KLASIFIKASI *TRAFFIC* JARINGAN *ONLINE GAMBLING* BERBASIS *DEEP LEARNING*

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

Rahayu Prasiska

09011182126002

PROGRAM STUDI SISTEM KOMPUTER

JURUSAN SISTEM KOMPUTER

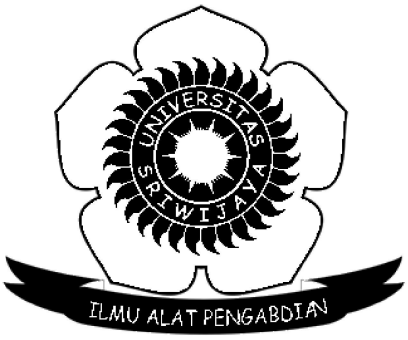
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

KLASIFIKASI *TRAFFIC* JARINGAN *ONLINE GAMBLING* BERBASIS *DEEP LEARNING*

TUGAS AKHIR



OLEH:

Rahayu Prasiska

09011182126002

PROGRAM STUDI SISTEM KOMPUTER

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

KLASIFIKASI *TRAFFIC* JARINGAN *ONLINE GAMBLING* BERBASIS *DEEP LEARNING*

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

RAHAYU PRASISKA

09011182126002

Pembimbing 1 : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**

NIP.197806172006041002

Pembimbing 2 : **Nurul Afifah, M.Kom**

NIP.199211102023212049

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DEEP LEARNING-BASED ONLINE GAMBLING NETWORK TRAFFIC CLASSIFICATION

As one of the requirements for completing the Bachelor's

Degree Program in Computer Systems.

By:

RAHAYU PRASISKA

09011182126002

Supervisor 1 : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**

NIP. 197806172006041002

Supervisor 2 : **Nurul Afifah, M.Kom**

NIP. 199211102023212049

Approved by,

Head of Computer System Department

Dr. Ir. Sukemi, M.T

196612032006041001

HALAMAN PERSETUJUAN

Telah diuji pada:

Hari : Jum'at

Tanggal : 11 Juli 2025

Tim Penguji:

1. **Ketua : Dr. Ir. Ahmad Heryanto, M.T.**
2. **Penguji : Ahmad Fali Oklilas, M.T.**
3. **Pembimbing 1 : Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing 2 : Nurul Afifah, M.Kom**

Mengetahui 9/8/25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

NIP. 196612032006041001

HALAMAN PERNYATAAN

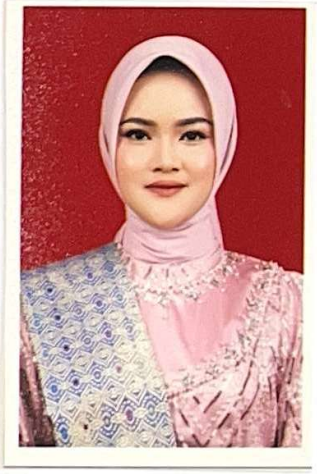
Yang bertanda tangan di bawah ini:

Nama : Rahayu Prasiska
NIM : 09011182126002
Program Studi : Sistem Komputer
Judul : Klasifikasi *Traffic* Jaringan *Online Gambling* Berbasis *Deep Learning*

Hasil Pengecekan Software *iThentivate*/Turnitin: 2%

Menyatakan bahwa laporan tugas akhir saya ini merupakan hasil karya sendiri dan bukan hasil menjiplak atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademi dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar atau tidak dipaksakan.



Indralaya, 28 Juli 2025

Rahayu Prasiska
09011182126008

Deep Learning-Based Online Gambling Network Traffic Classification

Rahayu Prasiska (09011182126002)

Dept. of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email: 09011182126002@student.unsri.ac.id

ABSTRAK

The rapid growth of online gambling activities has created an urgent need for accurate and efficient detection systems. This study aims to detect online gambling activity within network traffic using a combination of Autoencoder and Deep Neural Network (DNN) methods. The dataset was obtained from network traffic data in PCAP format, extracted using Tshark and converted into CSV format. The process began with feature extraction using an Autoencoder to generate low-dimensional data representations, followed by classification using a DNN model. Evaluation was conducted across three data split scenarios (70:15:15, 80:10:10, and 90:5:5) and various training configurations. The best results were achieved using the 70:15:15 data split with the fourth DNN variant at epoch 200, attaining an F1-score of 99.38% and an accuracy of 99.87%. The model demonstrated stable performance with no signs of overfitting and provided more representative evaluations than other data proportions. This research highlights the effectiveness of the Autoencoder-DNN approach in reliably and automatically identifying online gambling traffic.

Keywords: *Online Gambling, Network Traffic, Autoencoder, Deep Neural Network, Automatic Detection*

Klasifikasi *Traffic* Jaringan *Online Gambling* Berbasis *Deep Learning*

Rahayu Prasiska (09011182126002)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: 09011182126002@student.unsri.ac.id

ABSTRACT

Pesatnya pertumbuhan aktivitas judi *online* menimbulkan kebutuhan akan sistem deteksi yang akurat dan efisien. Penelitian ini bertujuan untuk mendeteksi aktivitas judi *online* dalam lalu lintas jaringan menggunakan kombinasi Autoencoder dan *Deep Neural Network* (DNN). *Dataset* diperoleh dari data lalu lintas jaringan dalam format PCAP yang kemudian diekstraksi menggunakan Tshark dan dikonversi ke format CSV. Proses dimulai dengan ekstraksi fitur melalui Autoencoder untuk menghasilkan representasi data berdimensi rendah, dilanjutkan dengan klasifikasi menggunakan model DNN. Evaluasi dilakukan dengan tiga skenario proporsi data (70:15:15, 80:10:10, dan 90:5:5) dan berbagai variasi parameter pelatihan. Hasil terbaik diperoleh pada proporsi data 70:15:15 dengan varian model DNN keempat pada *epoch* ke-200, yang mencapai *F1-score* sebesar 99,38% dan akurasi 99,87%. Model menunjukkan stabilitas performa tanpa indikasi *overfitting*, serta hasil evaluasi yang lebih representatif dibanding proporsi data lainnya. Penelitian ini menunjukkan bahwa pendekatan Autoencoder-DNN efektif dalam mengidentifikasi *traffic* judi *online* secara otomatis dan andal.

Kata Kunci: Judi *Online*, Lalu Lintas Jaringan, Autoencoder, *Deep Neural Network*, Deteksi Otomatis.

KATA PENGHANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dengan penuh rasa syukur, penulis panjatkan kehadirat Allah SWT, yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Skripsi ini dengan judul "**Klasifikasi *Traffic* Jaringan *Online Gambling* Berbasis *Deep Learning***". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana pada Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.

Penyusunan Tugas Akhir ini berdasarkan hasil penelitian dan kajian yang penulis lakukan, serta didukung oleh berbagai referensi yang relevan. Dalam kesempatan ini, penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada semua pihak yang telah memberikan dukungan dan bantuan selama proses penyusunan Tugas Akhir ini, khususnya kepada:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan sehingga bisa menyelesaikan skripsi ini dengan sebaik-baiknya.
2. Untuk kedua Orang Tua dan Adik penulis, skripsi ini adalah persembahan kecil sebagai wujud terima kasih atas segala dukungan, kasih sayang, dan pengorbanan yang telah kalian berikan.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. Selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi., M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Akademik dan Dosen Pembimbing I Skripsi.
6. Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Skripsi.
7. Kakak Angga selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.

8. Semua Dosen dan Staff Administrasi Jurusan Sistem Komputer Universitas Sriwijaya.
9. Kepada seseorang yang tidak kalah penting kehadirannya, Dandi Saputra. Terima kasih telah menjadi bagian dalam proses perjalanan penulis menyusun skripsi. Berkontribusi baik tenaga, waktu, menemani, mendukung, serta menghibur penulis dalam kesedihan, mendengarkan keluh kesah dan meyakinkan penulis untuk pantang menyerah hingga penyusunan skripsi ini terselesaikan.
10. Sahabat penulis dibangku perkuliahan yang selalu membersamai dalam empat tahun ini yaitu: Ayu Lestari, Sefiyah, Fitri Alfatiyah, dan M. Arif Abdillah yang banyak membantu penulis dalam mengerjakan skripsi dan tidak pernah henti saling menyemangati.
11. Terima kasih kepada Mutia Andini dan teman-teman dari riset Judi *Online* yang sudah membantu penulis dalam pengerjaan skripsi ini.
12. Teman-teman seperjuangan Angkatan 2021 Jurusan Sistem Komputer, terima kasih untuk segala bentuk dukungannya selama ini.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga tugas akhir ini bermanfaat dan berguna bagi khalayak.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, 22 Mei 2025

Penulis,

Rahayu Prasiska

NIM.09011182126002

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada penelitian [1] menyebutkan bahwa *online gambling* telah berkembang menjadi fenomena global yang semakin meluas dan menjadi salah satu bisnis paling populer sekaligus menguntungkan di dunia maya. Hal ini didorong oleh kemajuan teknologi komunikasi dan meningkatnya akses internet. Beragam jenis permainan judi kini tersedia melalui platform *online*, seperti permainan slot, kasino, hingga taruhan skor. Menurut sumber berita dari DetikInet [2], jumlah individu yang terlibat dalam perjudian *online* di Indonesia diperkirakan mencapai 8,8 juta orang, dengan nilai transaksi judi *online* yang berputar selama tahun 2024 diperkirakan mencapai Rp900 triliun. Menurut sumber berita dari Tempo [3], *online gambling* memberikan dampak negatif signifikan, baik secara sosial, seperti kecanduan, maupun dalam ekonomi dan keamanan. Aktivitas ini melibatkan banyak masyarakat dan berdampak pada sektor ekonomi, termasuk transaksi ilegal dan peningkatan kriminalitas. Pencegahan yang efektif sangat diperlukan, angka ini diprediksi akan terus meningkat, mengancam stabilitas sosial dan keamanan negara.

Menurut penelitian [4] mengungkapkan bahwa faktor utama yang memengaruhi niat seseorang untuk terlibat dalam *online gambling*, terutama di kalangan Generasi Z dan Milenial, meliputi harapan terhadap hasil yang diinginkan, kebiasaan, pengaruh sosial, kebutuhan akan hiburan, dorongan untuk mengembangkan diri, persepsi harga yang terjangkau, serta kemudahan akses ke platform perjudian *online*. Pada penelitian [5] menyebutkan bahwa sifat *online gambling* yang berisiko tinggi dan menawarkan kepuasan instan, banyak orang sulit melepaskan diri dari kecanduan berjudi tanpa henti. Masalah ini, terutama bagi mereka yang terlilit utang besar akibat perjudian seluler, dapat berkembang menjadi *pathological gambling* akibat pola pikir spekulatif mereka. Hal ini memberikan ancaman serius terhadap stabilitas keuangan dan kehidupan sehari-hari mereka. Untuk mengatasi dampak negatif tersebut, banyak negara dan wilayah telah mengambil langkah tegas dengan melarang atau membatasi penggunaan aplikasi

perjudian seluler. Selain itu, deteksi dini terhadap aktivitas perjudian *online* juga sangat penting untuk mencegah dan memitigasi dampak buruk yang ditimbulkan.

Menurut penelitian [5] Lalu lintas jaringan yang dihasilkan oleh aktivitas *online gambling* sering kali disamarkan melalui enkripsi data atau protokol yang menyerupai aktivitas legal, sehingga sulit terdeteksi oleh sistem keamanan konvensional. Seperti yang dijelaskan dalam penelitian [6] salah satu metode yang banyak digunakan untuk mendeteksi ancaman terhadap jaringan adalah menggunakan *Intrusion Detection System* (IDS). IDS adalah perangkat lunak yang dirancang untuk memantau lalu lintas jaringan dan mendeteksi aktivitas berpotensi membahayakan, yang membantu administrator sistem mengidentifikasi serta menanggulangi serangan dengan cepat. Sementara itu, menurut informasi yang disediakan oleh Snort [7], dengan menggunakan metode deteksi berbasis tanda tangan (*signature-based detection*), telah menjadi alat yang populer untuk mendeteksi ancaman pada jaringan komputer, termasuk mendeteksi aktivitas yang berhubungan dengan *online gambling*.

Menurut penelitian yang dilakukan oleh J. S. Abbasi et al. [8] telah menunjukkan efektivitas *deep learning* dalam mengekstrak fitur dan mengoptimalkan pencocokan pola dalam deteksi intrusi. Meskipun metode ini menunjukkan hasil yang signifikan dalam meningkatkan kinerja NIDPS, sebagian besar penelitian tersebut berfokus pada jenis serangan yang umum, tanpa mempertimbangkan ancaman baru yang spesifik, seperti *online gambling*. Penelitian ini menggunakan *dataset* yang berkaitan dengan deteksi intrusi dan menerapkan metode *Deep Learning-based Feature Extraction* (DLFE) dengan teknik autoencoder serta *Optimization of Pattern Matching* (OPM) untuk mengoptimalkan algoritma pencocokan pola tradisional. Hasil penelitian ini menunjukkan pengurangan waktu pemrosesan paket, peningkatan *throughput*, dan pengurangan penggunaan memori. Namun, penelitian ini juga menghadapi keterbatasan dalam hal pengujian dengan *dataset* yang lebih beragam dan kurangnya evaluasi terhadap berbagai jenis serangan, yang dapat meningkatkan generalisasi dan efektivitas model dalam kondisi nyata.

Menurut penelitian yang dilakukan oleh R. Ding et al. [9], yang menggunakan *dataset* USTC-TFC2016, ISCX2016, dan CICIoT2023, metode yang diterapkan adalah serangan *adversarial* universal yang dapat ditransfer menggunakan teknik *deep learning*. Hasil penelitian tersebut menunjukkan bahwa metode ini dapat melakukan serangan *adversarial* dengan tingkat keberhasilan rata-rata di atas 80%, 85%, dan 88% pada ketiga *dataset*, dengan biaya waktu yang sangat rendah, yaitu sekitar 0-0,3 ms. Namun, penelitian ini memiliki kekurangan, yaitu meskipun menunjukkan kinerja yang baik, serangan ini lebih fokus pada *transferabilitas* antar *dataset* dan model, sehingga kurang mempertimbangkan ancaman baru atau spesifik.

Pada penelitian yang dilakukan oleh M. Alotaibi et al. [10] yang menggunakan *dataset* UNSW-NB15, metode yang diterapkan adalah hibridisasi antara *Grey Wolf Optimization* (GWO) dan *Quantum Binary Bat Algorithm* (QBBA) untuk pemilihan fitur dalam deteksi intrusi. Hasil penelitian tersebut menunjukkan bahwa model GWQBBA mencapai akurasi klasifikasi sebesar 98,5% menggunakan *classifier Random Forest*. Namun, penelitian ini memiliki kekurangan, yaitu model ini hanya diuji pada *dataset* UNSW-NB15 dan belum menguji keandalan model pada *dataset* yang lebih besar atau beragam, serta tidak mempertimbangkan ancaman yang lebih spesifik, seperti serangan yang tidak umum dalam *dataset* tersebut.

Berdasarkan penelitian terdahulu yang menunjukkan efektivitas *deep learning* dalam deteksi intrusi, terutama dalam mengidentifikasi ancaman jaringan secara umum, penulis tertarik untuk melakukan penelitian yang lebih terfokus pada peningkatan kinerja Snort IDS dalam mendeteksi *traffic* judi *online*, yang merupakan ancaman spesifik yang sering kali terabaikan dalam penelitian sebelumnya. Meskipun *deep learning* telah diterapkan dalam berbagai metode deteksi intrusi, sebagian besar penelitian masih lebih fokus pada ancaman yang bersifat umum, sementara untuk ancaman yang lebih spesifik, seperti *traffic* judi *online*, penelitian lebih lanjut masih terbatas. Oleh karena itu, penelitian ini berfokus pada klasifikasi *traffic* jaringan *online gambling* dan memanfaatkan teknologi *deep learning* untuk memvalidasi hasil deteksi yang dihasilkan oleh Snort

IDS, dengan tujuan untuk meningkatkan akurasi dan efektivitas dalam mengidentifikasi ancaman tersebut.

Penelitian ini berjudul "**Klasifikasi *Traffic* Jaringan *Online Gambling* Berbasis *Deep Learning***." Penulis berharap hasil penelitian ini dapat memberikan kontribusi dalam meningkatkan akurasi deteksi *traffic* judi *online* menggunakan Autoencoder dan *Deep Neural Network*, serta memberikan wawasan lebih dalam mengenai bagaimana teknologi *deep learning* dapat memperbaiki efektivitas sistem deteksi intrusi dalam menangani ancaman yang lebih spesifik.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, dapat diuraikan perumusan masalah sebagai berikut:

1. Bagaimana proses ekstraksi data dilakukan pada data *traffic* jaringan untuk mendeteksi aktivitas *online gambling*?
2. Bagaimana Autoencoder (AE) dan *Deep Neural Network* (DNN) dapat digunakan untuk mendeteksi *traffic* jaringan *online gambling*?
3. Bagaimana hasil evaluasi kinerja model Autoencoder dan DNN berdasarkan metrik *Confusion Matrix*?

1.3. Batasan Masalah

Adapun batasan masalah yang dibahas dalam penelitian ini adalah:

1. *Dataset* yang digunakan dalam penelitian ini merupakan *dataset* yang dibuat oleh *research group* COMNETS Universitas Sriwijaya.
2. Penelitian ini hanya akan memfokuskan pada deteksi *traffic* jaringan yang berkaitan dengan aktivitas *online gambling*, dan tidak akan mencakup jenis *traffic* lain.
3. Metode yang digunakan dalam penelitian ini terbatas pada Autoencoder untuk representasi data dan *Deep Neural Network* (DNN) untuk klasifikasi.

1.4. Tujuan

Berdasarkan rumusan masalah di atas, tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui dan menjelaskan proses ekstraksi data dari data *traffic* jaringan *online gambling*.
2. Untuk menerapkan metode Autoencoder (AE) dan *Deep Neural Network* (DNN) dalam membangun model pendeteksian terhadap *traffic* jaringan yang mengandung aktivitas *online gambling*.
3. Mengevaluasi kinerja kombinasi model Autoencoder dan DNN dalam klasifikasi data menggunakan metrik *Confusion Matrix*.

1.5. Manfaat

Manfaat yang dapat dihasilkan dari penelitian ini adalah sebagai berikut:

1. Memberikan pemahaman teknis yang mendalam mengenai penerapan Autoencoder sebagai metode ekstraksi fitur dalam proses analisis data *traffic* jaringan, dengan menekankan bagaimana Autoencoder mampu membentuk representasi tersembunyi yang lebih ringkas dan informatif dari data mentah, sehingga dapat digunakan untuk mendukung tahapan analisis lanjutan seperti deteksi anomali atau klasifikasi.
2. Menjadi referensi yang bermanfaat dalam pemanfaatan metode *Deep Learning*, khususnya penggunaan Autoencoder (AE) dan *Deep Neural Network* (DNN), untuk mendeteksi *traffic* jaringan yang bersifat anomali, termasuk aktivitas yang mencurigakan seperti judi *online*, dengan harapan dapat memberikan kontribusi terhadap pengembangan sistem keamanan jaringan yang lebih adaptif, cerdas, dan responsif terhadap ancaman tersembunyi..
3. Menjadi referensi bagi pengembangan sistem deteksi aktivitas *online gambling* berbasis *deep learning* dengan validasi melalui metrik evaluasi seperti *Confusion Matrix*, sehingga dapat dimanfaatkan dalam sistem keamanan jaringan yang lebih cerdas dan efektif.

1.6. Sistematika Penulisan

Dalam proses penyusunan tugas akhir, penulis menggunakan sistematika penulisan yang terstruktur untuk memudahkan pemahaman isi dari setiap bab yang ada dalam skripsi.

BAB I PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, batasan masalah, tujuan, dan manfaat penelitian untuk menjaga fokus serta memberikan kontribusi ilmiah dan praktis.

BAB II TINJAUAN PUSTAKA

Bab ini membahas teori dan konsep yang mendasari penelitian, termasuk penelitian terdahulu, *online gambling*, *Intrusion Detection System* (IDS), *tools* yang digunakan seperti Snort dan Tshark, serta metode *deep learning* Autoencoder dan (DNN). Juga dijelaskan metrik evaluasi seperti *confusion matrix* untuk menilai performa model.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metodologi penelitian, mulai dari kerangka kerja, persiapan alat, pembuatan dan pengolahan *dataset,* hingga pemodelan dan evaluasi klasifikasi menggunakan *deep learning* pada *traffic* jaringan *online gambling*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian mulai dari analisis dan *preprocessing* data hingga pemodelan dengan Autoencoder dan DNN, serta evaluasi kinerjanya menggunakan metrik yang relevan.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan kesimpulan dari hasil penelitian yang dilakukan dan memberikan saran untuk penelitian selanjutnya serta rekomendasi untuk penerapan praktis dari temuan yang diperoleh dalam penelitian ini.

DAFTAR PUSTAKA

[1] H. Harahap and F. Ridho, "Detection of *Online Gambling* Web Defacement in University Domains Using Attack Signatures," *2024 Int. Conf. Artif. Intell. Blockchain, Cloud Comput. Data Anal. ICoABCD 2024*, pp. 73–78, 2024, doi: 10.1109/ICoABCD63526.2024.10704413.

[2] A. T. Haryanto, "Indonesia Darurat Judi *Online*, Pemainnya 8,8 Juta Orang!," *DetikInet*, 2024. [*Online*]. Available: https://inet.detik.com/law-and-policy/d-7649616/indonesia-darurat-judi-*online*-pemainnya-8-8-juta-orang

[3] O. Ivani S, "Budi Arie Beberkan Dampak Sosial Ekonomi dari Judi *Online*: Kasus Perceraian Melonjak jadi 1.572," *Tempo*, Oct. 03, 2024. [*Online*]. Available: https://www.tempo.co/ekonomi/budi-arie-beberkan-dampak-sosial-ekonomi-dari-judi-*online*-kasus-perceraian-melonjak-jadi-1-572--3006?

[4] J. C. Antonio, A. K. S. Ong, J. F. T. Diaz, M. M. L. Cahigas, and M. J. J. Gumasing, "The Perceived Risk and Return, Curiosity, and Control Analysis of *Online Gambling* Intention Among Gen Z and Millennials Using Extended UTAUT3," *Entertain. Comput.*, vol. 52, no. October 2024, p. 100918, 2025, doi: 10.1016/j.entcom.2024.100918.

[5] Z. Gu *et al.*, "Let *Gambling* Hide Nowhere: Detecting Illegal Mobile *Gambling* Apps via Heterogeneous Graph-Based Encrypted *Traffic* Analysis," *Comput. Networks*, vol. 243, no. January, p. 110278, 2024, doi: 10.1016/j.comnet.2024.110278.

[6] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, vol. 11, no. July, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[7] Snort, "What is Snort?," snort.org. Accessed: Jan. 07, 2025. [*Online*]. Available: https://snort.org/

[8] J. S. Abbasi, F. Bashir, K. N. Qureshi, M. Najam ul Islam, and G. Jeon, "*Deep Learning*-Based Feature Extraction and Optimizing Pattern Matching for Intrusion Detection Using Finite State Machine," *Comput. Electr. Eng.*, vol. 92, no. March, p. 107094, 2021, doi: 10.1016/j.compeleceng.2021.107094.

[9] R. Ding, L. Sun, W. Zang, L. Dai, Z. Ding, and B. Xu, "Towards Universal and Transferable Adversarial Attacks Against Network *Traffic* Classification," *Comput. Networks*, vol. 254, no. May, p. 110790, 2024, doi: 10.1016/j.comnet.2024.110790.

[10] M. Alotaibi *et al.*, "*Hybrid* GWQBBA Model for Optimized Classification of Attacks in Intrusion Detection System," *Alexandria Eng. J.*, vol. 116, no. November 2024, pp. 9–19, 2025, doi: 10.1016/j.aej.2024.12.057.

[11] O. Ussatova, A. Zhumabekova, Y. Begimbayeva, E. T. Matson, and N. Ussatov, "Comprehensive DDoS Attack Classification Using Machine Learning Algorithms," *Comput. Mater. Contin.*, vol. 73, no. 1, pp. 577–594, 2022, doi: 10.32604/cmc.2022.026552.

[12] M. Shoab and L. Alsbatin, "GRU Enabled Intrusion Detection System for IoT Environment with Swarm Optimization and Gaussian Random Forest Classification," *Comput. Mater. Contin.*, vol. 81, no. 1, pp. 625–642, 2024, doi: 10.32604/cmc.2024.053721.

[13] K. Narayana Rao, K. Venkata Rao, and P. R. Prasad, "A *hybrid* Intrusion Detection System based on Sparse autoencoder and *Deep Neural Network*," *Comput. Commun.*, vol. 180, no. April, pp. 77–88, 2021, doi: 10.1016/j.comcom.2021.08.026.

[14] F. S. Alrayes, M. Zakariah, S. U. Amin, Z. I. Khan, and J. S. Alqurni, "Network Security Enhanced with *Deep Neural Network*-Based Intrusion Detection System," *Comput. Mater. Contin.*, vol. 80, no. 1, pp. 1457–1490, 2024, doi: 10.32604/cmc.2024.051996.

[15] García-Pérez, A. Krotter, and G. Aonso-Diego, "The Impact of *Gambling* Advertising and Marketing on *Online Gambling* Behavior: An Analysis of

Spanish Data," *Public Health*, vol. 234, pp. 170–177, 2024, doi: 10.1016/j.puhe.2024.06.025.

[16] M. K. U. Ahamed and A. Karim, "Cascaded Intrusion Detection System Using Machine Learning," *Syst. Soft Comput.*, vol. 7, no. January, 2025, doi: 10.1016/j.sasc.2024.200182.

[17] M. Masdari and H. Khezri, "A Survey and Taxonomy of Fuzzy Signature-Based Intrusion Detection Systems," *Appl. Soft Comput. J.*, vol. 92, p. 106301, 2020, doi: 10.1016/j.asoc.2020.106301.

[18] M. J. Idrissi *et al.*, "Fed-ANIDS: Federated Learning for Anomaly-Based Network Intrusion Detection Systems," *Expert Syst. Appl.*, vol. 234, no. May, p. 121000, 2023, doi: 10.1016/j.eswa.2023.121000.

[19] R. Chinnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, "*Deep Learning*-Based Methods for Network Intrusion Detection Systems: A Systematic Review," *ICT Express*, vol. 11, no. 1, pp. 181–215, 2025, doi: 10.1016/j.icte.2025.01.005.

[20] Z. T. Sworna, Z. Mousavi, and M. A. Babar, "NLP Methods in Host-Based Intrusion Detection Systems: A Systematic Review and Future Directions," *J. Netw. Comput. Appl.*, vol. 220, no. September, p. 103761, 2023, doi: 10.1016/j.jnca.2023.103761.

[21] "What is Snort?", [*Online*]. Available: https://www.snort.org/

[22] A. Waleed, A. F. Jamali, and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek," *Comput. Networks*, vol. 213, no. March, p. 109116, 2022, doi: 10.1016/j.comnet.2022.109116.

[23] Z. Noor, S. Hina, F. Hayat, and G. A. Shah, "An Intelligent Context-Aware Threat Detection and Response Model for Smart Cyber-Physical Systems," *Internet of Things (Netherlands)*, vol. 23, no. June, 2023, doi: 10.1016/j.iot.2023.100843.

[24] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine Learning and *Deep Learning* Approaches for

CyberSecurity: A Review," *IEEE Access*, vol. 10, no. Ml, pp. 19572–19585, 2022, doi: 10.1109/ACCESS.2022.3151248.

[25] G. Chen and Z. Han, "The Rise of *Deep Learning*: AI and Engineering Applications under the Spotlight of the 2024 Nobel Prize," *Intell. Geoengin.*, 2025, doi: 10.1016/j.ige.2025.03.002.

[26] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband Tuned *Deep Neural Network* With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud," *IEEE Access*, vol. 8, pp. 181916–181929, 2020, doi: 10.1109/ACCESS.2020.3028690.

[27] Z. Yang, P. Baraldi, and E. Zio, "A Method for Fault Detection in Multi-Component Systems Based on Sparse Autoencoder-Based *Deep Neural Network*s," *Reliab. Eng. Syst. Saf.*, vol. 220, no. March 2021, p. 108278, 2022, doi: 10.1016/j.ress.2021.108278.

[28] M. Nakajima, K. Tanaka, and T. Hashimoto, "Neural Schrödinger Equation: Physical Law as *Deep Neural Network*," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 33, no. 6, pp. 2686–2700, 2022, doi: 10.1109/TNNLS.2021.3120472.

[29] S. Bhalgaonkar, M. Munot, and A. Anuse, "Model Compression of *Deep Neural Network* Architectures for Visual Pattern Recognition: Current Status and Future Directions," *Comput. Electr. Eng.*, vol. 116, no. March, p. 109180, 2024, doi: 10.1016/j.compeleceng.2024.109180.

[30] J. Erbani, P.-édouard Portier, E. Egyed-zsigmond, and D. Nurbakova, "Confusion Matrices : A Unified Theory," *IEEE Access*, vol. 12, no. October, 2024.

[31] D. Valero-Carreras, J. Alcaraz, and M. Landete, "Comparing Two SVM Models Through Different Metrics Based on the *Confusion Matrix*," *Comput. Oper. Res.*, vol. 152, no. April 2022, p. 106131, 2023, doi: 10.1016/j.cor.2022.106131.