normal (biru) yang berderajat tinggi tampak terkonsentrasi sebagai simpul pusat yang dikelilingi banyak *node* ancaman (merah) berderajat rendah. Pola spasial yang secara visual menegaskan struktur *star-topology honeypot*, satu *host* target menerima koneksi dari banyak IP penyerang yang masing-masing hanya berinteraksi dengan sedikit tujuan. Hubungan terbalik antara derajat *node* dan probabilitas diklasifikasikan sebagai ancaman (rata-rata derajat 1,38 untuk *node* ancaman berbanding 6,25 untuk *node* normal, sebagaimana dilaporkan pada Visualisasi Graf dengan Hasil Klasifikasi *GCN*) memberikan sinyal struktural yang secara intuitif dapat diverifikasi oleh analis keamanan tanpa perlu membedah bobot internal model. Sebuah bentuk yang melekat pada representasi graf itu sendiri, berbeda dari model yang umumnya memerlukan teknik penjelasan tambahan (misalnya, *SHAP* atau *LIME*) untuk mengungkap alasan di balik suatu prediksi. Karakteristik ini relevan secara praktis, dalam konteks operasional, kemampuan menelusuri mengapa suatu *node* ditandai sebagai ancaman. Misalnya karena posisinya yang terisolasi pada pinggiran graf dengan derajat sangat rendah, dapat mempercepat proses validasi manual sebelum tindakan mitigasi, sekaligus mengurangi risiko keputusan mitigasi yang keliru akibat *false positive* yang tidak dapat dijelaskan.

2. Pengujian Kinerja, Akurasi, dan Kecepatan Sistem

Untuk memperjelas hasil pengujian *GCN* dalam mendeteksi ancaman sekaligus menghasilkan rekomendasi mitigasi, Gambar 3 menyajikan visualisasi perbandingan akurasi dan *macro F1* pada ketiga kondisi data (panel a), serta rincian *F1-score* per kelas pada kondisi *NSL-KDD* yang paling memiliki tantangan secara ketidakseimbangan kelas (panel b).



Gambar 3. Hasil Pengujian *GCN* dalam Deteksi Ancaman dan Rekomendasi Mitigasi

Selain akurasi, kecepatan pemrosesan merupakan pertimbangan penting bagi kelayakan penerapan operasional suatu sistem deteksi ancaman, mengingat rekomendasi mitigasi yang dihasilkan hanya bernilai praktis apabila tersedia dalam rentang waktu yang relevan bagi analis keamanan. Tabel 2 merangkum waktu komputasi yang tercatat pada tiap tahapan pemrosesan untuk ketiga kondisi data. Diukur pada perangkat komputasi standar tanpa akselerasi *Graphic Processing Unit (GPU)*.

Tabel 2. Waktu Komputasi per Tahapan Pemrosesan

Kondisi Data	*Jumlah Node*	*Waktu Pelatihan (150 epoch)*	*Waktu Inferensi (Seluruh Node)*
Honeypot	7.905	0,468 detik	1,54 milidetik
Botnet & C2	3.350	0,263 detik	0,88 milidetik
NSL-KDD (multi-kelas)	4.000	1,514 detik	21,3 milidetik

Sebagaimana tampak pada Tabel 2, waktu inferensi tetap berada pada orde milidetik pada ketiga kondisi data. Kondisi *NSL-KDD* mencatat waktu inferensi per *node* tertinggi (0,0053 milidetik per *node*) meskipun total *node*-nya (4.000) lebih kecil dibandingkan kondisi *honeypot* (7.905 node). Mengindikasikan bahwa kepadatan graf lebih berpengaruh terhadap beban komputasi dibandingkan jumlah *node*, graf *NSL-KDD* berbasis k-*NN* memiliki rata-rata derajat 14,79, jauh lebih padat dibandingkan graf *honeypot* (2,53) dan *botnet* (3,73) yang bersifat *sparse* mengikuti pola relasi IP eksplisit. Waktu pelatihan penuh (150 *epoch*) juga tidak pernah melampaui dua detik pada kondisi data yang diuji. Dikombinasikan dengan tingkat akurasi yang tinggi (96,3%-100%) sebagaimana ditunjukkan pada Gambar 3(a), temuan ini mengindikasikan bahwa implementasi *GCN* dari nol pada penelitian ini tidak hanya akurat, tetapi juga cukup ringan secara komputasi untuk dipertimbangkan pada konteks penerapan yang mendekati waktu nyata, tanpa memerlukan perangkat keras akselerasi khusus seperti GPU.

3. Interpretasi Kritis terhadap Akurasi Sempurna

Performa hampir sempurna pada data *honeypot* (akurasi 99,9%) dan performa sempurna pada data *botnet* (akurasi dan *F1* 1,000). Kedua kondisi data berasal dari lingkungan *honeypot* yang secara inheren bersifat sintetis dan terisolasi, di mana fitur penguat antara *node attacker* dan *node* normal, seperti derajat keluar, rasio kegagalan autentikasi, dan keteraturan interval *beacon*, dirancang memiliki pemisahan statistik yang sangat kontras. Kondisi terisolasi ini secara alami menghasilkan separabilitas yang jauh lebih tegas dibandingkan trafik produksi nyata, sehingga performa tinggi pada kedua kondisi data ini semestinya diinterpretasikan sebagai bukti kelayakan pipeline (*proof of concept*) pada populasi data uji yang kini juga cukup besar (1.187 dan 503 node). Dan bukan estimasi performa pada lingkungan operasional berskala gigabit yang jauh lebih kompleks dan bervariasi. Sebaliknya, hasil pada data *NSL-KDD* yang mencakup ketidakseimbangan kelas yang justru menunjukkan variasi performa yang lebih realistis, dengan *F1* terendah pada kategori *R2L* (0,875). Pola ini selaras dengan tantangan yang secara umum dihadapi berbagai kerangka *machine learning* dalam menangani kelas minoritas *R2L* dan *U2R* pada *NSL-KDD* tanpa strategi penyeimbangan kelas yang eksplisit. Dengan demikian, pelaporan metrik per kelas dan *PR-AUC* bukan sekadar akurasi keseluruhan.

Dari catatan tersebut, penelitian ini menggabungkan dataset *honeypot* dan *botnet* pada kondisi standar dengan dataset berskala lebih besar (masing-masing 1.006.157 dan 1.011.311 baris *raw log*) menjadi satu kesatuan data uji. Konfigurasi model, hiperparameter, dan *seed* tetap identik dengan rancangan eksperimen pada Tabel 1, sehingga N uji yang lebih besar sepenuhnya mencerminkan populasi data uji Tunggal, dan bukan hasil dua percobaan berbeda yang dibandingkan.

4. Pengujian Teknik Penyeimbangan Kelas untuk Minoritas *R2L/U2R*

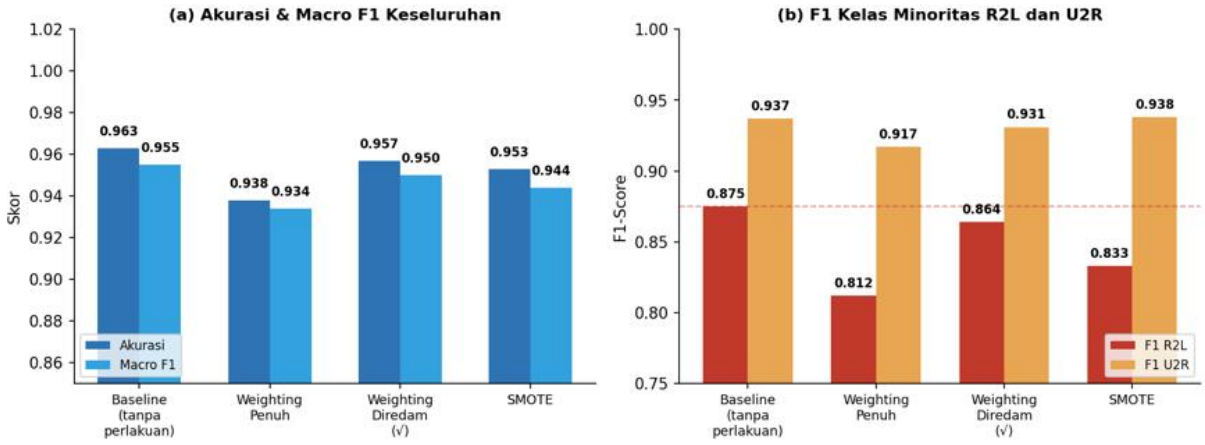
Dalam mengatasi ketidakseimbangan kelas *R2L/U2R*, subbab ini menguji secara empiris apakah class *weighting* pada *loss function* maupun teknik *resampling SMOTE (Synthetic Minority Over-sampling Technique)* [26] dapat meningkatkan performa kelas minoritas dibandingkan pelatihan tanpa perlakuan khusus. Tiga skenario yang diuji: (1) pembobotan penuh dengan skema *inverse-*

frequency standar, (2) pembobotan menggunakan akar kuadrat dari bobot penuh antara bobot seragam dan bobot penuh, dan (3) augmentasi *SMOTE* yang diimplementasikan dari nol mengikuti algoritma. Diterapkan hanya pada data latih untuk kelas *R2L* dan *U2R* hingga jumlah sampelnya menyamai kelas mayoritas, dengan graf *k-NN* dibangun ulang agar *node* hasil augmentasi memiliki *edge* yang konsisten dengan metodologi konstruksi graf. Ketiga skenario menggunakan hiperparameter, pembagian data, dan *seed* acak yang identik dengan konfigurasi yang sudah ada, serta dievaluasi pada data uji yang sama (600 *node*). Sehingga perbedaan hasil, murni disebabkan oleh perubahan strategi penyeimbangan kelas.

Tabel 3. Perbandingan Skenario *Class Weighting* pada Klasifikasi *NSL-KDD*

Skenario	*Akurasi*	*Macro F1*	*F1 R2L*
Tanpa weighting (baseline)	0,963	0,955	0,875
Weighting penuh	0,938	0,934	0,812
Weighting diredam (√)	0,957	0,950	0,864
SMOTE	0,953	0,944	0,833

Gambar 4 memvisualisasikan perbandingan keempat skenario tersebut, baik pada metrik keseluruhan (panel a) maupun rincian *precision, recall,* dan *F1* khusus kelas *R2L* (panel b).



Gambar 4. Perbandingan Skenario *Class Weighting* pada Klasifikasi NSL-KDD

Dari hasil tersebut, ketiga skenario penyeimbangan kelas tidak berhasil memperbaiki *baseline* pada *F1* kelas *R2L*. Pembobotan penuh menurunkan *F1 R2L* yang semula 0,875 menjadi 0,812, meskipun *recall* meningkat dari 0,831 menjadi 0,949. Ini dikarenakan presisi mengalami penurunan dari 0,925 menjadi 0,709. Pembobotan diminimalisir memberikan *trade-off* lebih moderat (F1 = 0,864). Dalam *SMOTE*, meskipun secara konseptual berbeda namun menambah keragaman sampel melalui interpolasi fitur mengubah bobot loss, sehingga menunjukkan pola yang serupa yaitu, *F1 R2L* mengalami penurunan menjadi 0,833, dengan pola *presisi-recall* yang sebanding (presisi turun ke 0,753, *recall* naik ke 0,932), sementara *F1 U2R* (0,938) relatif setara dengan *baseline* (0,937). Akurasi dan *macro F1* keseluruhan turut menurun pada ketiga skenario dibandingkan *baseline* (Gambar 6a), menunjukkan bahwa baik modifikasi *loss function* maupun augmentasi data pada level fitur sama-sama cenderung memperbaiki *recall* kelas minoritas dengan menhilangkan presisi secara tidak proporsional. Konsistensi pola ini di dua pendekatan yang secara mekanisme berbeda mengindikasikan bahwa tantangan utama kelas *R2L* kemungkinan besar bukan pada kuantitas sampel maupun pembobotan loss, melainkan pada tumpang tindih pola fitur antara *R2L* dan kelas lain yang telah diidentifikasi. Temuan ini sejalan dengan pengamatan pada penelitian terkait yang menemukan bahwa *class weighting* dapat mengganggu stabilitas pelatihan *GNN* pada kondisi ketidakseimbangan kelas yang ekstrem, memperkuat perlunya kehati-hatian sebelum menerapkan teknik penyeimbangan kelas secara baku pada representasi graf.

5. Perbandingan dengan Arsitektur *GNN* Lain

Penelitian ini secara sengaja menggunakan arsitektur *GCN second layer* yang relatif sederhana, dibandingkan dengan varian yang lebih kompleks seperti *graph attention network* yang mempelajari bobot relevansi berbeda untuk setiap tetangga, *GraphSAGE* dengan koneksi *jumping-knowledge* yang menggabungkan representasi dari berbagai kedalaman lapisan, maupun pendekatan penataan ulang fitur untuk memperkaya representasi multi-kelas. Hasil penelitian ini menunjukkan bahwa *GCN second layer* yang sederhana sudah cukup untuk mencapai performa tinggi pada ketiga kondisi data yang diuji. Ini mengindikasikan bahwa kompleksitas arsitektur tambahan mungkin baru diperlukan pada kondisi data dengan graf yang jauh lebih besar dan heterogen, atau ketika ancaman *adversarial* terhadap model itu sendiri menjadi pertimbangan utama. Penerapan arsitektur konvolusi graf dengan fokus pada deteksi *botnet* maupun pembelajaran kontrastif turut menegaskan bahwa pilihan arsitektur *GNN* idealnya disesuaikan dengan karakteristik domain, bukan diseragamkan secara universal. Keberhasilan penerapan *GCN* pada domain finansial seperti deteksi kecurangan transaksi *Bitcoin* turut memperkuat bahwa formulasi *GCN* tetap relevan lintas domain aplikasi keamanan siber, sejalan dengan cakupan luas survei berbasis graf dalam keamanan siber maupun tinjauan sistematis deteksi serangan berbasis graf.

6. Integrasi dengan Tata Kelola Keamanan

Kontribusi praktis penelitian ini terletak pada penerjemahan keluaran klasifikasi menjadi rekomendasi mitigasi yang secara otomatis terpetakan ke kontrol *NIST CSF* dan *ISO/IEC 27001:2022*. Pendekatan ini merespons kesenjangan yang umum ditemukan pada penelitian *GNN* untuk keamanan siber, yang cenderung berhenti pada tahap deteksi tanpa menjembatani hasil tersebut dengan kerangka tata kelola operasional. Relevansi pendekatan ini semakin meningkat mengingat kerangka *NIST Cybersecurity Framework* kini turut memuat profil khusus kecerdasan buatan, yang secara eksplisit menekankan kebutuhan untuk mengamankan sistem *Artificial Intelligence* itu sendiri sekaligus memanfaatkannya untuk memperkuat pertahanan siber. Dua sisi yang tercermin pada penelitian ini melalui penggunaan *GCN* sebagai alat deteksi sekaligus kesadaran akan keterbatasannya sendiri. Integrasi dengan *ISO/IEC 27001:2022* melengkapi kerangka *NIST* dengan kontrol operasional yang lebih rinci, sehingga organisasi yang telah menerapkan salah satu standar dapat langsung memanfaatkan pemetaan yang dihasilkan sistem tanpa perlu menerjemahkan ulang secara manual.

Hasil

1. Kinerja Model pada Ketiga Kondisi Data

Tabel 4 berikut merangkum kinerja model *GCN* pada data uji untuk ketiga kondisi data dalam mode klasifikasi biner (perbandingan antara normal dan ancaman).

Tabel 4. Kinerja Model GCN pada Data Uji (Mode Biner)

Kondisi Data	*N Uji*	*Akurasi*	*Macro F1*	*PR-AUC (Kelas Positif)*
Honeypot	1.187	0,999	0,999	1,000
Botnet & C2	503	1,000	1,000	1,000

Pada data *honeypot*, model mencapai akurasi 99,9% pada 1.187 *node* data uji (219 node berlabel normal dan 968 node berlabel penyerang), dengan satu *node* kelas normal salah diklasifikasikan. Pada data *botnet*, model mencapai akurasi dan *F1* sempurna pada 503 node data uji (117 normal, 386 bot/attacker). Skala penuh graf pada kedua kondisi data ini masing-masing mencakup 7.905 *node* dengan 9.990 *edge* (*honeypot*) dan 3.350 *node* dengan 6.254 *edge* (*botnet*), dengan rata-rata derajat *node* berturut-turut 2,53 dan 3,73.

2. Evaluasi Multi-Kelas pada *NSL-KDD*

Kondisi data *NSL-KDD* dievaluasi dalam mode multi-kelas (lima kategori: normal, *DoS*, *Probe*, *R2L*, dan *U2R*) pada graf berskala penuh (4.000 *node*, 29.571 *edge*, k = 10). Model mencapai akurasi keseluruhan 96,3% dengan *macro F1* sebesar 0,955. Tabel 5 menyajikan metrik performa secara terpilah per kelas.

Tabel 5. Metrik Performa per Kelas pada Kondisi Data NSL-KDD (Multi-Kelas)

Kelas	*Precision*	*Recall*	*F1-Score*	*Support*
DoS	1,000	1,000	1,000	56
Normal	0,955	0,986	0,970	365
Probe	0,984	1,000	0,992	61
R2L	0,925	0,831	0,875	59
U2R	1,000	0,881	0,937	59

Sebagaimana tampak pada Tabel 5, performa model tidak seragam di seluruh kelas. Kategori *DoS* dan *Probe* menunjukkan *F1* mendekati atau mencapai 1,000, sedangkan kategori *R2L* mencatat *F1* terendah (0,875), diikuti *U2R* (0,937). Pola ini konsisten dengan kesulitan klasifikasi minoritas yang umum ditemukan pada literatur *NSL-KDD*, di mana kategori *R2L* dan *U2R* secara inheren memiliki jumlah sampel yang jauh lebih sedikit dan pola fitur yang 59umpeng tindih dengan kelas normal.

3. Ringkasan Struktur Graf

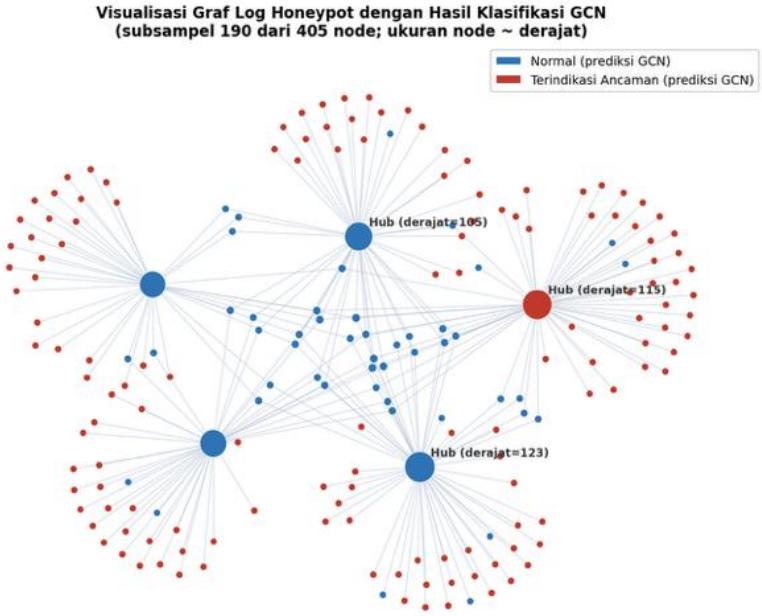
Tabel 6 menunjukkan bahwa ketiga graf memiliki karakteristik struktural yang berbeda secara mencolok. Graf *honeypot* dan *botnet* memiliki derajat maksimum yang jauh lebih tinggi dibandingkan rata-ratanya (mengindikasikan *node hub*, seperti *host* target *honeypot* atau *server C2*), sedangkan graf *NSL-KDD* berbasis *k-NN* memiliki distribusi derajat yang jauh lebih homogen (derajat maksimum mendekati k = 10, sesuai desain konstruksinya).

Tabel 6. Karakteristik Graf pada Ketiga Kondisi Data

Karakteristik	*Honeypot*	*Botnet & C2*	*NSL-KDD*
Jenis konstruksi graf	Relasi IP eksplisit	Relasi IP eksplisit	Kemiripan k-NN
Jumlah node	7.905	3.350	4.000
Jumlah edge	9.990	6.254	29.571
Rata-rata derajat	2,53	3,73	14,79
Derajat maksimum	2.019	434	45
Node terisolasi	0	0	0

4. Visualisasi Graf dengan Hasil Klasifikasi GCN

Untuk melengkapi metrik kuantitatif pada Tabel 4, 5 dan 6, Gambar 5 menyajikan visualisasi langsung graf *log honeypot* beserta hasil klasifikasi model *GCN* pada tingkat *node*. Mengingat skala penuh graf kini mencapai ribuan *node*, ditampilkan sub-populasi ilustratif sebanyak 405 *node* (setara skala *honeypot* standar) untuk menjaga keterbacaan visual pola structural. Terdiri atas 8 *node* berderajat tertinggi pada sub-populasi tersebut (agar struktur hub tetap tampak) ditambah sampel acak dari *node* lainnya. Sub-sampel 190 *node* ditampilkan dari sub-populasi ini, dengan ukuran setiap *node* dibuat proporsional terhadap derajatnya.



Gambar 5. Visualisasi Graf Log Honeypot dengan Hasil Klasifikasi GCN

Analisis lebih lanjut terhadap sub-populasi 405 *node* ini mengungkap pola struktural yang konsisten dengan temuan pada populasi data uji yang lebih besar. Dari 10 *node* berderajat tertinggi pada graf, 9 di antaranya diklasifikasikan sebagai normal oleh model. Mengindikasikan bahwa *node-node* tersebut adalah infrastruktur target (misalnya: *host honeypot*) yang secara alami menerima banyak koneksi masuk dari berbagai sumber, bukan entitas yang berperilaku mencurigakan. Sebaliknya, *node* yang diklasifikasikan sebagai ancaman memiliki rata-rata derajat 1,38, jauh lebih rendah dibandingkan rata-rata derajat *node* normal sebesar 6,25, dengan 301 dari 302 *node* ancaman (99,7%) berderajat rendah (kurang dari atau sama dengan tiga). Pola ini menunjukkan bahwa model *GCN* secara implisit memanfaatkan sinyal derajat *node*. Selain fitur eksplisit seperti rasio kegagalan autentikasi dan jumlah port berbeda yang dihubungi sebagai salah satu penanda pembeda antara infrastruktur legitimate dan entitas penyerang.

5. Keluaran Rekomendasi Mitigasi

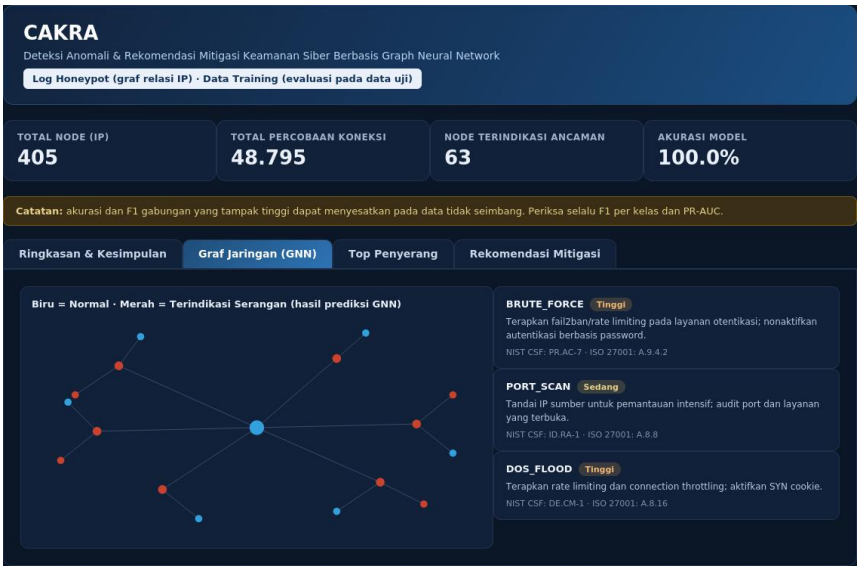
Setiap *node* yang terklasifikasi sebagai ancaman pada ketiga kondisi data secara otomatis menghasilkan rekomendasi mitigasi yang terpetakan ke kontrol *NIST CSF* dan *ISO/IEC 27001:2022*. Tabel 7 menyajikan pemetaan untuk beberapa kategori ancaman yang teridentifikasi.

Tabel 7. Pemetaan Kategori Ancaman ke Rekomendasi Mitigasi

Kategori Ancaman	*Tingkat Keparahan*	*Referensi NIST CSF*	*Referensi ISO/IEC 27001*
Brute-force login	Tinggi	PR.AC-7; DE.CM-3	A.9.4.2; A.9.4.3
Port scanning	Sedang	ID.RA-1; DE.CM-1	A.8.8; A.8.16
DoS / flood	Tinggi	DE.CM-1; RS.MI-1	A.8.16; A.5.26
Beaconing C2	Kritis	RS.MI-1; RS.AN-1	A.5.26; A.8.7
Partisipan DDoS	Kritis	RS.MI-1; DE.CM-1	A.5.26; A.8.16

6. Prototype Model Sistem

Sistem yang dikembangkan pada penelitian ini diimplementasikan pula sebagai *prototype* berbasis *web* untuk mendemonstrasikan kelayakan penerapannya. Gambar 6 menyajikan simulasi antarmuka *prototype* yang menampilkan panel ringkasan metrik (total *node*, total percobaan koneksi, *node* terindikasi ancaman, akurasi model), visualisasi graf jaringan dengan pengkodean warna hasil prediksi (biru untuk *node* normal, merah untuk *node* terindikasi ancaman), serta panel rekomendasi mitigasi yang tersusun otomatis berdasarkan kategori ancaman dan tingkat keparahannya.



Gambar 6. Simulasi Antarmuka Aplikasi CAKRA

Antarmuka ini dirancang agar keluaran model yang secara teknis berupa probabilitas klasifikasi pada tiap *node* graf dapat langsung diinterpretasikan oleh pengguna non-teknis (misalnya : analis keamanan operasional) tanpa memerlukan pemahaman mendalam terhadap mekanisme internal *GCN*. Ini sejalan dengan tujuan penelitian untuk menjembatani hasil deteksi dengan tindakan mitigasi yang konkret dan dapat segera ditindaklanjuti.

Kesimpulan dan Saran

Penelitian ini mengembangkan dan mengevaluasi sistem deteksi ancaman dan rekomendasi mitigasi keamanan siber berbasis *Graph Convolutional Network* yang diimplementasikan dari prinsip dasar, diuji pada tiga kondisi data dengan struktur relasional yang berbeda, yaitu *log honeypot*, trafik *botnet* dan *command-and-control*, serta dataset *benchmark NSL-KDD*. Model mencapai akurasi 99,9% pada graf *honeypot* dan akurasi 100% pada graf *botnet*, serta akurasi 96,3% dan *macro F1* 0,955 pada data *NSL-KDD*. Pelaporan metrik per kelas mengungkap bahwa performa model pada kategori minoritas seperti *R2L* (*F1* = 0,875) secara nyata lebih rendah dibandingkan kategori mayoritas, menegaskan pentingnya evaluasi yang tidak hanya mengandalkan akurasi keseluruhan. Integrasi keluaran deteksi dengan mesin rekomendasi mitigasi yang terpetakan ke *NIST Cybersecurity Framework* dan *ISO/IEC 27001:2022* menunjukkan bahwa pendekatan berbasis graf dapat diperluas melampaui klasifikasi semata, menjadi bagian dari alur kerja tata kelola keamanan yang dapat ditindaklanjuti secara konkret.

Berdasarkan temuan dan keterbatasan penelitian ini, beberapa arah pengembangan lanjutan disarankan sebagai berikut:

1. Validasi pada trafik nyata yang lebih heterogen diperlukan untuk mengonfirmasi generalisasi model di luar kondisi *honeypot* yang sintetis dan terisolasi, termasuk kemungkinan kolaborasi dengan penyedia infrastruktur *honeypot*.
2. Eksplorasi arsitektur *GNN* yang lebih kompleks, seperti *graph attention network* atau *GraphSAGE* dengan koneksi *jumping-knowledge*. Disarankan untuk kondisi data dengan graf berskala jauh lebih besar dan heterogen, guna menguji apakah kompleksitas tambahan memberikan peningkatan performa yang signifikan dibandingkan *GCN second layer* yang digunakan pada penelitian ini.
3. Integrasi *large language model* dengan *GNN* dan *explainable AI*. Sebagaimana mulai dieksplorasi pada penelitian generasi ke depan, seperti sistem deteksi intrusi, berpotensi memperkaya interpretabilitas rekomendasi mitigasi yang dihasilkan sistem.

Ucapan Terimakasih

Ucapan terima kasih disampaikan kepada Kementerian Pendidikan Tinggi, Sains, dan Teknologi Republik Indonesia atas dukungan finansial melalui Hibah Penelitian Dosen Pemula Tahun Anggaran 2026 dengan judul *Intelligent Cybersecurity Mitigation Recommendation System*: Pendekatan Adaptif dengan *Graph Neural Networks*. Dan Nomor Kontrak 285/C3/DT.05.00/PL-BARU/2026 tanggal 30 Januari 2026 dan No. Kontrak Turunan 071/LL6/AL.04.03/PL-BARU/2026 tanggal 2 Februari 2026.

Referensi

[1] T. Bilot, N. El Madhoun, K. Al Agha, and A. Zouaoui, "Graph neural networks for intrusion detection: A survey," IEEE Access, vol. 11, pp. 49114–49139, 2023, doi: 10.1109/ACCESS.2023.3275789.

[2] M. Zhong, M. Lin, C. Zhang, and Z. Xu, "A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges," Computers & Security, vol. 141, p. 103821, Jun. 2024, doi: 10.1016/j.cose.2024.103821.

[3] L. Xu, Z. Zhao, D. Zhao, X. Li, X. Lu, and D. Yan, "AJSAGE: An intrusion detection scheme based on jump-knowledge connection to GraphSAGE," Computers & Security, vol. 150, art. 104263, 2025, doi: 10.1016/j.cose.2024.104263.

[4] H.-D. Le and M. Park, "Enhancing multi-class attack detection in graph neural network through feature rearrangement," Electronics, vol. 13, no. 12, p. 2404, Jun. 2024, doi: 10.3390/electronics13122404.

[5] P. Deng and Y. Huang, "Edge-featured multi-hop attention graph neural network for intrusion detection system," Computers & Security, vol. 148, art. 104132, 2025, doi: 10.1016/j.cose.2024.104132.

[6] A. S. Ahanger, S. M. Khan, F. Masoodi, and A. O. Salau, "Advanced intrusion detection in Internet of Things using graph attention networks," Scientific Reports, vol. 15, art. 9831, Mar. 2025, doi: 10.1038/s41598-025-94624-8.

[7] H. G. Mohan, J. Kumar, and M. Nandish, "GrMA-CNN: Integrating spatial-spectral layers with modified attention for botnet detection using graph convolution for securing networks," International Journal of Intelligent Engineering and Systems, vol. 18, no. 1, 2025, doi: 10.22266/ijies2025.0229.72.

[8] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, "Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques," Sensors, vol. 24, no. 11, p. 3571, 2024, doi: 10.3390/s24113571.

[9] G. Karyağdı and İ. Özçelik, "Botnet node detection using graph learning," Applied Sciences, vol. 16, no. 1, p. 24, 2026, doi: 10.3390/app16010024.

[10] A. Asiri and K. Somasundaram, "Graph convolution network for fraud detection in Bitcoin transactions," Scientific Reports, vol. 15, art. 11076, Apr. 2025, doi: 10.1038/s41598-025-95672-w.

[11] Y. Li, G. Chen, and Z. Dong, "Multi-view graph contrastive representative learning for intrusion detection in EV charging station," Applied Energy, vol. 385, p. 125439, May 2025, doi: 10.1016/j.apenergy.2025.125439.

[12] F. Abdullayeva and S. Suleymanzade, "Cyber security attack recognition on cloud computing networks based on graph convolutional neural network and GraphSAGE models," Results in Control and Optimization, vol. 15, p. 100423, 2024, doi: 10.1016/j.rico.2024.100423.

[13] G. Zurlo, E. Ronchieri, R. Cornali, L. B. Scarponi, D. Cesini, and L. Dell'Agnello, "Graph neural network solutions for interpretable anomaly detection in IT infrastructure monitoring time series," Journal of Business Analytics, 2026, doi: 10.1080/2573234X.2025.2607576.

[14] L. Lin, A. Gu, F. Min, and S. Zhou, "Multi-level graph attention network-based anomaly detection in industrial control system," Actuators, vol. 14, no. 5, p. 210, 2025, doi: 10.3390/act14050210.

[15] S. M. Alshehri, S. A. Sharaf, and R. A. Molla, "Systematic review of graph neural network for malicious attack detection," Information, vol. 16, no. 6, p. 470, Jun. 2025, doi: 10.3390/info16060470.

[16] S. AboulEla and R. Kashef, "Leveraging large language models, graph neural networks, and explainable AI for revolutionizing the next-generation network intrusion detection systems," Journal of Intelligent Information Systems, vol. 63, pp. 1807–1835, 2025, doi: 10.1007/s10844-025-00964-2.

[17] Y. A. Farrukh, S. Wali, I. Khan, et al., "XG-NID: Dual-modality network intrusion detection using a heterogeneous graph neural network and large language model," Expert Systems with Applications, art. 128089, 2025, doi: 10.1016/j.eswa.2025.128089.

[18] Y. Wang, Z. Han, Y. Du, J. Li, and X. He, "BS-GAT: A network intrusion detection system based on graph neural network for edge computing," Cybersecurity, vol. 8, art. 27, 2025, doi: 10.1186/s42400-024-00296-8.

[19] R. Xu, G. Wu, W. Wang, et al., "Applying self-supervised learning to network intrusion detection for network flows with graph neural network," Computer Networks, vol. 248, art. 110495, 2024, doi: 10.1016/j.comnet.2024.110495.

[20] M. Wang, N. Yang, and N. Weng, "K-GetNID: Knowledge-guided graphs for early and transferable network intrusion detection," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 7147–7160, 2024, doi: 10.1109/TIFS.2024.3431932.

[21] T. Altaf, X. Wang, W. Ni, G. Yu, R. P. Liu, and R. Braun, "GNN-based network traffic analysis for the detection of sequential attacks in IoT," Electronics, vol. 13, no. 12, p. 2274, 2024, doi: 10.3390/electronics13122274.

[22] X. Ying, M. Pan, X. Chen, et al., "Research on virus propagation network intrusion detection based on graph neural network," Mathematics, vol. 12, no. 10, p. 1534, 2024, doi: 10.3390/math12101534.

[23] S. Ghosh, "Network traffic analysis based on cybersecurity intrusion detection through an effective automated separate guided attention federated graph neural network," Applied Soft Computing, vol. 169, art. 112603, 2025, doi: 10.1016/j.asoc.2024.112603.

[24] C. Huang and C. Wang, "CyberVeriGNN: A graph neural network-based approach for detecting fake cyber threat intelligence," Security and Privacy, vol. 8, no. 5, art. e70098, 2025, doi: 10.1002/spy2.70098.

[25] L. Lin, Q. Zhong, and Z. Liang, "E-GRACL: An IoT intrusion detection system based on graph neural networks," The Journal of Supercomputing, vol. 81, art. 42, 2025, doi: 10.1007/s11227-024-06471-5.

[26] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002, doi: 10.1613/jair.953.