ANALISIS MODEL *INTRUSION DETECTION SYSTEM* (IDS) UNTUK MENINGKATKAN KEAMANAN JARINGAN KAMPUS BERBASIS *MACHINE LEARNING*

SKRIPSI

Untuk memenuhi persyaratan mencapai gelar Sarjana Komputer (S.Kom) pada Program studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang

Oleh:

Thomas Mahendra
162022054

PROGRAM TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026

HALAMAN PENGESAHAN

ANALISIS MODEL INTRUSION DETECTION SYSTEM (IDS) UNTUK MENINGKATKAN KEAMANAN JARINGAN KAMPUS BERBASIS MACHINE LEARNING

Oleh:

Thomas Mahendra
162022054

Menyetujui,

Pembimbing Utama,

Assoc. Prof. Dr. Ir. Zulhipni R. S Elsi, S. T., M. Kom
NBM/NIDN : 1338529/0205118002

Pembimbing Pendamping,

M. Ihsan, S.T.,M.Kom
NBM/NIDN:1299825/0207129001

Disetujui
Dekan Fakultas Teknik

Ir. A. Junaidi, M. T
NBM/NIDN : 763050/0202026502

Program Studi Teknologi Informasi
Ketua Program Studi

Dr. Karnadi, S.Kom., M.Kom
NBM/NIDN : 1088893/ 0210038202

HALAMAN PERSETUJUAN

Judul Skripsi : Analisis Model Intrusion Detection System (Ids) Untuk Meningkatkan Keamanan Jaringan Kampus Berbasis Machine Learning

Oleh **Thomas Mahendra** NIM **162022054** Skripsi ini telah disetujui dan disah kanoleh Tim Penguji Program Studi Teknologi Informasi Konsentrasi Manajemen Tata Kelola Teknologi Informasi Program Strata 1 Universitas Muhammadiyah Palembang pada 22 Agustus 2026 dan telah Dinyatakan **Layak / Lulus**

Palembang, 25 Agustus 2026

Mengetahui,

Ketua Program Studi Teknologi Informasi Universitas Muhammadiyah Palembang

Dr. Karnadi, S. Kom., M. Kom
NBM/NIDN: 1088893/0210038202

Tim Penguji
Ketua Penguji

Assoc. Prof. Dr. Ir. Zulhipni R. S Elsi, S.T.,M.Kom
NBM/NIDN: 1338529/0205118002

Penguji 1,

Dedi Haryanto, S. Kom., M. Kom
NBM/NIDN: 1337459/ 0201089001

Penguji 2,

Kemas Muhammad Wahyu Hidayat, S.Kom.,M.Kom
NBM/NIDN: 1255881/0225068904

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Thomas Mahendra
NIM	: 162022054
Fakultas/Prodi	: Teknik / Teknologi Informasi
Judul Skripsi	: Analisis Model Intrusion Detection System (Ids) Untuk Meningkatkan Keamanan Jaringan Kampus Berbasis Machine Learning

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah benar-benar hasil karya asli saya sendiri bukan merupakan plagiarism, pencurian hasil karya orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material maupun non-material, ataupun segala kemungkinan lain yang pada hakekatnya bukan merupakan karya tulis skripsi saya secara orisinil dan otentik.

Bila dikemudian hari diduga kuat ada ketidaksesuaian antara fakta dengan kenyataan ini, saya bersedia diproses oleh tim Fakultas yang dibentuk untuk melakukan verifikasi, dengan sanksi terberat berupa pembatalan kelulusan/kesarjanaan.

Demikian surat pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak maupun demi menegakan integritas akademik di institusi ini.

Hormat Saya,

Thomas Mahendra
162022054

MOTTO DAN PERSEMBAHAN

MOTTO

"Fokus, konsisten, selesai."

PERSEMBAHAN

Dengan penuh rasa syukur kepada Tuhan Yang Maha Esa, karya sederhana ini saya persembahkan dengan segala kerendahan hati kepada:

1. **Kedua orang tua tercinta, Bapak Feros dan Ibu Hermawati**, yang menjadi alasan utama saya untuk terus melangkah meskipun jalan terasa berat. Terima kasih atas setiap doa yang tak pernah terputus, setiap pengorbanan yang mungkin tidak selalu terlihat, serta kasih sayang yang begitu tulus tanpa syarat. Tidak ada kata yang mampu menggambarkan betapa besar jasa kalian dalam hidup saya. Setiap tetes keringat, setiap usaha, dan setiap harapan yang kalian panjatkan menjadi kekuatan terbesar saya untuk bertahan hingga sejauh ini. Skripsi ini adalah wujud kecil dari rasa terima kasih saya atas segala yang telah kalian berikan, meskipun saya sadar bahwa ini belum sebanding dengan pengorbanan kalian.
2. **Kepada istri tercinta, Bunga**, yang selalu hadir di setiap proses perjalanan ini. Terima kasih atas cinta, kesabaran, pengertian, serta dukungan yang tidak pernah berhenti, bahkan di saat saya berada di titik lelah dan hampir menyerah. Kehadiranmu memberikan semangat baru bagi saya untuk terus melangkah dan menyelesaikan apa yang telah saya mulai.
3. **Kepada kakak tercinta, Sindy Nerentika, dan adik tersayang, Khava**, terima kasih atas kasih sayang, perhatian, dukungan, dan kebersamaan yang selalu diberikan. Kehadiran kalian menjadi bagian penting dalam perjalanan hidup saya. Semoga kita selalu dapat saling mendukung, menjaga, dan menjadi keluarga yang selalu memberikan kekuatan satu sama lain.

   diberikan, sehingga saya tidak pernah merasa sendiri dalam menjalani proses ini.

4. **Kepada dosen pembimbing dan seluruh civitas akademika Universitas Muhammadiyah Palembang**, yang telah memberikan ilmu, bimbingan, serta pengalaman berharga selama saya menempuh pendidikan. Terima kasih atas dedikasi dan kesabaran dalam mendidik serta membimbing saya hingga mampu menyelesaikan skripsi ini.
5. **Kepada teman-teman seperjuangan, khususnya Yedi Alsantani, Rifki Adilim, dan Hidayat Efendi**, terima kasih atas kebersamaan, dukungan, bantuan, serta semangat yang selalu kalian berikan. Kehadiran kalian membuat perjalanan ini terasa lebih ringan dan penuh makna. Setiap canda, diskusi, dan perjuangan yang kita lalui bersama akan selalu menjadi kenangan berharga.
6. **Dan yang terakhir, untuk diri saya sendiri, Thomas Mahendra.** Terima kasih karena tidak menyerah ketika keadaan terasa sulit, terima kasih karena tetap bertahan saat lelah datang berulang kali, dan terima kasih karena terus berusaha meskipun sering kali merasa ragu. Perjalanan ini bukanlah hal yang mudah, tetapi setiap langkah yang telah dilalui menjadi bukti bahwa saya mampu melewatinya. Skripsi ini bukan hanya tentang hasil akhir, tetapi tentang perjuangan, kesabaran, dan keteguhan hati dalam meraih sebuah tujuan.

Semoga karya ini dapat menjadi awal dari langkah yang lebih besar di masa depan, serta menjadi kebanggaan bagi orang-orang yang saya cintai

ABSTRAK

Intrusion Detection System (IDS) merupakan sistem keamanan jaringan yang digunakan untuk mendeteksi aktivitas serangan pada jaringan komputer. Penelitian ini bertujuan untuk menganalisis penerapan IDS berbasis machine learning menggunakan metode entropy dan Information Gain dalam mendeteksi serangan Denial of Service (DoS) pada jaringan kampus. Penelitian dilakukan menggunakan lingkungan simulasi jaringan virtual yang terdiri dari server, client, dan attacker menggunakan VirtualBox. Proses pengambilan data dilakukan dengan melakukan capture trafik normal dan trafik serangan menggunakan Wireshark. Simulasi serangan dilakukan menggunakan tools Hping3 pada sistem operasi Kali Linux dengan metode SYN Flood menuju port 22 (SSH) server target. Dataset hasil capture kemudian dianalisis menggunakan metode entropy dan Information Gain untuk proses seleksi fitur sebelum dilakukan klasifikasi menggunakan algoritma Decision Tree. Hasil penelitian menunjukkan bahwa sistem IDS mampu mendeteksi trafik serangan berdasarkan pola trafik abnormal yang didominasi paket TCP SYN. Penerapan metode entropy dan Information Gain membantu meningkatkan relevansi fitur sehingga proses klasifikasi trafik normal dan serangan dapat dilakukan dengan lebih efektif. Penelitian ini diharapkan dapat membantu meningkatkan keamanan jaringan kampus terhadap serangan DoS.

Kata Kunci: Intrusion Detection System, DoS, SYN Flood, Entropy, Information Gain, Decision Tree.

ABSTRACT

Intrusion Detection System (IDS) is a network security system used to detect attack activities on computer networks. This study aims to analyze the implementation of a machine learning-based IDS using entropy and Information Gain methods in detecting Denial of Service (DoS) attacks on campus networks. The research was conducted using a virtual network simulation environment consisting of a server, client, and attacker using VirtualBox. The data collection process was carried out by capturing normal traffic and attack traffic using Wireshark. Attack simulation was performed using the Hping3 tool on the Kali Linux operating system with the SYN Flood method targeting port 22 (SSH) of the target server. The captured dataset was then analyzed using entropy and Information Gain methods for feature selection before classification using the Decision Tree algorithm. The results showed that the IDS system was able to detect attack traffic based on abnormal traffic patterns dominated by TCP SYN packets. The implementation of entropy and Information Gain methods helped improve feature relevance so that the classification process between normal and attack traffic could be carried out more effectively. This research is expected to help improve campus network security against DoS attacks.

***Keywords**: Intrusion Detection System, DoS, SYN Flood, Entropy, Information Gain, Decision Tree.*

KATA PENGANTAR

Penulis memanjatkan puji syukur ke hadirat Allah SWT, Tuhan Semesta Alam, atas rahmat dan karunia-Nya sehingga Skripsi ini dapat diselesaikan dengan sukses dan tepat waktu. Laporan ini disusun untuk memenuhi persyaratan Skripsi bagi mahasiswa Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Muhammadiyah Palembang.

Penulis ingin menyampaikan ucapan terima kasih yang tulus kepada semua pihak yang telah membantu dalam pengembangan dan pelaksanaan proyek penelitian ini, antara lain:

1. Rektor Universitas Muhammadiyah Palembang, Prof. Dr. Abid Djazuli, S.E., M.M.
2. Dekan Fakultas Teknik Universitas Muhammadiyah Palembang, Ir. A. Junaidi, M.T.
3. Ketua Program Studi Teknologi Informasi, Karnadi, S.T., M.Kom.
4. Dosen Pembimbing Utama Skripsi, Assoc, Prof, Dr. Ir. Zulhipni Reno Saptura, S.T., M.Kom.
5. Dosen Pembimbing Pendamping, M. Ihsan, S.T., M.Kom.
6. Orang tua tercinta dan teman-teman kelompok "Tanpo Bolon".

Mengingat keterbatasan yang dimiliki, penulis sangat menghargai saran dan kritik membangun dari berbagai pihak demi penyempurnaan dan peningkatan kualitas proyek penelitian ini.

Palembang 25 Agustus 2026

Thomas Mahendra
162022054

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pengelolaan dan pemanfaatan jaringan komputer di berbagai sektor industri, khususnya di perguruan tinggi, telah mengalami perubahan signifikan akibat pesatnya perkembangan teknologi informasi [1]. Saat ini, jaringan komputer bukan sekadar alat komunikasi sederhana, melainkan komponen vital yang memfasilitasi pembelajaran berbasis digital, sistem informasi akademik, layanan administrasi kampus, pengelolaan data mahasiswa dan dosen, hingga kegiatan penelitian [2]. Akibat transformasi digital ini, jaringan kampus telah menjadi infrastruktur yang sangat penting, dan kualitasnya sangat menentukan mutu layanan pendidikan yang diberikan. Oleh karena itu, keamanan dan keandalan jaringan menjadi aspek krusial dalam pengelolaan teknologi informasi di perguruan tinggi [3].

Tingginya ketergantungan aktivitas akademik dan administrasi terhadap jaringan komputer menjadikan setiap gangguan pada jaringan sebagai permasalahan serius[4]. Gangguan jaringan dapat berdampak langsung pada terhambatnya proses pembelajaran daring, kesulitan akses sistem akademik, keterlambatan pengolahan data administrasi, serta terganggunya komunikasi antar civitas akademika[5]. Dalam jangka panjang, kondisi ini dapat menurunkan kualitas layanan institusi dan kepercayaan pengguna terhadap sistem teknologi informasi kampus[6]. Oleh karena itu, aspek keamanan jaringan menjadi sangat krusial untuk

menjamin keberlangsungan layanan serta melindungi data penting milik institusi dan seluruh civitas akademika[7].

Ancaman terhadap keamanan jaringan menjadi semakin beragam dan kompleks seiring dengan meningkatnya penggunaan jaringan komputer [8]. Serangan siber yang menyasar kelemahan dalam sistem jaringan dapat terjadi kapan saja dan mencakup Denial of Service (DoS), pemindaian (scanning), malware, serta akses ilegal [9]. Serangan-serangan ini sering kali memanfaatkan celah keamanan yang belum terdeteksi pada sistem atau perangkat jaringan yang saling terhubung [10]. Akibatnya, jaringan kampus rentan terhadap berbagai ancaman siber yang terus berubah seiring dengan kemajuan teknologi [11].

Serangan siber terhadap jaringan kampus berpotensi menimbulkan kerugian besar yang berdampak pada kegiatan akademik dan operasional [12]. Serangan yang berhasil dapat mengakibatkan penurunan kinerja jaringan, gangguan pada layanan penting, serta kebocoran data pribadi pengguna dan catatan akademik [13]. Serangan siber juga dapat mengganggu proyek penelitian, tugas administratif yang bergantung pada infrastruktur jaringan, serta proses belajar-mengajar. Oleh karena itu, diperlukan sistem keamanan jaringan yang mampu mengidentifikasi, menghentikan, dan menangani serangan secara efisien dan akurat [14].

Pemasangan Intrusion Detection System (IDS) merupakan salah satu metode populer yang digunakan untuk menjaga keamanan jaringan [15]. IDS memantau lalu lintas jaringan secara terus-menerus untuk mendeteksi aktivitas yang mencurigakan atau tidak lazim [16]. Dengan adanya IDS, administrator

jaringan dapat mengambil tindakan pencegahan atau perbaikan sebelum serangan menimbulkan dampak yang lebih serius. Dalam sistem keamanan jaringan kampus, IDS merupakan lini pertahanan awal yang sangat penting [18].

Namun demikian, IDS konvensional yang berbasis aturan atau signature memiliki berbagai keterbatasan[19]. Sistem ini hanya mampu mendeteksi serangan yang telah memiliki pola atau tanda tangan yang telah didefinisikan sebelumnya. Akibatnya, IDS konvensional kurang efektif dalam mendeteksi serangan baru atau serangan yang mengalami modifikasi pola[20]. Selain itu, IDS berbasis aturan cenderung menghasilkan tingkat kesalahan deteksi yang tinggi, seperti false positive yang memicu alarm palsu dan false negative yang menyebabkan serangan tidak terdeteksi[21].

Teknik pembelajaran mesin (machine learning) semakin banyak digunakan dalam pengembangan sistem deteksi intrusi (IDS) untuk mengatasi keterbatasan-keterbatasan tersebut. Tanpa hanya bergantung pada kriteria statistik, pembelajaran mesin memungkinkan komputer untuk mengidentifikasi pola dari lalu lintas jaringan secara otomatis [22]. Sistem deteksi intrusi berbasis pembelajaran mesin dapat mengklasifikasikan lalu lintas sebagai berbahaya atau normal dengan lebih akurat melalui pemanfaatan data historis. Selain itu, metode ini memungkinkan sistem untuk beradaptasi dengan lebih baik terhadap pola serangan yang terus berubah [23].

Terlepas dari berbagai manfaat tersebut, kualitas data dan pemilihan fitur merupakan faktor krusial bagi keberhasilan penerapan pembelajaran mesin dalam

IDS. Meskipun data jaringan sering kali memuat beragam karakteristik yang kompleks, tidak semuanya relevan dengan proses kategorisasi [24]. Penyertaan karakteristik yang tidak informatif dapat mengakibatkan penurunan akurasi deteksi, peningkatan kompleksitas komputasi, serta kualitas model yang kurang optimal. Oleh karena itu, pemilihan fitur yang tepat sangatlah penting dalam pengembangan IDS berbasis pembelajaran mesin [25].

Untuk mengatasi masalah ini, fitur-fitur yang paling relevan dan informatif harus ditentukan menggunakan teknik seleksi fitur yang efisien [26]. Dalam seleksi fitur, entropi dan information gain merupakan teknik yang sering digunakan untuk mengukur kedekatan data serta mengidentifikasi karakteristik terpenting untuk klasifikasi [26]. Information Gain mengukur penurunan ketidakpastian yang diperoleh dengan membagi data berdasarkan properti tertentu, sedangkan entropi mengukur tingkat ketidakpastian (atau ketidakprediksian) distribusi kelas di dalam data tersebut. Teknik-teknik ini membantu dalam memilih fitur yang benar-benar dapat meningkatkan kinerja model [27].

Penelitian ini bertujuan untuk mengkaji penggunaan entropi dan information gain dalam pengembangan sistem deteksi intrusi berbasis pembelajaran mesin (machine learning) untuk jaringan kampus, guna menjawab permasalahan yang telah disebutkan sebelumnya. Proyek ini diharapkan dapat meningkatkan akurasi deteksi serangan, mengurangi tingkat false positive dan false negative, serta menghasilkan sistem keamanan jaringan kampus yang lebih efisien, efektif, dan responsif terhadap serangan siber. Hasil penelitian ini juga diharapkan dapat

mendukung pengembangan mekanisme keamanan jaringan di lingkungan perguruan tinggi.

Penulis tertarik untuk membahas topik ini dalam proposal penelitian berjudul "Analisis Model IDS untuk Meningkatkan Keamanan Jaringan Kampus Menggunakan Machine Learning" karena permasalahan yang telah disebutkan pada bagian latar belakang.

1.2 Identifikasi masalah

Berdasarkan konteks yang dijelaskan di atas, berikut adalah hambatan utama dalam meningkatkan keamanan jaringan kampus:

1. Seiring dengan meningkatnya penggunaan jaringan komputer, keamanan jaringan kampus masih rentan terhadap berbagai ancaman.
2. Sistem deteksi intrusi (IDS) konvensional kurang adaptif dan lebih rentan terhadap kesalahan deteksi karena keterbatasannya dalam mengidentifikasi ancaman baru.
3. Meskipun pemilihan fitur memiliki dampak signifikan terhadap kinerja sistem deteksi intrusi berbasis pembelajaran mesin (machine learning), tidak semua fitur lalu lintas jaringan bersifat relevan atau informatif.
4. Untuk meningkatkan akurasi deteksi serangan, penggunaan teknik pemilihan fitur khususnya entropy dan information gain dalam sistem deteksi intrusi kampus belum dioptimalkan sepenuhnya.

1.3 Rumusan Masalah

Berdasarkan konteks dan identifikasi masalah yang telah diuraikan sebelumnya, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Seberapa baik sistem deteksi intrusi (IDS) berbasis machine learning dalam mengidentifikasi serangan pada jaringan kampus?
2. Seberapa baik sistem deteksi intrusi (IDS) dapat membedakan antara lalu lintas yang sah dan berbahaya pada jaringan kampus?
3. Apa dampak penggunaan teknik seleksi fitur entropy dan information gain terhadap peningkatan akurasi deteksi serangan pada IDS?
4. Sejauh mana teknik entropy dan information gain dapat menurunkan tingkat kesalahan deteksi, seperti false positive dan false negative, guna meningkatkan efisiensi dan akurasi IDS?

1.4 Batasan Masalah

Ruang lingkup penelitian ini ditetapkan sebagai berikut untuk memastikan penelitian tetap terfokus dan selaras dengan tujuan yang telah ditentukan:

1. Tujuan utama penelitian ini adalah untuk mengidentifikasi serangan Denial of Service (DoS) pada jaringan perguruan tinggi.
2. Data yang digunakan berupa kumpulan data simulasi lalu lintas jaringan yang mencakup lalu lintas normal maupun lalu lintas serangan.
3. Penelitian ini menggunakan pendekatan Decision Tree berbasis pembelajaran mesin (machine learning) yang menerapkan information gain dan entropi untuk pemilihan fitur.

4. Fokus penelitian ini terletak pada kemampuan sistem dalam membedakan antara lalu lintas yang sah dan lalu lintas berbahaya.

1.5 Tujuan Masalah

Berikut adalah tujuan penelitian yang didasarkan pada rumusan masalah yang telah disebutkan sebelumnya:

1. Mengevaluasi kinerja sistem deteksi intrusi (IDS) berbasis machine learning dalam mendeteksi serangan pada jaringan kampus.
2. Mengevaluasi kemampuan IDS dalam membedakan antara lalu lintas yang sah dan berbahaya pada jaringan kampus.
3. Mengkaji bagaimana penggunaan teknik seleksi fitur, khususnya entropy dan information gain, dapat meningkatkan kemampuan IDS dalam mengidentifikasi serangan.
4. Mengevaluasi efektivitas teknik entropy dan information gain dalam menurunkan tingkat kesalahan deteksi, termasuk false positive dan false negative.

1.6 Manfaat Penelitian

Berikut adalah keunggulan penelitian ini berdasarkan tujuan penelitian yang telah ditetapkan:

1. Menambah khazanah pengetahuan di bidang keamanan jaringan, khususnya terkait penggunaan machine learning dalam sistem deteksi intrusi (IDS).
2. Menjadi panduan bagi penelitian lanjutan mengenai penerapan teknik information gain dan entropi dalam deteksi serangan jaringan.

3. Membantu administrator jaringan mendeteksi serangan Denial of Service (DoS) secara lebih akurat dan efektif guna meningkatkan keamanan sistem.
4. Berfungsi sebagai sarana pembelajaran untuk membantu mahasiswa memahami bagaimana machine learning digunakan dalam sistem keamanan jaringan.

1.7 State Of The Art and Kebaruan

Tinjauan mengenai perkembangan terkini (state of the art), yang merangkum penelitian terdahulu yang relevan dengan topik studi ini, disajikan dalam Tabel 1. Tabel ini bertujuan untuk memberikan ringkasan mengenai perkembangan teknik, strategi, dan kesimpulan dari penelitian-penelitian sebelumnya, khususnya dalam bidang yang sedang dikaji. Dengan mengidentifikasi kelebihan dan kekurangan masing-masing penelitian, perbandingan semacam itu menjadi landasan untuk menentukan celah penelitian (research gap) serta menyoroti pentingnya dan orisinalitas studi yang diusulkan.

Tabel 1. 1 State Of The Art

No.	Judul Penelitian	Tujuan	Metode	Hasil Utama	Keterbatasan	Relevansi	Kebaruan
1.	Analisis Kinerja IDS Berbasis Signature untuk Serangan DoS	Mengidentifikasi kemampuan IDS tradisional mendeteksi DoS	Signature-based IDS (Snort)	Mampu mengenali serangan yang telah memiliki pola tetap	Tidak mampu mendeteksi serangan baru	Menjadi baseline perbandingan IDS modern	Digunakan sebagai pembanding karena tidak memanfaatkan entropy dalam analisis fitur
2.	Penerapan SVM untuk Deteksi Serangan DDoS	Mengklasifikasi trafik DoS/DDoS	Support Vector Machine	Mampu membedakan trafik normal dan serangan berdasarkan margin klasifikas	Sensitif terhadap pemilihan parameter	Membuktikan efektivitas ML untuk IDS	Belum menganalisis entropy sebagai dasar pemilihan fitur
3.	Deteksi Intrusi Jaringan Menggunakan	Membedakan trafik normal dan serangan	K-NN Classifier	Mengklasifikasikan trafik berdasarkan	Kurang efisien pada data berskala besar	Metode pembanding	Tidak membahas ketidakpastian data menggunakan entropy

	K-NNMengguna kan K-NN			kedekatan jarak antar data		model sederhana	
4.	Identifikasi Serangan DoS Menggunakan Naïve Bayes	Menganalisis pola DoS berdasarkan probabilitas	Naïve Bayes	Mampu mendeteksi serangan berdasarkan distribusi probabilitas data	Sensitif terhadap data tidak seimbang	Referensi metode probabilistik	Digunakan sebagai pembanding karena pendekatan probabilistik berbeda dengan entropy
5.	Deteksi Serangan DoS Menggunakan Decision Tree	Mengklasifikas ikan trafik normal dan DoS	Decision Tree (Entropy)	Menghasilkan aturan klasifikasi yang mudah dipaham	Rentan overfitting	Relevan untuk IDS yang interpretatif	Menggunakan entropy dan information gain sebagai dasar pemilihan fitur IDS
6.	Evaluasi IDS Berbasis Machine Learning pada Dataset Klasik	Mengevaluasi performa IDS ML	Decision Tree (Entropy)	Mampu mengidentifikasi fitur jaringan yang dominan	Dataset kurang representatif jaringan modern	Pembanding dataset lama	Menunjukkan keterbatasan entropy pada dataset klasik

7.	Deteksi DoS Menggunakan Deep Learning	Mendeteksi DoS pada trafik kompleks	CNN / LSTM	Mampu mengenali pola trafik kompleks secara otomatis	Membutuhkan sumber daya komputasi tinggi	Pembanding metode kompleks	Menegaskan keunggulan entropy dari sisi interpretabilitas
8.	Analisis IDS Menggunakan Dataset CIC-IDS	Evaluasi IDS pada dataset modern	Decision Tree (Entropy)	Efektif dalam mengidentifikasi fitur penting trafik jaringan	Proses preprocessing relatif lama	Dataset mendekati kondisi nyata	Mengadaptasi entropy pada dataset yang menyerupai jaringan kampus
9.	Analisis IDS Jaringan Kampus	Mendeteksi anomali jaringan kampus	Decision Tree (Entropy)	Mampu membedakan trafik normal dan serangan DoS	Belum diuji secara real-time	Sangat relevan dengan penelitian ini	Fokus penerapan entropy pada jaringan kampus
10.	Analisis Model IDS Berbasis Entropy	Meningkatkan kualitas deteksi DoS	Entropy & Information Gain	Memberikan analisis fitur dan kesalahan deteksi yang lebih terstruktur	Perlu optimasi struktur pohon	Menjadi dasar penelitian ini	Menganalisis entropy terhadap false positive dan false negative IDS

1.8 Sistematika Penulisan

Bab-bab berikut ini menyusun kerangka tesis ini:

PENDAHULUAN (BAB I)

Latar belakang, rumusan masalah, tujuan studi, urgensi penelitian, dan struktur tesis dibahas dalam bab ini.

TINJAUAN PUSTAKA (BAB II)

Sistem Deteksi Intrusi (IDS), pembelajaran mesin (machine learning), entropi, information gain, pohon keputusan, dan konsep-konsep lain yang mendasari studi ini dibahas dalam bab ini.

METODE PENELITIAN (BAB III)

Teknik studi, arsitektur jaringan, prosedur pengumpulan data, simulasi serangan, dan tahapan pemrosesan data diuraikan dalam bab ini.

HASIL DAN PEMBAHASAN (BAB IV)

Hasil implementasi, pengujian sistem IDS, analisis lalu lintas jaringan, serta pembahasan mengenai temuan penelitian disajikan dalam bab ini.

KESIMPULAN DAN SARAN (BAB V)

Berdasarkan temuan penelitian, bab ini menyajikan kesimpulan dan saran

DAFTAR PUSTAKA

[1] A. Zulherry, I. Riadi, And R. Umar, “Jite (Journal Of Informatics And Telecommunication Engineering) Anomaly Detection In Cloud Device-Based Information Technology,” Vol. 9, No. January, Pp. 584–596, 2026.

[2] A. Sandriana And F. Maulana, “Klasifikasi Serangan Malware Terhadap Lalu Lintas Jaringan Internet Of Things Menggunakan Algoritma K-Nearest Neighbour (K-Nn),” Vol. 03, No. 1, Pp. 12–22, 2022.

[3] T. Pustaka, “Menggunakan Metode Random Forest,” Vol. 8, No. 3, Pp. 2787–2793, 2024.

[4] N. O. Safira, E. Wahyudi, And F. Khair, “Analisis Manajemen Bandwidth Dan Keamanan Jaringan Menggunakan Metode Hierarchical Token Bucket Dan Port Knocking Pada Router Mikrotik,” Vol. 13, No. 2, Pp. 113–124, 2023.

[5] U. M. Malang And D. Tree, “Deteksi Dan Mitigasi Serangan Ddos Pada Software Defined Network Menggunakan Algoritma Decision Tree,” Vol. 2, No. 11, Pp. 1491–1502, 2020.

[6] A. Badar, F. R. Umbara, And P. N. Sabrina, “Peningkatan Klasifikasi Serangan Ddos Pada Sdn Menggunakan Xgboost Dan Ramoboost,” 2025, Doi: 10.33364/Algoritma/V.22-2.2460.

[7] M. L. Almanfaluthi, Z. Z. Shibghatullah, P. S. Informatika, And U. T. Digital, “Analisis Jaringan Wireless Untuk Rumah Kos Menggunakan Router Harry Pribadi Fitrian , Najwa Annisa Putri □ , Ikhsan Amrillah Arsy , Da ’ Ifa Maulana ,” Vol. 5, No. 2, Pp. 378–385, 2025.

[8] A. F. Saladin, M. Data, And T. N. Fatyanosa, “Pengembangan Alat Bantu Investigasi Serangan Siber Berdasarkan Log Server Web Menggunakan Algoritma K-Means,” Vol. 9, No. 12, Pp. 1–9, 2025.

[9] N. Flood And B. Supervised, “Jurnal Sains , Nalar , Dan Aplikasi Teknologi Informasi,” Vol. 4, No. 2, Pp. 129–137, 2025, Doi: 10.20885/Snati.V4.I2.38599.

[10] R. Fauzan, A. V. Vitianingsih, And D. Cahyono, “Application Of Classification Algorithms In Machine Learning For Phishing Detection Penerapan Algoritma Klasifikasi Pada Machine Learning Untuk Deteksi Phishing,” Vol. 5, No. April, Pp. 531–540, 2025.

[11] D. Z. Oktavia, D. A. Hidayat, D. Natalia, And S. K. Prabantara, “Machine Learning Performance Comparison For Web Application Security Threat Detection : A Systematic Review,” Vol. 5, No. 1, Pp. 326–339, 2026.

[12] I. Engineering, M. Jufri, F. I. Komputer, And U. I. Batam, “Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan That Network Security Is Very Influential On The Prevention Of Attacks Carried Out By Attackers .,” Vol. 5, No. 2, Pp. 98–108, 2021.

[13] M. B. Billah, M. Idhom, And H. Maulana, “Analisis Perbandingan Algoritma Machine Learning Untuk Deteksi Serangan Ddos Pada Jaringan Iot Comparative Analysis Of Machine Learning Algorithms For Ddos Attack Detection,” Vol. 4, Pp. 287–297, 2026.

[14] M. Ardiansyah, I. Suhardi, And A. Wahid, “Perancangan Dan Analisis Intrusion Detection System Terhadap Serangan Probe Menggunakan Metode Signature Based,” Vol. 03, Pp. 86–102, 2025.

[15] E. Prasetyo, R. D. Adityo, N. Suciati, And C. Fatichah, “Reduksi Data Latih Pada K-Support Vector Nearest Neighbor Menggunakan Entropy,” Pp. 1–6, 2018.

[16] P. Z. Wahida, M. Data, And K. Amron, “Pemanfaatan Data Log Suricata Dalam Pengembangan Model Machine Learning Untuk Deteksi Serangan Cross-Site Scripting (Xss),” Vol. 9, No. 12, Pp. 1–13, 2025.

[17] M. S. Ariyanto *Et Al.*, “Serangan Deauthentication Attack Pada Wireless

Access Point : Systematic Literatur Review," Vol. 9, No. 4, Pp. 6606–6612, 2025.

[18] N. Putri *Et Al.*, "Penerapan Feature Engineering Dan Hyperparameter Tuning Untuk Meningkatkan Akurasi Model Random Forest Pada Application Of Feature Engineering And Hyperparameter Tuning To Improve The Accuracy Of Random Forest Models On Credit Risk," Vol. 12, No. 2, Pp. 251–262, 2025, Doi: 10.25126/Jtiik.2025128472.

[19] D. Daniaty, B. Firmansyah, A. Ardiansyah, And T. Efendi, "Analisis Bibliometrik Pada Penerapan Artificial Intelligence Di Smart Manufacturing (Bibliometric Analysis On Application Of Artificial Intelligence In Smart Manufacturing)," Vol. 0, Pp. 491–506, 2022.

[20] J. I. Matematika, P. Stunting, I. Kabupaten, And K. Di, "Math Unesa," Vol. 13, No. 01, Pp. 236–245, 2025.

[21] C. M. Lauw, A. Anggrawan, N. Sulistianingsih, I. Komputer, And U. Bumigora, "Model Deteksi Serangan Jaringan Menggunakan Machine Learning Dengan Teknik Ensemble Learning," Pp. 24–38, 2023.

[22] M. Purnamasari And F. D. Hastuti, "Menggunakan Metode," Vol. 8, No. 2, Pp. 141–149, 2021.

[23] H. Rifa, R. Hamonangan, D. Ade, And K. Kaslani, "Implementasi Algoritma Decision Tree Dalam Klasifikasi Kompetensi Siswa," Vol. 06, No. 01, Pp. 15–20, 2022.

[24] M. Audina, A. Eka, I. W. Supriana, And I. K. Gede, "Klasifikasi Berita Hoaks Covid-19 Menggunakan Kombinasi Metode K-Nearest Neighbor Dan Information Gain," Vol. 10, No. 4, Pp. 319–328, 2022.

[25] I. Rahmadaniar, D. Adrian, A. Tondang, B. S. Fernando, And A. Setiawan, "Implementasi Firewall Menggunakan Iptables Untuk Melindungi Server Dari Serangan Ddos," No. 3, Pp. 1–10, 2024.

[26] K. Muhammad, W. Hidayat, And P. Sukadi, “Development Of A Web-Based Thesis Title Submission Information System : A Case Study At The Muhammadiyah University Of Palembang,” Vol. 02, Pp. 72–75, 2022.

[27] D. Haryanto, “Study Kepuasan Layanan Terhadap Sistem Akademik Menggunakan Serqual (Studi Kasus : Sekolah Menengah Kejuruan Negeri Di Kota Palembang) Service Satisfaction Study Of Academic System Using Serqual (Case Study : Middle Vocational School In Palembang City),” Vol. 1, No. 2012, 2018.