**ISIAN SUBSTANSI PROPOSAL PENELITIAN**

*Petunjuk: Pengusul hanya diperkenankan mengisi di tempat yang telah disediakan sesuai dengan petunjuk pengisian dan tidak diperkenankan melakukan modifikasi template atau penghapusan di setiap bagian.*

## JUDUL

Tuliskan judul penelitian.

Deteksi Dini Serangan Distributed Denial of Service Berbasis Anomali Menggunakan Adaptive Streaming DBSCAN–KNN Fusion

## RINGKASAN

Isian ringkasan penelitian tidak lebih dari 300 kata yang berisi urgensi, tujuan, metode, dan luaran yang ditargetkan.

Deteksi dini serangan DDoS merupakan tantangan serius bagi organisasi dan pengguna layanan online. Hal ini di karena serangan DDoS memiliki potensi untuk mengganggu akses layanan, ketersediaan sumber daya pada jaringan yang mengakibatkan kerugian bagi organisasi dan penggunanya. Oleh karena itu perlu adanya visualisasi serangan untuk mendeteksi dini serangan DDoS dengan mengidentifikasi perubahan pada pola trafik yang mencurigakan. Sehingga tim keamanan dapat dengan cepat melakukan respons lebih cepat dan mengambil tindakan guna melindungi sistem sebelum serangan tersebut mencapai tahapan yang dapat merusak sistem dan layanan. Pada penelitian ini, kami berfokus pada model deteksi dini menggunakan analisis machine learning berbasis pada clutering dan classification. Metode yang digunakan adalah clustering DBSCAN dan classification K-NN, dimana pendekatan clustering melibatkan pengelompokan data trafik menjadi kelompok-kelompok yang memiliki karakter yang sama, sehingga membantu dalam mengidentifikasi trafik biasa atau anomali. Sedangkan model clustering dapat mengklasifikasikan setiap kelompok untuk menentukan apakah anomali tersebut merupakan jenis serangan DDoS atau bukan.

## KATA KUNCI

Isian kata kunci maksimal 5 kata yang dipisahkan dengan tanda titik koma (;)

DDoS; Deteksi Anomali; DBSCAN; K-NN; Peringatan Dini

## PENDAHULUAN

Pendahuluan penelitian tidak lebih dari 1000 kata yang terdiri dari:
1. Latar belakang dan rumusan permasalahan yang akan diteliti
2. Pendekatan pemecahan masalah
3. *State of the art* dan kebaruan
4. Peta jalan (*road map*) penelitian 5 tahun

*Sitasi disusun dan ditulis berdasarkan sistem nomor sesuai dengan urutan pengutipan, mengikuti format Vancouver*

## 1. LATAR BELAKANG DAN RUMUSAN MASALAH

Seiring pertumbuhan penggunaan internet membawa konsekuensi serius berupa eskalasi ancaman keamanan siber yang semakin kompleks dan adaptif. Studi terkini menunjukkan bahwa insiden serangan Distributed Denial of Service (DDoS) mengalami peningkatan tahunan sebesar 19%, mencerminkan tren yang mengkhawatirkan dalam lanskap keamanan siber global. Fenomena ini tidak hanya mengancam stabilitas operasional organisasi, tetapi juga menimbulkan risiko sistemik terhadap infrastruktur kritis yang menopang kehidupan modern (1). menyampaikan evolusi serangan DDoS telah menunjukkan karakteristik yang semakin canggih, dengan varian seperti amplification attacks, slow-rate attacks, dan mixed flash-DDoS events yang memperumit proses deteksi real-time (2).

Metode deteksi serangan jaringan konvensional menghadapi keterbatasan fundamental yang menghambat efektivitasnya dalam menghadapi ancaman DDoS modern. pendekatan signature-based detection, meskipun efektif untuk serangan yang sudah dikenal dan terdokumentasi, menunjukkan kelemahan signifikan dalam mendeteksi zero-day attacks dan varian serangan yang belum pernah teridentifikasi sebelumnya (3). Di sisi lain, anomaly-based detection systems, walaupun mampu mendeteksi pola serangan yang tidak dikenal, seringkali mengalami trade-off antara sensitivitas deteksi dan tingkat false positive rate yang dapat mengganggu operasional normal (4).

Machine Learning telah menunjukkan kontribusi yang signifikan dalam meningkatkan kapabilitas deteksi serangan siber, dengan berbagai studi eksperimental mendemonstrasikan pencapaian akurasi deteksi yang tinggi. Implementasi Enhanced K-Nearest Neighbor (K-NN) dengan optimasi KD-tree telah mencapai akurasi deteksi DDoS lebih dari 95.6% dengan kemampuan line-speed processing (5). pendekatan hybrid yang menggabungkan DBSCAN clustering dengan auto-encoder telah menunjukkan performa superior dengan akurasi 98.22%-98.51% pada dataset benchmark standar seperti KDDCup99, UNSW-NB15, CICIDS2017, dan CSE-CIC-IDS2018 (6).

Sensitivitas algoritma DBSCAN dan K-NN terhadap parameter konfigurasi merupakan masalah kritis yang belum terpecahkan secara komprehensif. Studi menunjukkan bahwa pemilihan parameter yang tidak optimal dapat mengubah kinerja sistem hingga 2%-46% dalam kondisi normal, dan bahkan ribuan persen dalam kasus ekstrim (7). Parameter eps dan minPts pada DBSCAN serta nilai k pada K-NN memerlukan fine-tuning yang sangat teliti untuk setiap environment deployment yang berbeda. Analisis literatur mengungkapkan bahwa tidak ada solusi produksi yang dapat melakukan tuning parameter eps/minPts DBSCAN secara otomatis dan robust pada traffic nyata, sehingga deployment masih bergantung pada manual tuning yang time-consuming dan error-prone.

Masalah pada penelitian ini adalah bagaimana menentukan adaptive parameter tuning pada DBSCAN dan adaptive K-Selection pada K-NN dapat meningkatkan stabilitas dan akurasi deteksi pada trafik jaringan yang dinamis.

## 2. PENDEKATAN PEMECAHAN MASALAH

Solusi dari permasalah di atas adalah mengembangkan model deteksi dini serangan DdoS berbasis anomaly detection yang mengintegrasikan algoritma DBSCAN dan K-NN dalam kerangka Adaptive Streaming DBSCAN-KNN Fusion (ASD-KF). Selain itu, menganalisis pengaruh adaptive parameter tuning pada DBSCAN dan adaptive K-Selection pada K-NN terhadap stabilitas dan akurasi deteksi pada traffic dinamis.

## 3. *STATE OF THE ART* DAN KEBARUAN

Penelitian sebelumnya telah mengembangkan beragam metode deteksi DDoS. Integrasi DBSCAN dengan *auto-encoder* dilaporkan mampu menghasilkan akurasi tinggi pada beberapa dataset keamanan jaringan. K-NN yang dipercepat menggunakan KD-tree juga telah diterapkan untuk deteksi DDoS dengan keluaran berbasis risiko yang lebih mudah dijelaskan. Studi lain menggunakan *deep learning* dan arsitektur saraf adaptif untuk mengantisipasi serangan sebelum eksekusi aktual. Pendekatan *ensemble*, seleksi fitur, hierarchical clustering, dan deteksi berbasis SDN juga telah dikaji, tetapi masing-masing masih memiliki keterbatasan pada kompleksitas komputasi, interpretabilitas, generalisasi, atau integrasi dengan pemrosesan *real-time*.

Berdasarkan studi yang ditinjau, belum ditemukan kerangka yang secara bersamaan mengintegrasikan empat komponen berikut dalam satu sistem: *streaming DBSCAN*, K-NN adaptif, analisis temporal untuk peringatan dini, dan *explainable AI*. Kebaruan penelitian ini terletak pada:

1. integrasi DBSCAN dan K-NN dalam pipeline deteksi DDoS berbasis *streaming real-time*;
2. penyesuaian otomatis parameter eps, minPts, dan k berdasarkan perubahan trafik;
3. fusi analisis pada tingkat *flow*, klaster, dan jaringan;
4. integrasi deteksi anomali dengan mekanisme peringatan dini berbasis pola temporal;
5. penyediaan penjelasan berbasis tetangga, jarak, fitur, dan jalur keputusan.

Kebaruan tersebut tidak hanya diarahkan pada peningkatan akurasi, tetapi juga pada stabilitas model, latensi pemrosesan, keterjelasan hasil, dan kesiapan penerapan operasional.

## 4. PETA JALAN PENELITIAN

Roadmap penelitian keamanan siber ini diarahkan pada pengembangan sistem deteksi serangan berbasis Artificial Intelligence secara bertahap. Fase pertama berfokus pada penguatan fondasi riset melalui penyusunan arah penelitian, pengembangan infrastruktur, seminar nasional, dan publikasi ilmiah.

Fase kedua difokuskan pada deteksi dini serangan DDoS berbasis log server menggunakan Adaptive Streaming DBSCAN–KNN Fusion. Penelitian ini menjadi dasar pengembangan metode deteksi serangan yang adaptif dan real-time.

Fase ketiga memperluas penelitian ke deteksi berbagai jenis serangan, seperti DoS, DDoS, XSS, brute force, scanning, dan SQL injection, dengan memanfaatkan multi-source log serta metode AI/ML yang sesuai dengan karakteristik masing-masing serangan.

Fase keempat diarahkan pada deteksi serangan dari luar server berdasarkan trafik jaringan, pola koneksi, dan perilaku layanan dengan bantuan Artificial Intelligence.

Fase kelima mengintegrasikan hasil deteksi dari dalam dan luar server untuk membentuk sistem deteksi multi-layer dan peringatan dini keamanan siber yang lebih akurat, adaptif, dan komprehensif.


.

## METODE

| |
|---|
| Isian metode atau cara untuk mencapai tujuan yang telah ditetapkan ditulis tidak melebihi 1000 kata. Bagian ini dapat dilengkapi dengan diagram alir penelitian yang menggambarkan apa yang sudah dilaksanakan dan yang akan dikerjakan selama waktu yang diusulkan. Metode penelitian harus dibuat secara utuh dengan penahapan yang jelas, mulai dari awal bagaimana proses dan luarannya, dan indikator capaian yang ditargetkan yang tercermin dalam Rencana Anggaran Biaya (RAB). |

Penelitian ini menggunakan pendekatan eksperimental untuk mendeteksi dini serangan DDoS berbasis Adaptive Streaming DBSCAN dan KNN Fusion. Tahapan penelitian ini meliputi pengumpulan data log, prapemrosesan data, perancangan model, training dan testing/ pengujian.

### 1. Sumber Data

Data penelitian berupa data log diperoleh dari:

a. dataset CIC-DDoS2019;
b. dataset CIC-IDS2017;
c. dataset UNSW-NB15;
d. dataset CTU-13;
e. trafik sintetis dari lingkungan testbed terkontrol.

Data mencakup trafik normal dan serangan DDoS kategori volumetrik, berbasis protokol, serta lapisan aplikasi.

### 2. Persiapan Data

Tahap persiapan data mencakup:

- pemeriksaan kelengkapan dan konsistensi data;
- penghapusan duplikasi dan data rusak;
- penanganan nilai hilang;
- normalisasi fitur;
- ekstraksi fitur statistik, perilaku, dan temporal;
- seleksi fitur berdasarkan korelasi dan *information gain*;
- pembentukan jendela temporal;
- pembagian data menjadi 70% pelatihan, 15% validasi, dan 15% pengujian.

Pembagian data dilakukan secara terstratifikasi agar distribusi kelas tetap terwakili. Untuk mencegah kebocoran data temporal, data dari jendela atau sesi serangan yang sama tidak ditempatkan pada subset pelatihan dan pengujian secara bersamaan.

## 3. Pengembangan Model

Eksperimen melibatkan:

a. DBSCAN dengan parameter statis;
b. K-NN dengan parameter statis;
c. DBSCAN–K-NN hibrida dengan parameter statis;
d. ASD-KF dengan parameter adaptif.
e.

DBSCAN digunakan untuk menghasilkan klaster dan mengidentifikasi *noise*. K-NN digunakan untuk mengklasifikasikan data yang memerlukan evaluasi lebih lanjut. KD-tree diterapkan untuk mempercepat pencarian tetangga. Mekanisme adaptif menyesuaikan eps, minPts, dan k berdasarkan distribusi fitur, kepadatan data, dan kinerja pada jendela trafik sebelumnya.

### 4. Sistem Peringatan Dini

Sistem menghitung skor peringatan berdasarkan:

$$W(t + \Delta t) = \alpha T(t) + \beta V(t) + \gamma M(t) + \delta S(t)$$

Di mana:

- $T(t)$: tren skor risiko;
- $V(t)$: volatilitas;
- $M(t)$: momentum perubahan;
- $S(t)$: faktor temporal atau musiman;
- $\Delta t$: horizon peringatan dini.

*Lead time* dihitung sebagai:

$$Lead\ Time = T_{peak} - T_{alert}$$

Sistem dinilai mampu memberikan peringatan dini apabila nilai *lead time* positif dan konsisten pada berbagai skenario serangan.

### 5. Indikator Keberhasilan

Penelitian dinyatakan berhasil apabila:

a. ASD-KF menunjukkan peningkatan F1-score dan penurunan *false positive rate* secara signifikan dibandingkan model tunggal;
b. konfigurasi adaptif memiliki performa lebih stabil daripada konfigurasi statis;
c. sistem menghasilkan *lead time* positif sebelum puncak eskalasi serangan;
d. sistem dapat memproses trafik secara *streaming* dengan latensi dan penggunaan sumber daya yang layak;
e. sistem menghasilkan penjelasan keputusan yang dapat ditelusuri melalui tetangga terdekat, fitur dominan, dan skor risiko.

## JADWAL PENELITIAN

Jadwal penelitian disusun berdasarkan pelaksanaan penelitian, ditulis dengan mengisi langsung tabel berikut dan diperbolehkan menambahkan baris sesuai banyaknya jenis kegiatan.

| No. | Nama Kegiatan | Bulan | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | Mencari rujukan dari jurnal dan mempelajari mengenai DDoS, DBSCAN dan K-NN | | | | | | |
| 2. | Membuat proposal Penelitian | | | | | | |
| 3. | Pengumpulan data, prapemrosesan data dan analisis untuk dijadikan dataset | | | | | | |
| 4. | Merancang model deteksi dini serangan DdoS menggunakan metode DBSCAN dan KNN | | | | | | |
| 5. | Training dan Testing Dataset | | | | | | |
| 6. | Pembuatan Laporan Kemajuan | | | | | | |
| 7. | Pembuatan Laporan Penelitian | | | | | | |
| 8. | Publikasi | | | | | | |

## LUARAN DAN TARGET CAPAIAN

Tuliskan target luaran wajib dan tambahan (jika ada) yang akan dihasilkan.

| No. | Kategori Luaran | Jenis Luaran | Target Capaian |
|---|---|---|---|
| 1. | Artikel Ilmiah | Jurnal Bereputasi Nasional (Terakreditasi Sinta 3) | published |

## RENCANA ANGGARAN BIAYA

**Total RAB: Rp 9.676.000,-**

| Jenis Pembelajaan | Komponen | Item | Kuantitas | Biaya Satuan | Total |
|---|---|---|---|---|---|
| Belanja Bahan | ATK | Pembelian pulpen, kertas | 1 | 100.000 | 100.000 |
| Belanja Bahan | Bahan penelitian | Materai | 3 | 12.000 | 36.000 |

| | | | | | |
|---|---|---|---|---|---|
| | (habis pakai) | | | | |
| Pengumpulan Data | Honor pembantu peneliti | Honor pengambilan data dari log server | 3 | 200.000 | 600.000 |
| Pengumpulan Data | Konsumsi | Biaya konsumsi makan rapat (2x2 orang) | 4 | 80.000 | 320.000 |
| Analisis Data | Honor pengolah data | Honor untuk pembersihan data dan pemberian label | 2 | 1.500.000 | 3.000.000 |
| Sewa Peralatan | Peralatan penelitian | Sewa VPS, 2Core, 4GB Ram, 80GB SSD | 6 | 245.000 | 1.470.00 |
| Sewa Peralatan | Peralatan penelitian | Sewa Internet | 6 | 150.000 | 900.000 |
| Pelaporan penelitian | Honor administrasi peneliti | Administrasi laporan, keuangan, surat-menyurat | 1 | 750.000 | 750.000 |
| Pelaporan penelitian Lainnya | Biaya publikasi Sinta-3 | Jurnal Bereputasi Nasional (terakreditasi SINTA 3) | 1 | 2.500.000 | 2.500.000 |

## DAFTAR PUSTAKA

Sitasi disusun dan ditulis berdasarkan sistem nomor sesuai dengan urutan pengutipan, mengikuti format Vancouver. Sumber pustaka mengutamakan hasil penelitian pada jurnal ilmiah yang terkini (maksimal 5 tahun terakhir). Hanya pustaka yang disitasi pada usulan penelitian yang dicantumkan dalam Daftar Pustaka.

1. Desai V, Pradhani A, Majukar S. Detection of DDoS Attack in TCP protocol using Hybrid Machine Learning Techniques. Int J Sci Res Sci Eng Technol. 2020 Aug 12;253–8. doi:10.32628/IJSRSET207459

2. E Silva GLFM, de Neira AB, Nogueira M. A Deep Learning-based System for DDoS Attack Anticipation. In: 2022 IEEE Latin-American Conference on Communications (LATINCOM). IEEE; 2022. p. 1–6. doi:10.1109/LATINCOM56090.2022.10000427

3. Fan CI, Lai YL, Shie CH. Clustering-Based Network Intrusion Detection System. In: 2022 IEEE Conference on Dependable and Secure Computing (DSC). IEEE; 2022. p. 1–8. doi:10.1109/DSC54232.2022.9888886

4. Wang X. Detecting Cyber Attacks from Untrusted Components in Smart Electricity Substations. Queensland University of Technology; 2023.

5. Feng Y, Li J, Sisodia D, Reiher P. On Explainable and Adaptable Detection of Distributed Denial-of-Service Traffic. IEEE Trans Dependable Secure Comput. 2024 Jul;21(4):2211–26. doi:10.1109/TDSC.2023.3301293

6. Kaliyaperumal P, Periyasamy S, Periyasamy M, Alagarsamy A. Harnessing DBSCAN and auto-encoder for hyper intrusion detection in cloud computing. Bulletin of Electrical Engineering and Informatics. 2024 Oct 1;13(5):3345–54. doi:10.11591/eei.v13i5.8135

7. Hiệp LH, Hiếu LX, Tuyến HT, Quy DT. NGHIÊN CỨU PHƯƠNG PHÁP PHÁT HIỆN SỚM XÂM NHẬP BẤT THƯỜNG MẠNG DDOS DỰA TRÊN CÁC THUẬT TOÁN HỌC MÁY. TNU Journal of Science and Technology. 2022 Aug 5;227(11):136–43. doi:10.34238/tnu-jst.6248